2023

WACBD

WASHINGTON CENTER FOR BLEEDING DISORDERS

HIPAA Manual

WASHINGTON CENTER FOR BLEEDING DISORDERS
701 PIKE STREET, SUITE 1900 SEATTLE, WA 98101

Table of Contents

Privacy Policies

Security Policies

Appendices

Privacy Practices Overview	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 04/01/2022	**Effective Date:** 05/25/2022	**Next Review Date:** 05/25/2025

PURPOSE: Washington Center for Bleeding Disorders (WACBD) is required by the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Washington State laws to maintain the privacy of patient's health information, to provide individuals with this policy outlining our legal duties and privacy practices with respect to such information, and to abide by the terms of this policy. WACBD is required by law to notify affected individuals following a breach of their unsecured health information. WACBD safeguards the privacy of the comprehensive health care services provided to all patients receiving care, including interactions with payors, clearinghouses, partners, business associates and other healthcare professionals. WACBD's practice is to protect the privacy of all medical information about a patient or identifying a patient.

SCOPE: The scope of this policy applies to all WACBD patients and staff

POLICY STATEMENT: WACBD is dedicated to securing, protecting, and keeping private, the personal health information for all WACBD patients and any persons being treated and in our care.

COMMON TERMS:

Term	Definition
Accounting of Disclosures	A documented record of disclosures of a patient's PHI by the covered entity or business associate(s)
Business Associate	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to a covered entity
De-Identified Data	De-identification of PHI ensures that personal information cannot be tied to a specific patient. De-identification is achieved by removing certain data points that can be tied to a particular individual.
Electronic Health Records (EHR)	Electronic health records are any electronic record of patient health information generated within a clinical institution or environment, such as a hospital or doctor's office. This may include medical history, laboratory results, immunizations, demographics, etc.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under a covered entity
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Minimum Necessary	The minimum necessary standard is a key protection of the HIPAA privacy rule. It is based on the practice that protected health care information should not be used or disclosed when it is not necessary to satisfy a particular purpose. This standard requires healthcare entities to limit unnecessary or inappropriate access to and disclosure of protected health information.
Privacy Rule	The part of the HIPAA rule that addresses the saving, accessing, and sharing of medical and personal information of an individual, including a patient's own right to access

Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

Understanding PHI	
Protected Health Information (PHI)	PHI is typically found in medical forms, records, reports, bills, and documents. The following include identifiers of PHI: • Name • Address • Phone Number • Email Address • Dates (Except for year) DOB, Date of Death, Date of Service • SSN • Medical Records Number • IP Addresses/ URLs • Account Numbers • Health Plan Beneficiary Numbers • License Number/ License Plate Numbers/ Vehicle Identifiers • Device Identifiers • Biometric Identifiers (Fingerprints/ Voiceprints) • Full Face Image
De-Identified PHI	De-identified data has no privacy restrictions due to PHI/ direct identifiers are removed from records to the point where it cannot be traced back to any patient. De-identified patient data is health information from a medical record that has direct identifiers removed. Direct identifiers are information details that can be used to identify the patient from whose medical record the health information was derived.

Overview of HIPAA Uses and Disclosures	
HIPAA Uses and Appropriate Disclosures	HIPAA requires covered entities to safeguard PHI and sets boundaries on what PHI can be released with and without the patient's consent. PHI can be disclosed for two reasons: patient consent and HIPAA allows/requires the disclosure. The following are appropriate disclosure situations where PHI is released without patient consent.
Treatment	WACBD may disclose healthcare information about a patient internally and to an outside healthcare professional to provide treatment and to coordinate or manage healthcare services provided.
Payment	WACBD may disclose healthcare information to obtain payment for healthcare services provided. WACBD may disclose healthcare information to arrange payment, prepare bills, and to manage accounts.
Required by Law	WACBD may disclose medical information as required by law to do so. There are federal, state, and local laws requiring the disclosure of medical information. This

	disclosure includes worker's compensation, crime victim's compensation program, and examinations by WISHA (Washington Industrial and Safety Act).
Legal Proceedings	WACBD may disclose protected health information during any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), or in certain conditions in response to a subpoena, discovery request or other lawful process.
Law Enforcement	WACBD may also disclose protected health information for law enforcement purposes. These law enforcement purposes include: 1. legal processes and otherwise required by law, 2. limited information requests for identification and location purposes, 3. pertaining to victims of a crime, 4. suspicion that death has occurred as a result of criminal conduct, 5. in the event that a crime occurs on the premises of our practice, and 6. medical emergency (not on our practice's premises) and it is likely that a crime has occurred
Business Activities	WACBD may disclose information about patients when performing business activities for the improvement of quality of care, such as: • Reviewing and evaluating the skills, qualifications, and performance of healthcare providers taking care of patients. • Providing training programs for fellows, other healthcare providers or non-healthcare professionals for practice and professional development. • Compliance with outside organizations and government agencies that evaluate, certify or license healthcare providers, staff, or facilities. • Reviewing and improving the quality and efficiency of care provided to patients. • Planning for our organization's future operations. • Resolving grievances within WACBD. • Reviewing activities and using or disclosing medical information to make significant changes for the benefit of patients. • Working with outside entities such as attorneys, accountants and other providers who assist WACBD with compliance of this notice and other applicable laws. • Right to notification of breach of medical information.
Business Associates (BA)	The Privacy Rules allows covered providers and health plans to disclose protected health information to business associates if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

	Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate. The Privacy Rules requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate. WACBD obtains Business Associate Agreements (BAA), with every vendor that may be exposed to protected health care information.
Public Health	WACBD may disclose a patient's protected health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. For example, a disclosure may be made for the purpose of preventing or controlling disease, injury, or disability.
Communicable Diseases	WACBD may disclose a patient's protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.
Government Health Oversight	WACBD may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.
Abuse or Neglect	WACBD may disclose a patient's protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, WACBD may disclose a patient's protected health information if it is believed that a patient has been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.
Decedents	WACBD may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.
Research	The Privacy Rule permits WACBD to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: 1. Documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board

	2. Representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or 3. Representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought. WACBD also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes.

Understanding Disclosures to the Minimum Necessary Rule	
Minimum Necessary	WACBD puts into place measures that limits the use and disclosure of PHI to the minimum amount necessary to accomplish the intended task. The minimum necessary requirement is not imposed in any of the following circumstances: • disclosure to or a request by a health care provider for treatment • disclosure to an individual who is the subject of the information, or the individual's personal representative • use or disclosure made pursuant to an authorization • disclosure to HHS for complaint investigation, compliance review or enforcement • use or disclosure that is required by law; or • use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules • Disclosures allowed by Washington State's Medical Records-Health Care Information Access and Disclosure laws (RCW 70.02)
Access and Use	For internal uses, WACBD has developed and implemented policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. WACBD has identified the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

What is a Privacy Notice/Privacy Practices	
Notice of Privacy Practices	The Privacy Rule requires covered entities to make notice of privacy practices available to patients. The notice describes the ways in which WACBD may use and disclose protected health information, the duties that WACBD will keep PHI private, describe a patient's rights, including the right to file a grievance to HHS and to WACBD if they believe their privacy rights have been violated. WACBD's notice includes a point of contact for further information and for making

	complaints.(Appendix 1)
Notice Distribution	Following HIPAA and Washington State requirements, providers with a direct treatment relationship with individuals must have delivered privacy practices notice to patients as follows: • Not later than the first service encounter by personal delivery (for patient visits) • Supply notice to anyone on request • Make its notice electronically available.
Acknowledgement of Notice Receipt	WACBD will make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice. WACBD will acquire documentation of reason for patients who fail to provide written acknowledgement of receipt of privacy practices notice.

Understanding Patient Requested Restrictions	
Amendment	The Privacy Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If WACBD accepts an amendment request, reasonable efforts will be made to provide the amendment. If the request is denied, WACBD must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. WACBD must amend protected health information in its designated record set upon receipt of notice to amend from another WACBD.
Restriction Request	Individuals have the right to request that WACBD restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. Upon agreement to the request, WACBD will comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency. WACBD is under no obligation to agree to requests for restrictions

Understanding Patient Rights Under HIPAA	
Right to Access	Patients have the right to access PHI, Patients may access, inspect, obtain a copy of their PHI, and allow WACBD to share PHI with requested person or entity WACBD must complete the request within 15 days of request. If not possible, WACBD can extend an additional 21 days but must provide patient a written notice with reason of extension.
Right to Request Restriction	Patients have the right to request restriction of use and disclosure of PHI. This includes limiting PHI for healthcare operations, family member notification, and for

	payment reasons. [See procedure 5 for further information]
Right to Confidential Communications	Patients have the right to confidential communications with WACBD regarding their PHI. Patients may request how WACBD contacts them (ex. Being contacted by phone/ email or requesting if WACBD may leave voicemails on patient's phone)
Right to Amend Records	Patients have the right to amend their healthcare record. [See procedure 5 for more information]
Right to Request Accounting	Patients have the right to an accounting of the disclosures of their protected health information by WACBD or by WACBD's business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request. The Privacy Rule does not require accounting for allowable disclosures: • For treatment, payment, or health care operations • To the individual or the individual's personal representative • For notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories • Pursuant to an authorization • Of a limited data set • For national security or intelligence purposes • To correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody • Incident to otherwise permitted or required uses or disclosures. • Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities. WACBD must keep all requests with patient record with a copy of the written accounting provided to the patient and the name of the employee who provided the accounting. WACBD must complete the request within 60 days of request. If not possible, WACBD can extend an additional 30 days but must provide patient a written notice with reason of extension.
Right to File a Compliant	Patients have the right to file a complaint if they believe WACBD have violated a HIPAA Privacy Rule. Any patient or representative on patient's behalf may submit a written or verbal complaint regarding breach of a patient's privacy at WACBD without fear of jeopardizing their care to the privacy officer. Electronic correspondence should be sent to PG@wacbd.org or verbally by calling 206-614-1200 and speaking with the Privacy Officer. Patients also have the right to file a complaint with the OCR Patients have the options of: • The OCR Complaint Poral at: U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)

	• By Mail Print and mail the completed complaint and consent forms (found at HIPAA Complaint Process | HHS.gov) to: Centralized Case Management Operations U.S. Department of Health and Human Services 200 Independence Avenue, S.W. Room 509F HHH Bldg. Washington, D.C. 20201 • By email to OCRComplaint@hhs.gov

WACBD Responsibilities	
Policies and Procedures	WACBD, as a covered entity, will continue to create, implement, and maintain policies and procedures as required by HIPAA
Privacy Official	WACBD has a designated Privacy Official who is responsible for implementing privacy policies and is the point of contact for patients who file complaints.
Process for Complaints	WACBD has created a process for patients to easily file a complaint
Employee Training	All WACBD employees will be trained on HIPAA regulations on an annual basis
Mitigation	WACBD follows a mitigation plan to help mitigate any harmful effects that were caused by disclosure of PHI by its employees or BA.
No Retaliation	WACBD pledges to never retaliate against any patient or their representative for exercising their rights regarding their PHI. For more information see WACBD Whistleblower Policy

RELEVANT REFERENCES:

- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/permitted-uses/index.html
- Summary of the HIPAA Privacy Rule | HHS.gov
- https://www.cdc.gov/phlp/publications/topic/hipaa.html
- https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
- RCW 70.02: Medical Records-Health Care Information Access and Disclosure

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Accounting for Disclosures	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 05/05/2022	**Effective Date:** 05/25/2022	**Next Review Date:** 05/25/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: To establish a policy and procedure to ensure WACBD's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in providing an individual the right to receive an accounting of disclosures of and documenting persons who have accessed his/her Protected Health Information (PHI) made by WACBD.

SCOPE: The scope of this policy shall apply to health information that is generated during any of WACBD's normal business functions conducted under the auspices of WACBD or by any of its agents in all WACBD Units, Departments and owned or operated facilities or practices; and to any and all personnel or agents responsible for disclosing such information.

POLICY STATEMENT: Under the direction of the directors, managers, supervisors, and personnel over areas with responsibilities for disclosure of heath records (hard copy and electronic), WACBD shall ensure compliance with this policy.

DEFINITIONS:

Term	Definition
Accounting of Disclosures	Information about disclosures of a patient's PHI made by covered entity or business associate
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity
Disclosure	The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Personal Health Information (PHI)	Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI, under HIPAA (Health Insurance Portability and Accountability Act), is any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA covered entity, a healthcare provider, health plan or health insurer, or a healthcare clearinghouse, or a business associate of a HIPAA covered entity, in relation to the provision of past, present, or future healthcare or payment for healthcare services.

PROCEDURES:

Procedure 1- Understanding WACBD's Requirements	

Requirements	• WACBD will provide an individual with an accounting of disclosures of their PHI upon the individual's request.
	  ○ The individual's accounting of disclosure requests shall be completed by clinical/ medical administrative assistants
	  ○ Payer, legal, or other requests shall be completed by the medical billing manager
	  ○ An individual's request for an Accounting of Disclosures can be done either verbally or in written form
	• WACBD must provide the accounting in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by WACBD and the individual.
	• WACBD will act on an individual's request for an accounting disclosure within thirty (30) days of receipt of the request. If WACBD is unable to provide the accounting disclosure within thirty (30) days, it may extend the time period to provide the accounting disclosure by an additional thirty (30) days, but only if WACBD provides the individual with a written statement of the reasons for the delay and the date by which WACBD will provide the accounting disclosure prior to the expiration of the original 30-day period. WACBD is only permitted one extension per request.
	• WACBD will not charge patients for accounting of disclosures
	• As part of the accounting of the disclosures, WACBD will coordinate the releases of PHI with business associates as necessary.
	• If a law enforcement official states to WACBD that providing the accounting of disclosures is reasonably likely to impede law enforcement activities, WACBD must do the following:
	  ○ If the law enforcement statement is written and specifies the time a delay is required, delay providing the accounting of disclosures for time period specified; or
	  ○ If the law enforcement statement is oral, document the statement, the identity of the law enforcement official and temporarily delay providing the accounting of disclosures but for no more than 30 days from when the statement was made.
	  ○ If there is a law enforcement delay, WACBD will provide the accounting without the law enforcement disclosures within the required time period, and then provide the law enforcement disclosures upon expiration of the delay period requested.
	• Requests made for accountings of disclosures of PHI must be made to the employee or department designated by the EO, and/or Privacy Officer.

	WACBD shall provide the individual with the option to limit the accounting of disclosures to a specific time period, type of disclosure, or recipient.

Procedure 2- Understanding WACBD Responsibilities	

Responsibilities	• WACBD will implement a process to provide an accounting to individuals of all disclosures from the designated record set for requested time frame or up to six (6) years prior to the date of the request. The following disclosures must also be tracked and included in the accounting:
	  ○ For public health activities except for reports of child abuse or neglect
	  ○ For judicial and administrative proceedings
	  ○ For law enforcement purposes
	  ○ To avert a serious threat to health or safety
	  ○ For military and veterans' activities, the Department of State's medical suitability determinations, and government programs providing public benefits; and
	  ○ For workers' compensation
	  ○ The accounting disclosure must ***exclude*** any information that meets the definition of patient safety work product at 42 CFR 3.20.
	• WACBD must document and retain for six (6) years the following information:
	  ○ A copy of the written accounting given to the requesting individual.
	  ○ The titles of persons responsible for receiving and processing requests for an accounting disclosure.

Information Required to Include in Disclosures	An accounting must cover a period of six (6) years unless the request specifies a shorter period. The accounting for each disclosure must include: • date or approximate date range of the disclosure • name and address (if known) of the entity or person who received the PHI • brief description of the PHI disclosed • brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for disclosure (i.e., subpoena, etc.). If WACBD has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting of disclosures with respect to such multiple disclosures should provide the date of the last disclosure during the accounting period.
Information Not Required to be Included in Disclosures	An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity up to the six (6) years prior to the date on which the accounting is requested, except for disclosures: • To carry out treatment, payment, and health care • To individuals of PHI about them • Incidental uses and disclosures that occur as a byproduct of a permissible or required use or disclosure

	• Made pursuant to an authorization • On persons involved in the individual's care or other notification purposes • For national security or intelligence purposes • For Armed Services, National Security and Other Government Functions • To correctional institutions • That are part of a limited data • That occurred more than six (6) years before the individual's request

RELEVANT REFERENCES:

- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, 45 CFR Part 164.

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Authorization for Release of Protected Health Information	**Department:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 05/05/2022	**Effective Date:** 06/08/2022	**Next Review Date:** 06/08/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: It is the purpose of this policy to provide guidance to WACBD regarding the release of protected health information (PHI) when authorization is required and when it is not required. To understand that a patient has the right to revoke the authorization at any time and that WACBD will not withhold or alter treatment based on lack or change of an authorization under this policy.

SCOPE: The scope of this policy applies to all WACBD staff and patients.

POLICY STATEMENT: It is the policy of WACBD to be within compliance with all federal and state regulations regarding the use and disclosure of PHI and to allow disclosure of patient PHI without a patient authorization only for the purposes of treatment, payment and healthcare operations or as otherwise allowed by the Privacy Regulations or under other state and federal law.

DEFINITIONS:

Term	Definition
Authorization	Permission obtained from a patient or health plan member that permits a covered entity or business associate to use or disclose PHI to an individual/entity.
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI, under HIPAA (Health Insurance Portability and Accountability Act), is any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA covered entity, a healthcare provider, health plan or health insurer, or a healthcare clearinghouse, or a business associate of a HIPAA covered entity, in relation to the provision of past, present, or future healthcare or payment for healthcare services.

PROCEDURES:

Procedure 1- Understanding When Authorization is Required	

Authorization Required	Authorizations are required for the following uses and disclosures:
	• Use and disclosure of psychotherapy notes for any purpose
	• Health care operations activities, including:
	  ○ Fundraising (if more than limited information is used/disclosed)
	  ○ Marketing (under most situations when direct or indirect payment is received)
	  ○ Release to the media or public display
	• Certain activities including:
	  ○ about individuals who have been deceased for less than 50 years
	  ○ research (under certain conditions, particularly when individuals directly participate)
	• Any purpose not explicitly exempted from authorization.
	• Some use and disclosure purposes also have specific individual requirements. Authorizations are not to be used to circumvent prohibited uses and disclosures, such as for the sale of PHI.

Authorization Not Required	Authorizations are not required for the following uses and disclosures:
	• To the individual or personal representative
	• For treatment
	• For payment
	• For health care operations activities, including:
	  ○ Fundraising (if only limited information is used/disclosed)
	  ○ Marketing (under limited situations)
	  ○ Summary Health Information to Plan Sponsor
	  ○ Enrollment/Disenrollment information to Plan Sponsors
	• For facility directories
	• To family members, friends, and others an individual involves in his or her health care or payment for health care
	• For emergencies and disaster relief situations
	• For public interest activities including:
	  ○ required by law
	  ○ public health
	  ○ victims of abuse
	  ○ health care oversight
	  ○ judicial and administrative proceedings,
	  ○ law enforcement,
	  ○ about individuals who have been deceased for over 50 years
	  ○ cadaveric organ, eye, or tissue donation purposes

	○ research (under certain conditions) averts serious threat to health or safety ○ specialized government functions ○ workers compensation • For limited data set • To HHS for compliance and enforcement activities • All other uses and disclosures require an authorization unless other state or federal law mandates the specific use or disclosure.

Procedure 2- Authorizations for Release to/ from a Third Party	
Authorization for Release to a Third Party	If WACBD receives a request from a third party for release of PHI for other than treatment, payment, healthcare operations or as otherwise authorized by law or for public interest purposes exempted from authorization, the request will be routed to clinical admin and/or other authorized clinician. 1. The clinical admin and/or other authorized clinician will review the request and if needed can seek assistance of a supervisor/ acting supervisor to determine if specific authorization is required. 2. If specific authorization is required, clinical admin and/or other authorized clinician will contact the patient, plan member or authorized representative in a written letter explaining the nature of the request for release and send the appropriate authorization form with the letter. 3. If authorization is granted, the clinical admin and/or other authorized clinician will notify the third party requesting the information that authorization has been granted and will include requested information with the letter. 4. If the patient, plan member or authorized personal representative denies release, the clinical admin and/or other authorized clinician will notify the third party requesting the information that authorization has been denied by the patient, plan member or authorized personal representative. Notification will be in writing. 5. All letters and acknowledgement forms shall be recorded in the patient's electronic medical record. 6. All Privacy concerns will be directed to the Privacy Officer
WACBD's Request for Third Party Release of Information	If WACBD requires access to third party PHI for purposes other than treatment, payment, healthcare operations, as allowed by law or for public interest purposes exempted from authorization, the WACBD team member will first document the need and purpose for release. 1. The appropriate authorization form will be mailed or transmitted to the third party specifying in as much detail as possible the PHI requested accompanied by a letter specifying the reason for the release of PHI. 2. WACBD's team member will follow up by phone with the third party if no response has been received within two weeks from the date of the request. The phone call will be documented and become a part of the patient's electronic medical record.

	3. If the authorization is granted and the PHI is forwarded to WACBD, the released PHI shall only be used for the purposes documented. The authorization form received from the third party shall become part of the patient electronic medical record. 4. If the authorization is denied, the request will be forwarded to the appropriate WACBD team member, for review and determine if WACBD intends to contact the specific patient or authorized individual to directly request authorization. 5. If it is determined the PHI requested is critical, the WACBD team member will contact the patient or authorized individual in writing detailing the information requested and the reason for the release of PHI. The letter will be accompanied with the appropriate authorization form. 6. If authorization is granted, the WACBD team member, the third party will be contacted in writing. The letter to the third party shall be accompanied by a copy of the completed authorization request. 7. If the authorization is denied, all documentation will become part of the patient's electronic medical record and WACBD will be required to take appropriate action depending on the situation. This could include doing nothing, proceeding with the activity the information is to be released for without the requested PHI or, if the purpose of release is directly related to legal action, pursue obtaining a subpoena demanding release of specified information.
WACBD's Request for Individual Authorization to Release Information	If WACBD requires access to an individual's PHI for purposes other than treatment, payment, healthcare operations, as allowed by law or for public interest purposes exempted from authorization, the workforce member will first document the need and purpose for release. 1. The appropriate authorization form will be mailed or transmitted to the individual specifying in as much detail as possible the PHI requested accompanied by a letter specifying the reason for the release of PHI. 2. WACBD's authorized team member will follow up by phone with the individual if no response has been received within two weeks from the date of the request. The phone call will be documented and become a part of the patient's electronic medical record. 3. If the authorization is granted, WACBD shall only use the PHI requested for the purposes documented. The authorization form received from the individual shall become part of the patient's electronic medical record. 4. If the authorization is denied, the response will be forwarded to the original requester and this response will be recorded in the patient's electronic medical record. No further action to obtain or use the information will be made by WACBD.
Individual Authorization to Release Information	An individual can request WACBD to release his/her own PHI to a third party for any purpose at any time. The individual must complete an authorization for this release, and WACBD must, in almost all cases, honor the request. 1. The individual must complete the appropriate authorization form specifying in as much detail as possible the PHI requested. No reason for the release is

	required. 2. Any PHI release authorized by the individual must be granted. WACBD's clinical admin will send the PHI directly to the third party upon individual request. A letter to the third party shall be accompanied by the PHI and a copy of the completed authorization request. The authorization and response letter will be documented and become a part of the patient's electronic medical record.

Procedure 3 Understanding WACBD's Authorization Responsibilities	
Authorizations	WACBD must obtain a valid authorization for certain uses and disclosures and has adopted specific authorization forms for use when releasing or requesting PHI for purposes that require authorizations. For disclosures made in response to a valid authorization, WACBD will disclose the information to the extent specified in the authorization. When requesting PHI that requires an authorization to use/disclose, WACD will request the minimum amount of information needed to meet the purpose of the request. • WACBD may use and disclose PHI when a valid authorization is obtained. • Requests for authorization initiated by WACBD, all patients must use WACBD's ROI form (Appendix 2). All sections must be complete. • Changes or variations to the authorization forms must be approved by WACBD's Privacy Officer. Treatment may not be conditioned on obtaining the authorization (unless related to approved research clinical trial).
Authorization Received from an Individual or Third Party	If the authorization was received from the individual or third party, determine the validity of the authorization. The following elements must be present: • A description of the specific information to be used or disclosed. • Name of the specific person or entity authorized to disclose the information. • Name of the specific person or entity to whom WACBD may make the requested use or disclosure and, if information is to be mailed, the address of the person or entity. • The date, event, or condition upon which the authorization will expire. • The individual's signature and date. • A description of the personal legal representative's authority to sign, if applicable. • A description of the purpose of the disclosure. (Not required if the individual requests disclosure for own use). • A statement in which the individual acknowledges that he or she has the right to revoke the authorization, instructions on how to exercise such right, or to the extent the information is included in WACBD's notice, a reference to the notice. • A statement that treatment may not be conditioned on obtaining the authorization, unless it is research related and disclosure of the

	information is for the particular research study. If for purposes of research, where treatment may be conditioned on obtaining the authorization, a statement about the consequences of refusing to sign the authorization. • A statement in which the individual acknowledges that information used or disclosed to any entity other than a health plan or health care provider may no longer be protected by federal privacy law. • If the authorization is for marketing purposes and the marketing is expected to result in direct or indirect remuneration to WACBD from a third party, a statement of this fact. • If the disclosure requested involves mental health, substance abuse, HIV/AIDs, or reproductive health information, following chapter 70.02 RCW, the authorization must have authorization from the patient to release such information.
Invalid Authorizations	An authorization is not considered valid if it has any of the following defects: • The expiration date has passed. • The form has not been filled out completely. • The authorization is known by WACBD to have been revoked • The form lacks any required element. • The information on the form is known by WACBD to be false. • Treatment was conditioned upon obtaining the authorization.
Legal Representatives	If the authorization is signed by a legal representative or other person authorized to act for the individual, the request must be accompanied by documentation of the representative's legal authority to act on behalf of the individual.
Revocation of Authorization	A patient who has executed an authorization for disclosure or use of individual health information may revoke the authorization at any time by sending a written notice to WACBD. • The written notice must refer to the specific authorization being revoked (e.g., "my authorization of January 27, 2002") and be signed and dated by the individual or his or her legal representative. • The revocation becomes effective upon receipt by WACBD, with the exception of uses or disclosures made by WACBD prior to receipt.
For Research-Related Health Information	The core elements of an authorization as described below, may be combined with the informed consent to participate in the clinical research activities: • An authorization for a research study may be combined with another authorization or other written permission for the same or another research study. • WACBD may condition the provision of research related treatment (related to the clinical trial) on obtaining authorization. • WACBD may use and disclose for a specific research study, PHI that is created or received before and after HIPAA's compliance date (April 14, 2003), and/or prior to the new authorizations being implemented, as long as some other express legal permission to use and disclose the information for

	the research study was obtained. • Archived information may continue to be used and disclosed for the research study if an individual had originally signed an informed consent to participate in the research study, or IRB waived informed consent, in accordance with the Common Rule or FDA's human subject protection regulations. • An accounting of all disclosures made under an authorization must be documented and maintained. [See WACBD's Accounting of Disclosures of Health Information]

RELEVANT REFERENCES:

- https://www.hca.wa.gov/assets/billers-and-providers/60-0015-sharing-substance-use-disorder-information-guide.pdf
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- RCW 70.02

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Breach Notification Policy	**Department:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 07/01/2022	**Effective Date:** 08/03/2022	**Next Review Date:** 08/03/2025
Policy Contact: Privacy Officer	**Version:** #1	
Written By: Savannah Simmons, Savannah.simmons@wacbd.org		

PURPOSE: The purpose of this policy is to address the regulatory requirements surrounding breach notification and how a covered entity should report the breach under HIPAA. It is the responsibility of WACBD to prevent, protect against, and respond to privacy incidents and breaches involving Personally Identifiable Information (PII)/ Protected Health Information (PHI) that we maintain.

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

SCOPE: The scope of this policy applies to all WACBD patients and staff.

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) will train staff on Breach Notifications to ensure the proper channels are taken to notify the appropriate parties if a breach of PHI occurs. WACBD will notify the appropriate parties within the allotted timeframe and without unreasonable delay.

DEFINITIONS:

Term	Definition
Breach	An unauthorized acquisition, access, use, disclosure of unsecured PHI in a manner not permitted by the HIPAA Privacy Rule that compromises the PHI. Breach excludes: • The unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. • The inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. • If the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.
Healthcare Insurance	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US

Portability and Accountability Act (HIPAA)	Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Privacy Incident	Any event that has resulted in (or could result in) unauthorized use or disclosure of PII/PHI where persons other than authorized users have access (or potential access) to PII/PHI or use it for an unauthorized purpose.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Unsecured PHI	PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology such as encryption or destruction

PROCEDURES:

Procedure 1- Breach Discovery	
Breach Discovery	A breach is treated as "discovered" when a staff member, Business Associate (BA), or person becomes aware of such disclosure. Staff members who believe that a breach has occurred must immediately notify their supervisor and WACBD's Privacy Officer.

Procedure 2- Breach Investigation/ Risk Assessment	
Investigation	Immediately following the discovery, the privacy officer and the department director will conduct an investigation into the breach. Both the privacy officer and the department director will work together to begin the investigation while collaborating with other staff as appropriate to gain total knowledge of the breach.
Risk Assessment	During the investigation, a risk assessment should be done by the Privacy Officer and/or the BA to demonstrate that there is a low probability that the PHI has been compromised with at least the following factors: 1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification. 2. The unauthorized person who used the protected health information or to whom the disclosure was made. 3. Whether the protected health information was actually acquired or viewed. 4. The extent to which the risk to the protected health information has been mitigated. WACBD/ BAs have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

Procedure 3- Notification	
Breach Notification	When a PHI breach occurs, the HIPAA Breach Notification Rule requires covered entities to notify affected individuals, HHS, and, in some cases, the media. Generally, a breach is an unpermitted use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. Notifications are made as soon as possible, without unreasonable delay and in no case

	later than 60 calendar days after the breach discovery date. The notification may be delayed if the covered entity or BA contacts a law enforcement agency after discovery of a breach of the security of the system and a law enforcement agency determines that the notification will impede a criminal investigation. The notification shall be made after the law enforcement agency determines that it will not compromise the investigation. The notification must include, to the extent possible: • The name and contact information for the covered entity (or business associate, as applicable) • Brief description of the breach in plain language • Description of the types of information that were involved in the breach • A time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach • Steps affected individuals should take to protect themselves from potential harm • Brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches • The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed personal information
Individual Notice	WACBD must notify individuals whose PHI was breached. This individual notice must be done in written form by first class mail or alternatively by email if the affected individual has agreed to electronic communications. If there are insufficient or out-of-date contact information for 10 or more individuals, WACBD must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. Including a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If there are insufficient or out-of-date contact information for fewer than 10 individuals, WACBD may provide substitute notice by an alternative form of written notice, by telephone, or other means.
Media Notice	If a breach occurs that affects more than 500 residents of a state or jurisdiction, in addition to notifying individuals, covered entities are required to provide notice to prominent media outlets serving that state or jurisdiction. This can be done through a press release. This is to be done no later than 60 days after the date of discovery.
Notice to the Secretary	When notifying individuals, the media (if applicable), covered entities must also notify the Secretary of breaches through the HHS webpage: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true • If a breach affects 500 or more individuals, covered entities must notify the Secretary no later than 60 days following the date of discovery. • If a breach affects less than 500 individuals, covered entities must notify the Secretary on an annual basis no later than 60 days following the end of the

	calendar year.
Business Associate Notifications	The Breach Notification Rule also requires business associates to notify a covered entity of breaches at or by the business associate While the Business Associate is ultimately responsible for ensuring individuals are notified, if the breach occurs at their level, the covered entity may delegate the responsibility of providing individual notices for continuity of care. (Example: the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual).

Procedure 4- Administrative Burden of Proof	
Administrative Requirements and Burden of Proof	WACBD and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. With respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: 1. Its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or 2. The application of any other exceptions to the definition of "breach." WACBD, as a covered entity, is required to comply with administrative requirements with respect to breach notifications. WACBD has done the following: • Written policies and procedures regarding breach notifications • Trained employees on these policies and procedures • Developed appropriate sanctions against workforce members who do not comply with these policies and procedures • Created a workflow that the Privacy Officer and Compliance Committee follow when a breach occurs.

RELEVANT REFERENCES:

- Breach Notification Rule | HHS.gov

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Business Associate Contracts and Other Arrangements	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 06/01/2022	**Effective Date:** 07/06/2022	**Next Review Date:** 07/06/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: In accordance with federal law, the purpose of this policy is for all Washington Center for Bleeding Disorders (WACBD) employees to understand they must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of PHI data.

The Business Associate Agreement requires covered entities to obtain assurances from business associates that they will appropriately safeguard PHI in any form as required by the HIPAA Regulations [45 CFR 164.314].

The Washington Center for Bleeding Disorders, as a covered entity under the Health Insurance Portability and Accountability Act (HIPAA) is required to ensure that any Business Associate with whom it shares protected health information (PHI) handles that information in accordance with federal and state laws and regulations, including but not limited to HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH).

SCOPE: The scope of this policy applies to all WACBD workforce members (Covered entity) and its Business Associates.

POLICY STATEMENT: It is the policy of WACBD to ensure confidentiality, integrity, and availability of PHI and ePHI. WACBD will accomplish this by permitting a business associate to create, receive, maintain, or transmit PHI and/or ePHI on its behalf under a written agreement between WACBD and the business associate. This policy reflects WACBD's commitment to comply with such regulations.

DEFINITIONS:

Term	Definition
American Recovery and Reinvestment Act (AARA)	The American Recovery and Reinvestment Act of 2009 (ARRA) makes a number of modifications to the Health Insurance Portability and Accountability Act (HIPAA) regarding privacy and security rules. ARRA specifies that any entity that engages in health information exchanges or provides data transmission of PHI is considered a Business Associate. As such, these entities must enter into a business associate contract with the covered entity and will be subject to ARRA's civil and criminal penalty provisions.
Authorization	Permission obtained from a patient or health plan member that permits a covered entity or business associate to use or disclose PHI to an individual/entity.
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. BA is also a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.

Covered Entity (CE)	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Health Information Technology for Economic and Clinical Health Act (HITECH)	The HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009 is legislation that was created to stimulate the adoption of electronic health records (EHR) and the supporting technology in the United States. It is a part of the American Recovery and Reinvestment Act of 2009 (ARRA). Other than stimulating EHR adoption in the United States, the HITECH Act was passed to further expand data breach notifications and the protection of electronic protected health information (ePHI)
Individually Identifiable Health Information (IIHI)	The HIPAA Privacy Rule places restrictions on uses and disclosures of individually identifiable health information. This information, including demographic data, which relates to: -The individual's past, present or future physical or mental health or condition, -The provision of health care to the individual, or -The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number, etc.). HIPPA places restrictions as above, but not on health information that does not allow an individual to be identified.
Protected Health Information (PHI)	Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI, under HIPAA (Health Insurance Portability and Accountability Act), is any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA covered entity, a healthcare provider, health plan or health insurer, or a healthcare clearinghouse, or a business associate of a HIPAA covered entity, in relation to the provision of past, present, or future healthcare or payment for healthcare services.
Vendor	An entity that provides or performs a service on behalf of the organization but does have access to personal health information. For example, a cleaning company providing housekeeping services is a vendor who would not access personal health information.

PROCEDURES:

Procedure 1- Requirements of Business Associates	
Contract Engagement and Requirements – Business Associate Agreement (BAA)	The HIPAA Privacy rules require that all Covered Entities (CE) to have a signed Business Associate Agreement (BAA) with any Business Associate (BA) they hire that may come into contact with PHI. HIPAA requires Covered Entities to only work with Business Associates who ensure complete protection of PHI. The assurances must be in writing in the form of a contract/ agreement. The BAA must include the following minimum elements: • Describe the permitted and required PHI use by the BAA • Ensure that the BA will not use or further disclose PHI other than as permitted or required by the contract or as required by federal and/or state law. • Require the BA to use appropriate safeguards to prevent inappropriate use or disclosure of PHI. • Require the BA to report to the CE any breaches and/or unauthorized uses/disclosures of PHI
Accounting of Disclosures Regarding BAA	Business Associates/Vendors shall record any disclosures of a patient's PHI. Disclosures will be recorded as agreed upon within the BAA. It is the responsibility of the disclosing party to log the disclosure. Business Associates/Vendors must also be prepared to produce an access report of electronic disclosures upon request.
Patient Rights	Business Associates/Vendors will perform the following listed actions upon the request of WACBD in support of HIPAA Privacy Rule granted patient rights. • Make available PHI stored by Business Associates/Vendors to covered entities upon request in accordance with the patient's right of access his/her medical record. • Make available to WACBD, a list of any disclosures of patient information stored in the accounting of disclosures repository, or an access report retrievable from system audit logs. • Incorporate any amendments to PHI stored by Business Associates/Vendors in accordance with a patient's right to request an amendment to his/her medical record and as authorized by WACBD. • Make its internal practices, books, and records relating to the use and disclosure of PHI received from; or received, created, used or disclosed by the business associate on behalf of Physician available to the Secretary of the U.S. Department of Health and Human Services, Office of Civil Rights for purposes of investigating patient privacy complaints. • Adopt alternative means of communicating with the patient as authorized WACBD (only if Business Associate/Vendor communicates directly with the patient). • Restrict access or disclosure of patient information to certain individuals or the disclosure of certain information included in the patient's record as

	authorized by WACBD. • Ensure that patients' rights are executed under all applicable federal and state laws and regulations
Breach of PHI	Business Associates/Vendors shall notify WACBD immediately following the discovery of any security breach resulting in the inappropriate release of unencrypted patient PHI. Following the terms of the BAA, the responsible party shall provide appropriate notification to all affected parties/individuals. If Business Associate/Vendor is deemed the notifying entity (versus WACBD), the Business Associate/Vendor will notify affected individuals in a timely manner based on guidelines mandated by federal and state regulations. Covered Entities, such as WACBD, are not required to monitor or oversee the actions of its Business Associates nor are they liable for those actions. However, if WACBD is aware of patterns of activity or negligent practices by the Business Associate, and it constitutes a material breach or violation under the BAA, WACBD will terminate the contract/ agreement if feasible

Procedure 2- ARRA Requirements	

AARA Requirements	• Business Associates must independently comply with all provisions of the Title XIII of the American Recovery and Reinvestment Act of 2009 and its implementing regulations ("ARRA"). HIPAA security rule (45 CFR 164.302 through 164.318)
	• Business Associates must independently comply with certain provisions of the HIPAA privacy rule (45 CFR 162.502, 162.504)
	  ○ Use and disclosure of protected health information (PHI), general requirements
	  ○ Use and disclosure of PHI, organizational requirements
	• Business Associates are subject to civil and criminal penalties for violation of the HIPAA security rule and certain provisions of the HIPAA privacy rule
	• Creation of new categories of business associates including:
	  ○ Health Information Exchange Organizations
	  ○ Regional Health Information Organizations
	  ○ E-prescribing Gateways
	  ○ Vendors who contract with covered entities to provide a PHR to the covered entities' patients or health plan members
	• Covered entities are required to amend existing business associate contracts/agreements to reflect the change requiring business associates to comply with the HIPAA security rule and certain provisions of the HIPAA privacy rule
	• Covered entities are required to enter into business associate relationships with the new categories of business associates
	• Business associates are required to appropriately investigate and notify covered entities of any breaches.
	  ○ This includes providing WACBD with specific information about the breach and the individuals involved. It is the responsibility of

	WACBD to notify affected individuals.
Compliance with Anti-Kickback Laws	BA shall not take any actions that would violate (i) state or federal anti-kickback laws, including, without limitation, those provided for in Section 1128B of the SSA (42 U.S.C. 1320a-7b), and (ii) the HIPAA of 1996 and its implementing regulations (45 CFR Parts 160 and 164) and standards related to Individually Identifiable Health Information (the "Privacy Rule").

Procedure 3- Responsibility of WACBD	
Obtaining a BAA	For the continuity of business operations in regard to payor contracts, pharmacy operations, and research operations, BAAs may be obtained and negotiated with those department heads and the BA. For all other business or questions related to BAAs, please contact the Privacy Officer and/or Compliance Coordinator.

RELEVANT REFERENCES:

- ARRA § 13402, 42 U.S.C.A. § 17932
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, Privacy Rule Introduction | HHS.gov
- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS
- NIST SP 800-12, An Introduction to Computer Security and Chapters 10 and 14.
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-66 Rev. 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule, http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- Office of Civil Rights (OCR), Sample Business Associate Agreement Provisions http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- International Standards Organization (ISO/IEC 17799:2000(E))
- RCW 70.02

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Complaint Process for Privacy Concerns	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 06/09/2022	**Effective Date:** 8/24/2022	**Next Review Date:** 8/24/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to give information on the internal process on patient compliant process and options under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Including the right to file a complaint with Washington Center for Bleeding Disorders (WACBD) privacy officer or directly to Office of Civil Rights (OCR) if there is suspected noncompliance with Privacy/ Security Provisions of HIPAA. Patients may also file a complaint with Centers for Medicare & Medicaid Services (CMS) for any noncompliance with the non-privacy/ security provisions of HIPAA.

All WACBD patients must be allowed to file a complaint if they think their privacy rights have been violated. The process for both shall be clearly defined in the notice of privacy practices provided to the patient. (Appendix 1) Complaints will be handled expeditiously if received by the privacy officer. If a complaint is filed with OCR, WACBD shall comply with all OCR requests for information in an effort to expeditiously address the complaint. More information on how/ where patients file a complaint, see the notice of privacy practices.

SCOPE: The scope of this policy applies to all WACBD patients and staff

POLICY STATEMENT: WACBD will provide guidance regarding patients and authorized representatives' rights to file a complaint with WACBD or with the US Department of Health & Human Services (HHS) Office of Civil Rights (OCR) regarding HIPAA Privacy and/or Security concerns.

DEFINITIONS:

Term	Definition
Business Associate	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to a covered entity
Complaint	An individual who believes that a patient's protected health information has been improperly used or disclosed
Privacy Officer	Oversees and investigates all ongoing activities related to the development, implementation, and maintenance of the organization's Privacy Policies and Procedures in accordance with applicable federal and state laws
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1– Privacy Complaint Investigation	
Privacy Officer	All complaints received by the privacy officer need to be thoroughly investigated. This may include a phone or in-person interview with the patient. The privacy officer

	will conduct the investigation or refer the investigation to the appropriate party.

Investigation	• The privacy officer will review any complaints received to determine the events that resulted in a complaint being filed, the departments involved and the scope of the investigation to be completed.
	• If the complaint is related to activities performed by a business associate of WACBD, the privacy official shall include the business associate activity as part of the complaint investigation process.
	• If the complaint resulted from the actions of a third party not affiliated with WACBD, the privacy officer will inform the patient in writing that the complaint will need to be filed with the third party not affiliated with WACBD.
	• The privacy officer or designated representative shall conduct an investigation to determine if any policies, procedures, or practices were violated and the nature of the violation (intentional or inadvertent).
	• If the privacy officer finds no violation of privacy occurred, the privacy officer shall inform the patient in writing of his/her findings.
	• If the privacy officer finds that a privacy breach occurred but no violation of current policies, procedures, or practices occurred, the privacy officer will work with the appropriate department to amend policies, procedures, and practices to prevent such breaches in the future. The privacy officer shall also notify the patient of his/her findings and what remediation action has been taken.
	• If the privacy officer finds that a violation of WACBD's policy, procedure and practice occurred, the privacy officer shall work with the appropriate department or business associate and human resources (if not a violation by a business associate). Appropriate sanctions will be initiated and documented.
	  ○ The privacy officer shall inform the patient of findings and actions taken.
	• If the incident involved a business associate, the privacy officer shall contact the business associate and require the business associate to conduct an investigation, resolve the privacy breach and provide a report to WACBD. This will be communicated to the patient.
	  ○ If the business associate is unwilling or unable to correct activities that resulted in the breach, WACBD shall sever the contract with the business associate.
	  ○ A second notification of actions taken by the business associate should be provided to the patient.
	• All notifications to the patient, regardless of findings or actions, must include notification to the patient of the right to file a complaint with the OCR.
	• All documentation from the complaint investigation process shall be retained

	with the patient record.

Procedure 2- HIPAA Complaints Filed Outside of WACBD	
Complaints Filed with OCR	• If a formal complaint is filed with OCR, OCR will verify the complaint is valid and within their jurisdiction. If the compliant is valid, OCR must notify WACBD of the complaint. Once a notice is received by WACBD, it will be forwarded to the privacy officer immediately. • The privacy officer and appropriate members of the workforce will fully comply with any OCR requests for information during the investigation process. • Privacy Officer, in conjunction with the compliance committee, will review any findings from the investigation and take appropriate action. Appropriate action may include complying with OCR informal requests for a change in policies, procedures, and practices; sanctioning a workforce member; working with a business associate to address any actions on the part of the business associate to address the breach (including possible termination of the contract between WACBD and the business associate if the business associate is unable or unwilling to take action). • Any needed action on the part of WACBD to mitigate damages and address the cause of the breach shall be addressed immediately. • OCR will notify the patient or plan member regarding the outcome of the investigation and any remediation action taken on the part of WACBD or WACBD's business associate. • If informal cooperation with OCR does not satisfy, OCR and WACBD receives a notice of proposed penalties. WACBD will consult with legal counsel to determine if WACBD intends to request a hearing and follow the formal appeal process outlined in the HIPAA Enforcement Rule. WACBD may elect to involved legal counsel earlier in the process if deemed necessary. • All documentation from the complaint investigation process shall be retained within the EMR system.
Centers for Medicare & Medicaid Services (CMS)	• CMS allows for multi-factor authentication HIPAA complaint reporting o To file a complaint on HIPAA transactions, code sets, unique identifiers (employer and provider Identifiers) or operating rules electronically: https://asett.cms.gov/

RELEVANT REFERENCES:

- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.

- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Enforcements/FileaComplaint
- WACBD Grievance Policy
- WACBD Notice of Privacy Practices

APPROVING COMMITTEE(S):
Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

De-Identified Information & Limited Data Sets	**Department:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 07/03/2022	**Effective Date:** 8/24/2022	**Next Review Date:** 8/22/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to outline what de-identified data is and how its created, what limited data sets and data use agreements are, and what Washington Center for Bleeding Disorders (WACBD) compliance obligations are.

The American Recovery and Reinvestment Act of 2009 (ARRA) requires HHS to issue guidance on methods for de-identification of protected health information (PHI) as designated in HIPAA's Privacy Rule. Under Section 164.514(a) of the HIPAA Privacy Rule, the standards for de-identification of protected health information are outlined, including, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual

SCOPE: The scope of this policy applies to all WACBD patients and staff

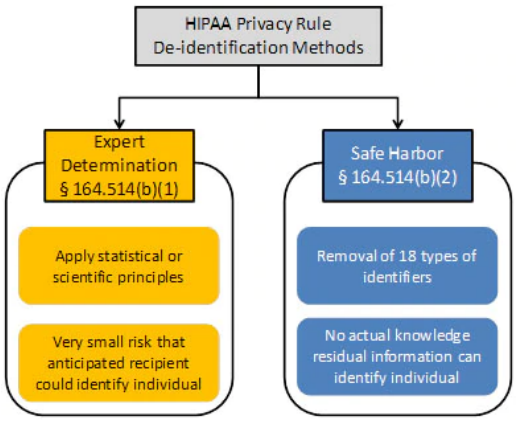
POLICY STATEMENT: WACBD will abide by HIPAA requirements on limited data sets including when to de-identify protected health information. WACBD's Privacy Officer will oversee patient requests on limited data sets and will report any wrongdoing to HHS as required.

DEFINITIONS:

Term	Definition
Data Use Agreement (DUA)	Establishes who is permitted to use and receive the (limited data set) LDS, and the permitted uses and disclosures of such information by the recipient, and provides that the recipient will: • not use or disclose the information other than as permitted by the DUA or as otherwise required by law, • use appropriate safeguards to prevent uses or disclosures of the information that are inconsistent with the DUA, • report to the covered entity uses or disclosures that are in violation of the DUA, of which it becomes aware • ensure that any agents to whom it provides the LDS agree to the same restrictions and conditions that apply to the LDS recipient, with respect to such information, and • not re-identify the information or contact the individual.
De-Identified Data	De-identification of PHI ensures that personal information cannot be tied to a specific patient. De-identification is achieved by removing certain data points that can be tied to a particular individual.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Limited Data Set	A limited set of identifiable patient information (See Procedure 2)

(LDS)	
Privacy Rule	The part of the HIPAA rule that addresses the saving, accessing, and sharing of medical and personal information of an individual, including a patient's own right to access
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- Creating De-Identified Data	
Creating De-Identified Data	There are two acceptable methods for creating de-identified information that is no longer governed by the HIPAA privacy rules: • The safe harbor method • The expert determination method  Provided by HHS at (https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard)
Safe Harbor Method	The safe harbor method for creating de-identified health information requires the removal of the following person identifiers prior to use and disclosure: 1. Name 2. All geographical subdivisions smaller than a state a. Address b. City c. County d. Zip code (including equivalent geocodes) 3. Names of relatives and employers 4. Birth date, date of death 5. Admission and discharge dates 6. Telephone and fax numbers 7. E-mail addresses 8. Social security number 9. Medical record number 10. Health plan beneficiary number 11. Account number (organization and health plan account numbers)

	12. Certificate/license number 13. Vehicle or other device serial number (including license plate number) 14. Web URL 15. Internet Protocol (IP) address 16. Finger or voice prints 17. Photographic images 18. Any other unique identifying number, characteristic, or code • Age and some geographic location information may be included in the de-identified information, but all dates directly related to the subject of the information must be removed or limited to the year, and zip codes must be removed or aggregated (in the form of most 3-digit zip codes) to include at least 20,000 people. • Ages of 90 and over must be aggregated to a category of 90+ to avoid the risk of re-identification. Other demographic information, such as gender, race, ethnicity, and marital status are not included in the list of identifiers that must be removed. • Codes and similar means of marking records may be used so they may be linked or later re-identified but only by WACBD as long as the code does not contain information about the subject of the information (for example, the code may not be a derivative of the individual's social security number), and the code is not used or disclosed for any other purpose. • WACBD cannot disclose the mechanism for re-identification, such as tables, algorithms, or other tools that could be used to link the code with the subject of the information.
Expert Determination Method	Expert determination method requires a statistical expert, using generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, to: 1. Determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, to identify an individual(s); and 2. Documents the results for justification.

Procedure 2- Understanding Limited Data Sets and Data Use Agreements	
Limited Data Set	A limited data set is protected health information (PHI) that excludes all the following direct identifiers of the individual or of relatives, employers or household members of the individual: 1. Names 2. Postal address information, other than town or city, state, Zip code 3. Telephone numbers 4. Fax numbers 5. Electronic mail addresses 6. Social security numbers

	7. Medical record numbers 8. Health plan beneficiary numbers 9. Account numbers 10. Certificate/license numbers 11. Vehicle identifiers and serial numbers, including license plate numbers 12. Device identifiers and serial numbers 13. Web Universal Resource Locators (URLs) 14. Internet Protocol (IP) address numbers 15. Biometric identifiers, including finger and voice prints 16. Full face photographic images and any comparable images The health information that <u>may remain</u> in the data set includes: 1. Dates, such as admission, discharge, service, date of birth, date of death 2. City, state five digit or more zip code 3. Ages in years, months or days or hours • WACBD may use or disclose a limited data set if WACBD enters into a data use agreement with the recipient of limited data set and if the purpose of the use or disclosure is for research, public health, or health care operations. • WACBD may use or disclose PHI to create a limited data set or to disclose to a business associate for such purpose, whether or not the limited data set is to be used by WACBD. • WACBD is not required to account for the disclosures of PHI contained in a limited data set.
Data Use Agreement	WACBD may use or disclose a limited data set only if WACBD has a signed data use agreement that the limited data set recipient will only use or disclose the PHI for limited, designated purposes. (See Appendix 3) A data use agreement between WACBD and the limited data set recipient must: 1. Limit the permitted uses and disclosures of such information by the limited data set recipient to the purposes of research, public health, health care operations or to create a limited data set 2. Prohibit the limited data set recipient from using or further disclosing the information in a manner that would violate HIPAA if such use or disclosure were done by WACBD 3. Establish who is permitted to use or receive the limited data set 4. Provide that the limited data set recipient will: a. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement c. Report to WACBD any use or disclosure of the information not provided for by its data use agreement of which it becomes aware

	d. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information e. Not identify the information or contact the individuals

Procedure 3- Compliance	
Reporting to HHS	If WACBD knows the limited data set recipient is in material breach or violation of the data use agreement, WACBD must report this breach immediately to Compliance and the Privacy Officer to take reasonable steps to cure the breach or end the violation, as applicable. If WACBD is unable to cure the breach or end the violation, WACBD must discontinue disclosure of PHI to the recipient and report the problem to the US Department of Health and Human Services (HHS).
Compliance	• Any requests for de-identified information or a limited data set needs to be approved by the Privacy Officer or Compliance Committee prior to any release. • Any requests for a limited data set require the execution of a limited data set data use agreement. • All data use agreements, following approval and execution shall be forwarded to the Privacy Officer who shall maintain copies for a minimum of ten years. • Following approval of release of de-identified data or use and disclosure of a limited data set, de-identified data created by the expert statistical method shall be forwarded to the contracted IT department if appropriate. • Any coding mechanisms used to later re-identify data shared shall be retained internally and will be secured by the contracted IT department. Access shall be limited to appropriate IT members, the Privacy Officer and appropriately designated members of WACBD's workforce. • The Privacy Officer or Compliance Committee shall be responsible for periodic monitoring of use of limited data sets by designated recipients to reasonably ensure the privacy of the data and that such data is only used for research, public health, or health care operations. • Any discovered or reported breaches will be investigated and the designated recipient(s) who previously had entered into a data use agreement is fully responsible for mitigation of damages and shall report mitigation activities to the Privacy Officer. • If the designated recipient(s) is unable or unwilling to cure any noted breaches, the data use agreement shall be terminated, and the breach reported to the Office of Civil Rights (OCR). • Documentation related to the breach, mitigation activity and any reports to

	OCR shall be retained for a minimum of ten years.

RELEVANT REFERENCES:

- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Document Retention Requirements	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 07/20/2022	**Effective Date:** 09/21/2022	**Next Review Date:** 09/21/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance to Washington Center for Bleeding Disorders (WACBD) regarding the appropriate retention and disposal of privacy-related documents containing protected health information (PHI) created, obtained or in the possession of WACBD related to the activities of the Privacy Officer, designees of the Privacy Officer or WACBD's activities related to privacy matters and HIPAA privacy compliance.

SCOPE: The scope of this policy applies to all WACBD patients and staff

POLICY STATEMENT: WACBD will maintain records in compliance with the federal Privacy Rule and Washington State laws in such a manner that the records are:

1. available to any government authority or agency (e.g., CMS, HHS, the OIG, the OCR, or WA State Agency) for the purpose of review or to assist with a complaint or compliance investigation or audit;
2. retained for the mandated time period as required to comply with the HIPAA rules,
3. available to provide upon request as required to be disclosed to a patient

It is the policy of WACBD to retain its records for the periods provided by in the strictest of controlling regulation and must be readily accessible in a reasonable time period. Under Washington State Law, the retention period is ten years following the most recent discharge. Minor's records shall be maintained and preserved for a period of no less than three years following the attainment of the age of eighteen years.

DEFINITIONS:

Term	Definition
Privacy Officer	Oversees and investigates all ongoing activities related to the development, implementation, and maintenance of the organization's Privacy Policies and Procedures in accordance with applicable federal and state laws
Privacy Rule	The part of the HIPAA rule that addresses the saving, accessing, and sharing of medical and personal information of an individual, including a patient's own right to access
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- WACBD Responsibilities	
WACBD Responsibilities	• WACBD shall designate the Privacy Officer/supporting staff member to take an inventory of all privacy related documents (paper and electronic) as needed. • All documents related to privacy as identified in the inventory regardless of format, shall be readily available to respond to any government agency inquiries and potential civil action in accordance with the Federal Rules of

	Civil Procedure. • It is the responsibility of all members of WACBD's workforce to appropriately retain and store documents that have been identified as necessary to retain to meet regulatory and potential civil litigation requirements. • It is the responsibility of the Privacy Officer or designee to regularly audit retention activity to reasonably ensure all documents that are required to be retained are retained in such a way that they are accounted for and readily available if needed. • Inappropriate destruction of documents shall result in appropriate sanctions. • Unless deemed necessary by the Privacy Officer or legal counsel, all documents shall be confidentially destroyed at the end of their required retention period. • The Privacy Officer will reasonably ensure appropriate policies, procedures and practices have been implemented and are followed to reasonably ensure document destruction is done in such a way as to protect the privacy of the information being destroyed. • In the event of a civil or regulatory action involving such records, the document destruction process shall be suspended until such time as the legal or regulatory matter has been resolved. • WACBD has decided to retain records for patients beyond the 10-year statute because these are patients with an inherited condition whose record can inform the care of their descendants. ○ Deceased patient records and patient who have relocated, medical records are marked as "inactive" within the EMR system. • Business Associate Agreements require covered entities to obtain assurances from business associates that they will appropriately safeguard PHI in any form as required by the HIPAA Regulations.

Procedure 2- Documents Subject to HIPAA Records Retention Rules	
Documents Subject to HIPAA Records Retention Rules	Below are documents subject to the HIPAA record retention rules. This only a subset of the extensive list that applies to Covered Entities and their Business Associates but contains the most commonly used documents across the health sector. • Notices of privacy practices • Patient authorizations • Risk assessments and risk analyses • Disaster recovery and contingency plans • Business associate agreements • Information security and privacy policies • Employee Sanction Policies • Incident and breach notification documentation • Complaint and resolution documentation • Physical security maintenance records • Access logs • IT security system reviews (including new procedures or technologies

	implemented)

RELEVANT REFERENCES:

- RCW 70.41.190: Medical records of patients—Retention and preservation. (wa.gov)
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/sites/default/files/introduction.pdf
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Identifying Protected Health Information & Designated Record Sets	**Department:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 07/25/2022	**Effective Date:** 09/21/2022	**Next Review Date:** 09/21/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance to Washington Center for Bleeding Disorders (WACBD) regarding the identification of protected health information (PHI) and determining designated record sets. WACBD defines PHI as individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient. WACBD maintains a list of what identifies as PHI for each department.

SCOPE: The scope of this policy applies to all WACBD staff members

POLICY STATEMENT: To comply with the HIPAA Privacy and Security Rule provisions to safeguard protected health information (PHI), WACBD will define and document what is PHI and any external movement excluding the routine movement in to, out of, and within WACBD that is related to the daily activities of workforce members. This is done to protect the confidentiality, integrity, and availability and minimize the potential for unauthorized access, use or disclosure of PHI under its jurisdiction. It is the policy of WACBD to define and document its designated record sets to support provision of individual privacy rights for patients and plan members.

WACBD holds Business Associates responsible for defining and documenting their designated record sets to support provision of individual privacy rights for WACBD patients [45 CFR 164.314].

DEFINITIONS:

Term	Definition
Designated Record Set	Includes medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals.
Forced Encryption	Forced encryption converts a plain text email into code that is not readable by humans so if it is intercepted it is meaningless. The recipient of the encrypted email simply opens the email and because they are designated recipient their computer will translate the code back to readable plain text.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Privacy Officer	Oversees and investigates all ongoing activities related to the development, implementation, and maintenance of the organization's Privacy Policies and Procedures in accordance with applicable federal and state laws
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient.

PROCEDURES:

Procedure 1- Identifying PHI	
Identifying PHI	PHI includes person identifiers in combination with health information. Information that qualifies as PHI contains any of the specific identifiers below. 1. Name 2. Geographical information smaller than state a. Address b. City c. County d. Zip code (including equivalent geocodes) 3. Names of relatives and employers 4. Birth date, date of death 5. Admission and discharge dates 6. Telephone and fax numbers 7. E-mail addresses 8. Social security number 9. Medical record number 10. Health plan beneficiary number 11. Account number (organization and health plan account numbers) 12. Certificate/license number 13. Vehicle or other device serial number (including license plate number) 14. Web URL 15. Internet Protocol (IP) address 16. Finger or voice prints 17. Photographic images 18. Any other unique identifying number, characteristic, or code PHI also includes genetic information, such as DNA profiles, and any item which may provide DNA, such as tissue samples, used testing equipment, and other biologic materials. PHI does not include employment records held by employers, or records for persons deceased for over 50 years.
PHI Held by WACBD	1. WACBD shall define and maintain a list of all PHI under its jurisdiction. 2. PHI held by WACBD includes: a. All individually identifiable health information b. Health care payment information maintained or transmitted in any medium c. Demographic information collected from an individual, which identifies the individual or can be used to identify the individual 3. WACBD identifies and maintains PHI as required by the board of pharmacy, Washington state, CMS, OCR/ HHS. 4. PHI is held in the departments below as follows: a. Pharmacy- Records in CPR+, Therigy, and NextGen b. Clinic- medical records and communication within NextGen, Patient Portal, lab samples c. Research- records associated with clinical research trials, lab samples d. Billing- all billing records maintained in both pharmacy and EMR

	software management and insurance payor contracts e. Data management- data reports/records in Athn 5. WACBD has a secure list of email domains for organizations frequently emailed, and communication between those domains have forced encryption 6. Privacy Officer shall review all information written, and electronic, oral communications, documents, files, other items and materials that can be tied to specific individuals as needed. 7. If a department supervisor recognizes a privacy concern in regard to PHI, they shall document the movement of PHI under its jurisdiction and will develop and implement procedures to correct the concern such as implementing a PHI flow 8. PHI flow is as follows a) Describes the business processes and the information that flows within and between them by recording the input, transformation, and output of any information involved in those processes. b) PHI flows identify and document all the internal and external entities that send information to or receive information from WACBD's activities and capture how information moves from and to the various WACBD activities to provide a complete picture of the movement of PHI. PHI flows record the who, what, and where of a process.

Procedure 2- Defining Designated Record Sets	
Defining Designated Record Sets	1. WACBD shall define and maintain a designated record set(s) that an individual shall have the right to inspect, copy, and request amendment of his/her protected health information (PHI). 2. A Designated Record Set is a subset of all PHI held by WACBD, and is a group of records maintained by or for WACBD that includes a. The medical records and billing records about the individual(s) maintained by or for WACBD; or b. The enrollment, payment, claims, adjudication, and case or medical management record systems maintained by or for WACBD; or c. Used, in whole or in part, by or for WACBD to make decisions about individuals. 3. Each department shall document the designated record sets that are distributed along with the workforce member responsible, and they shall retrieve and distribute information as needed. A list of records to review is in the table below. 4. If any designated record sets are updated, each department shall notify the WACBD Privacy Officer.

Examples of Items Included/Excluded from Designated Record Sets	Types of Information Often Included in Designated Record Sets	Types of Information Often Excluded from Designated Record Sets
	Clinic records, medical reports and notes, lab test results, X-rays, prescriptions, consult reports, nurse and provider notes	**Reports generated or information provided for quality assurance, auditing, some utilization review, risk management, investigators re: licensure or lawsuits**
	Case management records, status notes, functional assessments, client and family contact notes; meeting notes re treatment options	**Information and reports used for cost management; program development; budget development; grant funding, etc.**
	Mental health and substance abuse evaluations, diagnoses and treatment plans, symptoms, prognosis; mental health professional's psychotherapy notes (although no client access)	**Research information not used to make decisions about a patient**
	Duplicate copies of records in other locations or media or in other designated record sets. (however, client only entitled to access of one copy)	**Information used for public health and health oversight functions, when not used to make individual decisions (i.e. disease registries, outcomes studies, prevention tools, provider fraud and abuse, licensure)**
	Email or written correspondence with clients, other providers, or a payer relating to eligibility, enrollment, payment, a claim, or treatment	
	Copies of reports generated by other providers used to make decisions about the individual	
	Eligibility and enrollment information maintained by Health Plans; records related to third party liability; member contacts/ statements; claims adjudication records	

RELEVANT REFERENCES:

- Privacy Rule Introduction | HHS.gov
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Minimum Necessary	**Department:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 08/11/2022	**Effective Date:** 9/28/2022	**Next Review Date:** 9/28/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance to Washington Center for Bleeding Disorders (WACBD) regarding the requirement to adhere to minimum necessary standards when releasing, accessing, or using Protected Health Information (PHI). Minimum necessary is based on a need-to-know basis which limits the access of PHI with role base access pertaining to a workforce member's job responsibilities.

SCOPE: The scope of this policy applies to all WACBD workforce members.

POLICY STATEMENT: It is the policy of WACBD, and its workforce members to make reasonable efforts in order to limit PHI to the minimum necessary to accomplish the intended purpose when using or disclosing individually identifiable health information (or when requesting individually identifiable health information from other health care providers, health plans and healthcare clearinghouses)

DEFINITIONS:

Term	Definition
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Minimum Necessary Standard	The standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient.
Role-Defined Person	Persons or employees with designated roles and responsibilities as described in his/her job description

PROCEDURES:

Procedure 1- WACBD and Minimum Necessary	
WACBD and Minimum Necessary	Access to PHI shall be limited to the role-defined persons only, and to the identified PHI only, based on WACBD or WACBD's management's reasonable determination of the persons or classes of persons who require PHI, and the nature of the health information they require, consistent with their job responsibilities. 1. WACBD will record and track workforce member access to PHI to reasonably ensure access is limited to the minimum necessary amount of PHI needed to perform their assigned duties

	2. For any type of disclosure that is made on a routine, recurring basis, review of each individual disclosure (to determine the minimum information necessary) is not required. In these situations, WACBD must disclose only the minimum PHI reasonably necessary to achieve the purpose of the disclosure. 3. WACBD will limit access to an entire medical record or claims record and will not allow access except when provided for in the workforce member's job responsibilities. 4. WACBD is required to use and disclose a limited data set of PHI instead of following the minimum necessary standard only in cases where the use and disclosure of the limited data set will satisfy use and disclosure requirements. This does not limit or eliminate any exceptions to the application of minimum necessary requirement upon ARRA enactment or following publication of a definition of "minimum necessary" such as for treatment purposes. 5. Specific disclosures within a type may vary, and WACBD has defined what is typical for the type of disclosure involved. 6. WACBD has developed criteria designed to limit disclosures of PHI to only the minimum amount necessary to accomplish the purpose of the disclosure and applies the criteria to each non-routine disclosure of PHI. a. Policies and procedures for reviewing such requests for disclosures on an individual basis in accordance with these criteria have been developed by WACBD. The member of WACBD's workforce releasing PHI for non-routine reasons must follow established criteria, policies and procedures. (Patient Request for Records Policy) 7. WACBD or a member of WACBD's workforce can request PHI from internal or external health care practitioners or health plans (or clearinghouses) in order to provide treatment and to coordinate or manage healthcare services provided within the minimum necessary standards. 8. WACBD has developed criteria designed to limit requests of PHI to only the minimum amount necessary to accomplish the purpose of the request, and WACBD's workforce must apply the criteria to each non-routine request of PHI.WACBD has established and implemented policies and procedures for reviewing such requests on an individual basis in accordance with these criteria.

Procedure 2- Minimum Necessary Guidelines for Partner Organizations	
Minimum Necessary Guidelines for Partner Organizations	As defined in service agreements, WACBD has limitations in place for its EMR systems and only allows contracted staff and WACBD staff access.

Procedure 3- Exemptions	
Exemptions	Certain types of uses, disclosures and requests of individually identifiable information are not subject to the minimum necessary requirements, and therefore not subject to WACBD's policy and procedure regarding minimum necessary

	1. Requests by or disclosures to health care practitioners for treatment purposes are not subject to the requirements of the minimum necessary standard; 2. Disclosures to the patient who is the subject of the information; 3. Disclosures based on the patient's written authorization; 4. WACBD is not required to apply the minimum necessary standard to the required or situational data elements specified in the implementation guides for HIPAA administrative simplification standard electronic transactions in the Transactions Rule. (The minimum necessary standard does apply for uses or disclosures in standard transactions that are made at WACBD) (https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA) 5. Certain disclosures that are required by law.

RELEVANT REFERENCES:

- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, https://www.ihs.gov/sites/privacyact/themes/responsive2017/display_objects/documents/PvcFR01.pdf
- WACBD's Confidentiality Agreement

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Notice of Privacy Practices	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 8/25/2022	**Effective Date:** 9/28/2022	**Next Review Date:** 9/28/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance regarding the distribution and maintenance of Washington Center for Bleeding Disorders' (WACBD) privacy practices. This includes guidance for direct care providers regarding obtaining acknowledgement of receipt by the patient and the health plan requirement to re-notify members of the availability of the notice of privacy practices.

SCOPE: The scope of this policy applies to all WACBD staff and patients

POLICY STATEMENT: It is the policy of WACBD to maintain and display a notice of privacy practices (NPP) for patients, distribute the NPP to all patients receiving services, periodically review the NPP to determine if the NPP continues to be accurate and, notify patients if any major changes are made in the NPP.

DEFINITIONS:

Term	Definition
Electronic Health Records (EHR)	Electronic health records are any electronic record of patient health information generated within a clinical institution or environment, such as a hospital or doctor's office. This may include medical history, laboratory results, immunizations, demographics, etc.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under a covered entity
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Privacy Rule	The part of the HIPAA rule that addresses the saving, accessing, and sharing of medical and personal information of an individual, including a patient's own right to access
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- Notice of Privacy Practices Standards	
Notice of Privacy Practices	WACBD's NPP adheres to the following: 1. Plain Language. WACBD has written the notice in plain language. 2. Headers. WACBD has included prominent and specific language in the NPP that informs the patient and the member that the NPP contains information about a patient's privacy rights and how medical information will be treated by WACBD.

	3. Describe Uses and Disclosures. WACBD has separately described all uses and disclosures of PHI that WACBD's workforce is permitted or required to make with and without authorization. WACBD has also clearly stated that if other law, including state law, prohibits or materially limits the ability to make a use or disclosure that would otherwise be permitted under HIPAA, WACBD will only make the uses and disclosures permitted under the more stringent law. 4. List Other Activities. WACBD has listed any or all of the following activities in the NPP where WACBD intends to contact individuals for: a. providing appointment and refill reminders, b. for treatment, case management, care coordination c. communicate about a drug or biologic currently prescribed (as long as any financial remuneration received is reasonably related to the cost of the communication) d. describing or recommending treatment alternatives, providing information about health-related benefits, products and services that may be of interest to the individual, e. describing plan benefits. WACBD does not receive financial remuneration for any of the above activities. 5. Separate Statements Required. WACBD must provide a separate statement for each of the following activities in the NPP that WACBD intends to engage in: a. for a health plan or health insurance issuer if PHI may be disclosed to a plan sponsor, with the exception of disclosing PHI that is genetic information for such purposes b. fundraising communications, with the right to opt out. 6. Authorized Uses and Disclosures. WACBD has stated that all other uses and disclosures will be made only with the individual's authorization and that the individual has the right to revoke such authorization. 7. Describe Individual Rights. WACBD has described individual's rights under HIPAA and how individuals may exercise those rights as follows: a. The right to request restrictions on certain uses and disclosures, including a statement that WACBD is not required to agree to a requested restriction EXCEPT when a disclosure to a health plan is for 1) carrying out payment or health care operations and is not otherwise required by law, and 2) the PHI pertains solely to a health care item or service for which the requester has paid in full, All restrictions must be documented. b. The right to receive confidential communications of PHI c. The right to inspect and copy PHI d. The right to request amendments PHI

	e. The right to an accounting of disclosures or access report of PHI f. The right of an individual, including one who has agreed to receive the notice electronically, to obtain a paper copy of the notice upon request 8. Describe WACBD's Duties. WACBD has stated that it is are required by law to maintain the privacy of PHI, to provide a notice of their legal duties and privacy practices, and to abide by the terms of the notice currently in effect. Additionally, WACBD has stated that it reserves the right to change its privacy practices and apply the revised practices to PHI previously created or received and has described how it will provide individuals with a revised notice. 9. Notify of Privacy Breaches. A statement that WACBD is required by law to maintain the privacy of PHI, provide individuals with notice of its legal duties and privacy practices with respect to PHI, and to notify affected individuals following a breach of unsecured PHI 10. Explain How to Make Complaints. WACBD has informed individuals about how they can lodge complaints with the privacy officer or the Secretary of the U.S. Department of Health and Human Services if they believe their privacy rights have been violated and included a statement that the individual will not suffer retaliation for filing a complaint. 11. Identify Contact Person. WACBD has identified a point of contact where the individual can obtain additional information about any of the matters identified in the notice. 12. Effective Date. WACBD has included the date the notice went into effect. If WACBD revises its privacy practices in a way that is inconsistent with WACBD's NPP (in effect at the time), WACBD will revise the notice accordingly. The revised privacy practices will not be implemented prior to the effective date of the revised notice. WACBD will apply the revised practices to only that PHI is created or received under the revised notice. WACBD will attempt to obtain a signed acknowledgement form from the patient when the NPP is provided. If the patient refuses to sign the acknowledgement form, it will be noted in the patient's record. WACBD will notify patients of the availability of the NPP at least once every three years. Notice will be provided via WACBD's patient portal.

Procedure 2- WACBD Standards	
WACBD Standards	• WACBD will provide the NPP upon request of any person. The requestor does not have to be a current patient or enrollee. The notice is a public document that people can use in choosing practitioners. • The NPP will be provided to all WACBD patients upon the patient's first visit

	or receipt of services. • In an emergency treatment situation, WACBD will provide the notice as soon as reasonably practicable after the emergency. • WACBD will prominently post a copy of the NPP statement at all points of patient access to alert patients • WACBD will make an additional copy of the NPP available on site for individuals to take on request. • In the event of a revision to the notice, WACBD will promptly post the revision, make it available upon request on site, and begin distributing it at the provision of care to new patients, returning patients or to patients who have not yet received a notice from your office. • WACBD has made the NPP available on its web site and the NPP is prominently posted. • WACBD will retain copies of every version of NPP issued for a minimum of ten years. • All WACBD direct care providers make an effort to obtain the patient's written acknowledgment that he or she received a copy of NPP on the patient's first visit to the office.

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Patients Right to Access PHI	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/16/2022	**Effective Date:** 10/5/2022	**Next Review Date:** 10/5/2022
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: To provide guidance to Washington Centers for Bleeding Disorders (WACBD) regarding the patient's or authorized representative's right to access protected health information (PHI) created and maintained in WACBD's medical record.

SCOPE: The scope of this policy applies to all WACBD staff and patients

POLICY STATEMENT: A patient has a right of access to inspect and obtain a copy of PHI contained in a designated record set, for as long as the PHI is maintained in the designated record set. It is the policy of WACBD to provide a method for requesting such access.

DEFINITIONS:

Term	Definition
Designated Record Set	Includes medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- PHI Requests & WACBD Responsibilities	
If PHI Request is Granted	1. If WACBD grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested. a. WACBD must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the PHI about them in designated record sets. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, WACBD need only produce the PHI once in response to a request for access. b. WACBD must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by WACBD and the individual

	c. If the PHI is in electronic designated record set(s), WACBD must provide an electronic copy of the PHI upon request in the form and format requested by the individual if feasible, and if not in another readable electronic form and format as agreed to by both WACBD and the individual. d. WACBD may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to such a summary or explanation; and e. WACBD must provide the access as requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request. WACBD may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
If PHI Request is Denied	1. If the WACBD denies the request, in whole or in part, it must provide the individual with a written denial a. WACBD must provide a timely, written denial to the individual. The denial must be in plain language and must contain: i. The basis for the denial; ii. If applicable, a statement of the individual's right to have the denial reviewed, including a description of how the individual may exercise such right; and iii. A description of how the individual file a complaint with WACBD or to the Secretary of HHS. The description must include the name, or title, and telephone number of the contact person or office for WACBD. b. WACBD must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which WACBD has a ground to deny access. c. If WACBD does not maintain the PHI that is the subject of the individual's request for access, and WACBD knows where the requested information is maintained, WACBD must inform the individual where to direct the request for access. 2. WACBD may deny an individual access without providing the individual an opportunity for review, in the following circumstances: a. PHI is exempted from right to access b. WACBD as a covered healthcare provider, acting as a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate c. An individual's access to PHI created or obtained by a covered health

	care provider in the course of research that includes treatment may be suspended while the research is in progress if the individual agreed to the denial of access when consenting to participate in the research, and the provider informed the individual that right of access will be reinstated upon completion of the research d. An individual's access to PHI contained in records subject to the Privacy Act (5 U.S.C. 552a) may be denied in accordance with the requirements of the Act (https://www.hhs.gov/foia/privacy/index.html#:~:text=The%20Privacy%20Act%20of%201974,other%20identifying%20number%20or%20symbol.) e. The PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information. 3. In all other instances of denial, WACBD may deny an individual access, provided that the individual is given a right to have such denials reviewed. These denial reasons may include: a. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; b. The request for access is made by the individual's personal representative and the PHI makes reference to another person (not a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to the individual or another person; c. The PHI makes reference to another person (not a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person. 4. The procedure for review shall be as follows: a. Upon request of the individual, the denial shall be reviewed by a licensed health care professional, designated by WACBD to act as a reviewing official, who did not participate in the original decision to deny. b. WACBD must promptly refer a request for review to the reviewing official, who must then determine, within a reasonable period of time, whether or not to deny the access requested based on the grounds set forth above. c. WACBD must promptly provide written notice to the individual of the reviewing official's determination and must provide or deny access in accordance with the determination.
WACBD Responsibilities	1. WACBD must permit a patient to request access to inspect or to obtain a copy of the PHI that is maintained in a designated record set. (More can be found in WACBD's Patient Request for Records Policy) 2. WACBD must act on a request for access no later than 30 days after receipt

	of the request. A one-time 30-day extension can be obtained by informing the requester in writing of the reasons for the delay.

Procedure 2- Exceptions	
Exceptions	An individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for: 1. Psychotherapy notes; 2. Information compiles in reasonable anticipation of, or for use in, a civil, criminal, or criminal or administrative action or proceeding; and 3. PHI maintained by a CE that is; subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), to the extent the provision of access to the individual would be prohibited by law; or exempt from CLIA. (https://www.cdc.gov/clia/law-regulations.html)

RELEVANT REFERENCES:

- Patient Request for Records Policy
- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Privacy Officer	**Department:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/26/2022	**Effective Date:** 10/5/2022	**Next Review Date:** 10/5/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance to Washington Center for Bleeding Disorders (WACBD) regarding the responsibilities of a privacy officer who will be assigned overall responsibility for maintaining the privacy of Protected Health Information (PHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA).

SCOPE: The scope of this policy applies to WACBD and its privacy officer

POLICY STATEMENT: It is the policy of WACBD to appoint a privacy officer with appropriate authority who is responsible for overseeing WACBD's privacy program and compliance with the HIPAA Privacy Rule. The privacy officer shall be trained on his/her duties as a privacy officer.

DEFINITIONS:

Term	Definition
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Privacy Officer	Oversees and investigates all ongoing activities related to the development, implementation, and maintenance of the organization's Privacy Policies and Procedures in accordance with applicable federal and state laws
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- WACBD Privacy Officer Responsibilities	
Privacy Officer Responsibilities	1. The privacy officer is responsible for periodically reviewing the privacy program to ensure it meets sound privacy practices and reasonably ensures WACBD is in compliance with appropriate federal and state privacy and release of information regulations. This includes a review of all internal privacy policies, procedures, practices and forms. 2. The privacy officer will work with WACBD's compliance committee to ensure all current regulations related to privacy, PHI and release of information are monitored through the privacy program and required reporting is completed. 3. If the Office of Civil Rights (OCR) or other regulatory agencies conducts an audit, the privacy officer will review audit criteria related to privacy and taking appropriate action depending on the audit report generated at the

	completion of the audit. 4. The privacy officer will assist members of WACBD's workforce to determine the appropriate action if questions arise regarding the release of PHI (internally and to a third party). This would include a review of questionable authorization forms, review of questionable documentation regarding a legal representative, review of questionable subpoenas, review questionable requests for release by law enforcement, etc. 5. The privacy officer will work with Human Resources if it is necessary to sanction a member of WACBD's workforce for a privacy violation and will maintain documentation related to the sanction (incident and action taken) for no less than ten years. 6. The privacy officer will work with the US Department of Health & Human Services (OCR) if a formal privacy complaint is filed with OCR. This includes providing requested information, assisting with remediation and damage mitigation and assisting in representing WACBD if a notice of proposed penalties is received. The privacy officer will work with legal counsel if WACBD deems necessary during and possibly after the conclusion of the OCR investigation and findings. 7. The privacy officer is responsible for leading the incident response team if a privacy violation occurs such as when PHI is released inappropriately. This includes, but is not limited to, leading the investigation and assisting with mitigation of damages and developing a solution that will assist WACBD in avoiding such incidents in the future. 8. The privacy officer is responsible for remaining current on all new state and federal laws that are passed or amended. 9. If laws change, the privacy officer is responsible to assist WACBD to change impacted policies, procedures, practices and forms to comply with new laws and revisions to existing laws.

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			

Revision			

Release of PHI	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 10/18/2022	**Effective Date:** 1/4/2023	**Next Review Date:** 1/4/2023
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance to Washington Center for Bleeding Disorders (WACBD) regarding the use and disclosure of protected health information (PHI). Disclosures include:

1. reporting of suspected abuse, neglect, or domestic violence to the appropriate government agency
2. fundraising purposes
3. health oversight
4. judicial or administrative proceedings
5. law enforcement activities
6. marketing
7. public health
8. research
9. specific Government functions
10. workers compensation
11. deceased patients
12. legal representatives
13. minors
14. minor's parents/guardians
15. friends or family members
16. avert serious threat to safety
17. psychotherapy

SCOPE: The scope of this policy applies to WACBD and its patients.

POLICY STATEMENT: It is the policy of WACBD to adhere to federal and state laws regarding the release of a patient's PHI.

DEFINITIONS:

Term	Definition
De-Identified Data	De-identification of PHI ensures that personal information cannot be tied to a specific patient. De-identification is achieved by removing certain data points that can be tied to a particular individual.
Electronic Health Records (EHR)	Electronic health records are any electronic record of patient health information generated within a clinical institution or environment, such as a hospital or doctor's office. This may include medical history, laboratory results, immunizations, demographics, etc.
Fundraising	The purpose of raising funds for its own benefit
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

Government Function	For the purposes of this policy, Government Functions for which covered entities will release PHI includes Military activity, National security or intelligence activity, protective services for the President and others, correctional institutions or law enforcement custodial situations, and Covered Entities that are governmental programs providing public benefits
Marketing	A communication about a product or service that encourages recipients of the communication to purchase or use the product or service
Medical Surveillance	The systematic assessment of employees exposed or potentially exposed to occupational hazards. This assessment monitors individuals for adverse health effects and determines the effectiveness of exposure prevention strategies.
Minimum Necessary	The minimum necessary standard is a key protection of the HIPAA privacy rule. It is based on the practice that protected health care information should not be used or disclosed when it is not necessary to satisfy a particular purpose. This standard requires healthcare entities to limit unnecessary or inappropriate access to and disclosure of protected health information.
Privacy Officer	Oversees and investigates all ongoing activities related to the development, implementation, and maintenance of the organization's Privacy Policies and Procedures in accordance with applicable federal and state laws
Psychotherapy Notes	Notes taken by a mental health care professional documenting or analyzing the contents of conversation during a counseling session and separated from the rest of the patient's medical record. (Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date).
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- Release of PHI for Abuse, Neglect, or Domestic Violence	
Statement	It is the policy of WACBD to report suspected cases of abuse (child and elder), neglect or domestic violence as required by federal and state law and to do so using the minimum amount of PHI necessary for such reporting purposes (45 CFR 164.512(c)). Such decisions to report are based on the professional judgment of WACBD providers after treating or seeing a patient (minor or adult).
Abuse, Neglect, or Domestic Violence	1. If a provider suspects or has reason to suspect abuse, neglect or domestic violence, the provider will document such information in the patient's record. Such decisions to document and subsequently report is based on the professional judgment of the provider(s) after treating or seeing a patient (minor or adult). 2. The provider will report such cases or suspected cases to the WA Department of Human Services (and other agencies/officials as required by state law). 3. The provider will notate the medical record indicating records are not to be released to the suspected abuser (if known) unless specifically authorized by the patient.

Procedure 2- Release of PHI for Fundraising Purposes	
Statement	It is the policy of WACBD to comply with federal and state regulations regarding the use and disclosure of PHI for the purposes of fundraising.
Fundraising Purposes	1. WACBD will not use PHI for any fundraising purposes without the patient's written consent. 2. WACBD cannot condition treatment or payment on the patient agreeing to receive fundraising communications.

Procedure 3- Release of PHI for Health Oversight	
Statement	It is the policy of WACBD to protect the PHI of its patients and to only release such information as authorized or allowed by federal and state regulations, laws or in matter that may affect the public health and safety of others, as permitted under 45 CFR 164.512. WACBD shall release PHI for health oversight purposes to a health oversight agency when required by law. Such releases shall be limited to the minimum amount of PHI necessary to meet the requirements of the health oversight requirement.
Health Oversight Requirements GOVERNING REGULATION 45 CFR 164.512(d)	1. WACBD shall release PHI for health oversight activities and purposes authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of: a. The health care system; b. Government benefit programs for which health information is relevant to beneficiary eligibility; c. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or d. Entities subject to civil rights laws for which health information is necessary for determining compliance. 2. **Exceptions:** A health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to: a. The receipt of health care; b. A claim for public benefits related to health; or c. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services. 3. **Joint Activities or Investigations:** If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity.

Internal Procedures for Health Oversight	1. If WACBD's Privacy Officer receives a request to release PHI for health oversight activities, the Privacy Officer, or designated member of the workforce, will review the request and work with the appropriate department to compile the necessary data. 2. Health oversight releases shall be made only to the appropriate health oversight authority. 3. Following release, the release of PHI shall be documented: a. in the patient's file and in the disclosure record to be included in the event the patient requests an accounting of disclosures; and b. In a log of reportable disclosures maintained in the Privacy or Compliance office or by electronic means. 4. Any information regarding the release shall be retained for a minimum of ten years.

Procedure 4- Release of PHI for Judicial or Administrative Proceedings	
Statement	It is the policy of WACBD to release PHI for judicial and administrative proceedings when court documents specifically authorize such release. Also, release may be made pursuant to a duly authorized subpoena. WACBD will ascertain that the patient whose PHI is to be released has been properly notified or attempts have been made to notify the patient.
Judicial or Administrative Proceedings	1. When WACBD receives a court order or governmental administrative request for a patient's PHI, the request will be authenticated before any PHI is released. a. The authenticity of the court order or governmental administrative request shall be referred to the Privacy Officer who is responsible for ascertaining the validity of the request. If legal representation is necessary, the privacy officer will contact them accordingly. b. If the court order or request is deemed valid, the minimum amount of PHI necessary to satisfy the court order or request will be released to the court or governmental agency. 2. Such releases will be documented in the patient record 3. The preceding procedure will also be followed if a subpoena is received. 4. All attorney subpoenas received requesting "any and all" PHI of a patient will be referred to the Privacy Officer. 5. The Privacy Officer will contact the attorney and request clarification regarding the need for the PHI or the specific purpose behind the request, require the attorney to obtain a court order or both. 6. WACBD will not release PHI to the attorney until WACBD receives a court order or revised subpoena specifically defining what PHI is needed and for what purpose. 7. When appropriate documentation is received, the Privacy Officer or designated representative will release the appropriate PHI to satisfy the subpoena.

Procedure 5- Release of PHI for Law Enforcement	
Statement	It is the policy of WACBD to release PHI to law enforcement authorities under certain specifically defined circumstances.
Activities for Law Enforcement to Request PHI	The following represent law enforcement activities for the purposes of disclosure and this policy: 1. The law enforcement official is conducting or supervising a law enforcement inquiry or proceeding authorized by law and the disclosure is: a. A warrant, subpoena, or order issued by a judicial officer (that documents a finding by the judicial officer) b. A grand jury subpoena; or c. An administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process authorized under law, provided that: i. The information sought is relevant and material to a legitimate law enforcement inquiry ii. The request is as specific and narrowly drawn as is reasonably practicable; and iii. De-identified information could not reasonably be used. 2. If the disclosure is for the purpose of identifying a suspect, fugitive, material witness, or missing person, WACBD may disclose only the following information: a. Name b. Address c. Social Security Number d. Date of Birth e. Place of Birth f. Type of injury or another distinguishing characteristic g. Date and time of treatment. 3. If the disclosure is of the PHI of an individual who is suspected to be a victim of a crime, abuse, or other harm, if the law enforcement official states that: a. Such information is needed to determine whether a violation of law by a person other than the victim has occurred; and b. immediate law enforcement activity that depends upon obtaining such information may be necessary. 4. For purposes of alerting law enforcement of the death of an individual if WACBD has a suspicion that such death may have resulted from criminal conduct. 5. To a law enforcement official if WACBD believes in good faith that the PHI constitutes evidence that criminal conduct occurred on the premises of the covered entity. 6. Disclosure of PHI to a law enforcement official where: a. A provider is providing health care in response to a medical emergency (other than on the premises of the provider) and b. such disclosure is necessary to alert law enforcement to the commission and nature of a crime, the location of the crime or its victims, and the identity, description, and location of the perpetrator

	(provided that victims of abuse, neglect or domestic violence will be treated in accordance with the provisions as above.
WACBD Procedure to Release PHI to Law Enforcement	1. When WACBD receives a request from law enforcement for a patient's PHI, the request will be authenticated before any PHI is released. 2. If there is a question regarding the authenticity of the law enforcement request, WACBD will refer the request for disclosure to the Privacy Officer that is responsible for ascertaining the validity of the request. 3. If the law enforcement request for PHI is deemed valid, the minimum amount of PHI necessary to satisfy the court order or request will be released to the requesting law enforcement agency only if it is determined that de-identified data will not meet the needs of law enforcement 4. Any release will be in accordance with the requirements outlined in the policy. 5. Such releases will be documented in the patient's record 6. PHI will be released in certain circumstances by WACBD to law enforcement without the receipt of such a request as required by WA law (e.g., certain wounds, injuries acquired in the commission of a crime, etc.)

Procedure 6- Release of PHI for Marketing Purposes	
Statement	It is the policy of WACBD to obtain appropriate authorization from the patient prior to utilizing PHI for marketing purposes.
Marketing Purposes	1. WACBD will not use PHI for any marketing purposes without a patient's written consent. 2. If WACBD receives any direct or indirect payment from a third party for a marketing activity or communication, the authorization for that activity or communication must contain a statement that notifies the patient of that fact.

Procedure 7- Release of PHI for Public Health	
Statement	It is the policy of WACBD to protect the PHI of its patients and to only release such information as authorized or allowed by federal and state regulations, laws or in matter that may affect the public health and safety of others, as permitted under 45 CFR 164.512. WACBD shall release PHI for public health purposes when required by law or requested by a public health authority. Such releases shall be limited to the minimum amount of PHI necessary to meet the requirements of the public health requirement or request.
Requirements	WACBD shall release PHI for public health activities and purposes as follows: 1. To a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability; or, at the direction of a public health authority, to an official of a

	foreign government agency that is acting in collaboration with a public health authority 2. To an appropriate government entity authorized by law to receive reports of child abuse or neglect 3. To those subject to the jurisdiction of the Food and Drug Administration (FDA) for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include: a. To collect or report adverse events products defects or problems (including problems with the use or labeling of a product), or biological product deviations b. To track FDA-related products c. To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or d. To conduct post market surveillance 4. To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, as authorized by law. 5. To a school for proof of immunization for a student or prospective student where such information is required for admission 6. Internally about a member of the workforce if: a. Made to a health care provider within WACBD who provides health care to the workforce member for the following: i. To conduct an evaluation relating to medical surveillance of the workplace; or ii. To evaluate whether the individual has a work-related illness or injury; b. The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance; c. WACBD needs such findings in order to comply with its obligations, under Federal or state law, to record illness or injury or to carry out responsibilities for workplace medical surveillance; and d. The health care provider within WACBD provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to WACBD i. By giving a copy of the notice to the workforce member at the time the health care is provided; or ii. If the health care is provided on the work site of the employer

	7. If the health care providers within WACBD discloses work-related illnesses and injuries to an employer or performs medical surveillance of the workplace, it shall provide written notice to the client.
WACBD Internal Procedure	1. If the Privacy Officer receives a request to release PHI for public health activities, the Privacy Officer or designated member of the workforce will review the request and work with the appropriate department to compile the necessary data. 2. Limited data sets can be released for public health purposes upon request. WACBD does not charge a fee to prepare and transmit the data for public health purposes. 3. Public health releases shall be made only to the appropriate public health individual or entity. 4. Following release, the release of PHI shall be documented within the patient record located within the Electronic Health Record (EHR) 5. Any information regarding the release shall be retained for a minimum of ten years.

Procedure 8- Release of PHI for Research Purposes	
Statement	It is the policy of WACBD that, in compliance with 45 CFR 164.512(i), PHI may be released for research purposes without authorization of the individual if such is approved by an Institutional Review Board (IRB) prior to release of PHI. If use without authorization is not approved by the IRB, specific patient authorization is required prior to use of the patient's PHI for research purposes.
Research Proceedings	1. Any research project proposals requiring the use of identifiable PHI shall be submitted to the Internal Review Board (IRB) for review. 2. The IRB has the authority to approve such research projects with or without requiring specific authorization from subjects of the research. 3. Such approval only applies to the specifically defined research project. Any changes in the scope of the research project need to be reviewed by the IRB with the same approval requirements. 4. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. 5. WACBD may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research. When this is the case, any compound authorization used must

	clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

Procedure 9- Release of PHI for Specific Government Functions	
Statement	It is the policy of WACBD to release PHI for certain specifically defined government functions. WACBD will review such releases for minimum necessary requirements and will only release the following information to law enforcement under circumstances noted.
Specific Government Functions	When WACBD receives a request from specific government organizations for a patient's PHII, the request will be authenticated before any PHI is released. 1. Military activity: WACBD may use and disclose PHI of Armed Services personnel to the appropriate authorities for activities deemed necessary by appropriate military command authorities and for foreign military personnel. 2. National security or intelligence activity: WACBD may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities. 3. Protective services for the President and others: WACBD may disclose PHI to authorized federal officials for the provision of protective services to the President, foreign heads of state or other authorized persons, or for the conduct of related investigations. 4. Correctional institutions or law enforcement custodial situations: WACBD may disclose PHI to a correctional institution or a law enforcement official having lawful custody of an inmate if the official or institution represents PHI is needed for the provision of health care to the individual, for the health and safety of the individual or others, for law enforcement on the premises of the correctional institution, or for , the administration, safety, security, and order of the correctional institution. 5. Covered entities that are governmental programs providing public benefits. a. WACBD, as a covered entity, may disclose PHI relating to government benefit programs. WACBD will review such releases for minimum necessary requirements. If there is a question regarding the authenticity of the request, WACBD will refer the request for disclosure to the privacy officer who is responsible for ascertaining the validity of the request. • If the request for PHI is deemed valid, the minimum amount of PHI necessary to satisfy the court order or request will be released to the requesting government organization only if it is determined that de-identified data will not meet the needs of the request. • Any release will be in accordance with the requirements outlined in the policy • Such releases will be documented in the patient's record.

Procedure 10- Release of PHI for Workers Compensation	
Statement	WACBD may disclose PHI to workers compensation programs for the purpose of meeting workers compensation activities. Workers compensation is specifically exempted from coverage under the HIPAA regulation, which permits covered entities to disclose protected health information to workers' compensation insurers, State administrators, employers, and other persons or entities involved in workers' compensation systems, with or without the individual's authorization.
Workers Compensation	1. If a valid request is made requesting release of patients' PHI for workers compensation, such a release shall be completed by WACBD's designated authority. 2. Any release made for workers compensation reasons shall include only the PHI necessary to meet the parameters of the request (minimum necessary): a. PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. b. Information must be limited to the amount and types of PHI that are necessary to obtain payment for health care provided to an injured or ill worker. Where protected health information is requested by a state workers' compensation or other public official. WACBD is permitted to reasonably rely on the official's representations that the information requested is the minimum necessary for the intended purpose. 3. Such a release shall be made only to the appropriate workers compensation individual or entity. 4. Following release, the release of PHI shall be documented in the patient's record and in the disclosure record to be included in the event the patient requests an accounting of disclosure. 5. Any information regarding the release shall be retained for a minimum of ten years.

Procedure 11- Release of PHI for Deceased Patients	
Statement	It is the policy of WACBD to protect a deceased person's PHI in the same way it protects a living person's PHI.
Deceased Patients	1. If the request is for a person who has been deceased for over 50 years and the records still exist, the records can be released without further approval or documentation. 2. If the request is for a person who has been deceased for less than 50 years, WACBD will require the appropriate documentation such as a will, court order or legal cite (in the event the request is from a government agency and release is required by law). There are some provisions which allow PHI to be disclosed including: a. alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct (§ 164.512(f)(4))

	b. to coroners or medical examiners and funeral directors (§ 164.512(g)) c. for research that is solely on the protected health information of decedents (§ 164.512(i)(1)(iii)) d. to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation (§ 164.512(h)). 3. In addition, the Privacy Rule permits WACBD to disclose protected health information about a decedent to a family member, or other person who was involved in the individual's health care or payment for care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity. This may include disclosures to spouses, parents, children, domestic partners, other relatives, or friends of the decedent, provided the information disclosed is limited to that which is relevant to the person's involvement in the decedent's care or payment for care

Procedure 12- Release of PHI for Legal Representatives	
Statement	It is the policy of WACBD to treat a legal representative of a patient, designated and authorized under applicable law, just as WACBD would the patient to the extent that PHI and relevant health information pertains to the matters for which the legal representative is authorized to represent the patient. This includes parents of minor children, court-appointed guardians, and persons with power of attorney.
Legal Representatives	1. If WACBD receives a request from a legal representative of a patient, documentation such as a court order or healthcare power of attorney needs to accompany the request. 2. If appropriate documentation does not accompany the request for PHI, WACBD shall request such documentation. 3. If appropriate documentation is not provided, release of PHI will be denied unless otherwise authorized under the HIPAA Privacy Rule. 4. Once appropriate documentation is received it will be reviewed by WACBD's designated authority and the appropriate PHI will be released to the legal representative of the patient. 5. Such release or denial of release shall be documented in the patient's record along with the documentation (or a copy of the documentation) and the signed request.

Procedure 13- Release of PHI for a Minor	
Statement	It is the policy of WACBD, with limited exceptions, to obtain written permission from a parent, guardian, or person acting in the place of a parent to use or disclose

	information about a minor where the minor does not have the capacity to give consent for care.
Legalities Around PHI and Minors	If WACBD has a reasonable belief that the parent, guardian or other person acting in the place of a parent has abused or neglected the minor and has determined it is not in the minor's best interest, WACBD will not allow the parent (or legal representative) to exercise the minor's rights and authorities under HIPAA. The minor, not the parent, can consent to the use or disclosure of PHI and exercise exclusive rights with respect to such information if: 1. The minor's parent assents to an agreement of confidentiality between the physician and the minor with respect to such health care service; or 2. The minor lawfully obtains a health care service without the consent of or notification to a parent, guardian or other person acting in the place of the parent and the minor has not requested that such person be treated as the legal representative. In those instances where WACBD must have the patient or legal representative's written permission to use or disclose their PHI, you must obtain the minor's written permission to use or disclose the PHI.
PHI Release to a Minor	1. If WACBD receives a request for release of PHI from a minor who is a patient, WACBD shall request parent or legal representative authorization prior to releasing information to the minor UNLESS: a. The minor's parent assents to an agreement of confidentiality between the physician and the minor with respect to such health care service; or b. The minor lawfully obtains a health care service without the consent of or notification to a parent, guardian or other person acting in the place of the parent and the minor has not requested that such person be treated as the legal representative. In those instances, WACBD must have the patient or legal representative's written permission to use or disclose their PHI, the minor's written permission to use or disclose the PHI must be obtained 2. If WACBD receives appropriate authorization in accordance with the above, the requested PHI will be released to the minor and the released information noted in the minor patient's record. 3. If authorization is not received, the minor's request for release of PHI will be denied in writing. The denial will also become part of the minor's record. 4. If the minor is of the age of consent, 18 years old (RCW 26.28.010), PHI will be released to the minor without authorization from the parent or legal representative except under circumstances where it is deemed inappropriate.

Procedure 14- Release of PHI for a Minor's Parent/ Guardian	
Statement	It is the policy of WACBD to be in compliance with federal and state privacy and security regulations as they relate to the protection of the PHI of minor patients. WACBD shall follow regulation guidance and state law when releasing the information of minor patients.

Minor's Patent/ Guardian	1. If WACBD receives a request for release of PHI for a minor patient, such release will be in accordance with this policy and guidance included herein. 2. WACBD will require the production of appropriate documentation such as a driver's license, passport or other form of acceptable individual identification to authenticate the person requesting access to a minor's PHI is the legal parent or guardian. WACBD shall exercise due diligence in obtaining these documents. 3. If appropriate documentation does not accompany the request for PHI, WACBD shall request such documentation. 4. If appropriate documentation is not provided, release of PHI will be denied unless otherwise authorized under the HIPAA Privacy Rule and WA law. 5. Once appropriate documentation is received it will be reviewed by the Privacy Officer or designated authority. Determination will be made if PHI will be released to the requesting party. 6. WACBD shall not release specifically protected minor PHI unless accompanied by an authorization from the minor. This includes: a. Treatment for STDs (RCW 70.02.220) b. Treatment for mental health (RCW 70.02.240) 7. If such a release request is accompanied by a signed authorization from the minor, WACBD will release the requested PHI to the legal parent or guardian. 8. If no authorization accompanies the request for release of information, WACBD shall only disclose PHI that does not include specifically protected PHI. 9. Such release or denial of release shall be documented in the minor's record. 10. All documentation related to the release of PHI of a minor will be retained in the medical record.
Exceptions	1. When state or other law does not require parental consent in order for a minor to obtain a health service, and the minor consents, the parent is not the personal representative (e.g., pregnancy, treatment for STD, HIV) 2. When a court authorizes someone other than the parent to make treatment decisions for a minor or the parent is not the personal representative, then the parent has no access to PHI of minor. 3. When the parent agrees to the confidential relationship between a physician and minor. 4. When a physician believes that the disclosure of information endangers the child, parental access is denied

Procedure 15- Release of PHI to Friends or Family Members	
Statement	It is the policy of WACBD to appropriately protect the privacy of health information that can identify its patients in accordance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and applicable state laws and to only release protected health information to family members, other relatives, and close personal friends of the patient, as well as any other persons identified by the patient, in specific limited circumstances.

Friends or Family Members	1. If WACBD receives a request for PHI from a patient's family, relative, close friend, or other persons identified by the patient, WACBD shall attempt to allow the patient the opportunity to agree or object to release of PHI. Such an agreement or objection does not need to be in writing but does need to be noted in the patient's record. 2. If the patient objects to release of information to the family, relative, close friend, or other identified persons requesting access to PHI, WACBD will not disclose PHI including health condition to the individual requesting the information unless, in the professional judgment of the WACBD provider, the individual is critical to the care of the patient and the need to know is appropriate. 3. If the patient does not object or is not in a position to object, WACBD shall use professional discretion and release PHI appropriate to the situation. This shall also be documented in the patient's record. 4. PHI may be disclosed to a family member, relative, close friend, or other persons identified by the patient, when: a. That information is relevant to such person's involvement with the patient's care or payment related to such care, or b. To notify (or assist in the notification of) such persons of the patient's location, general condition, or death, 5. PHI may be disclosed if the patient is not present, due to incapacity or emergency circumstances only if: a. The PHI is directly relevant to the person's involvement with the patient's health care, and it is in the patient's best interest. b. WACBD may use professional judgment and experience with common practice to make reasonable inferences regarding the patient's best interest in allowing a person to act on behalf of the patient to "pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI."

Procedure 16- Release of PHI to Avert Serious Threat to Safety	
Statement	It is the policy of WACBD to protect the PHI of its patients and to only release such information as authorized or allowed by federal and state regulations, laws or in matter that may affect the public health and safety of others, as permitted under 45 CFR 164.512. WACBD may release PHI in the event, in the professional judgment of WACBD, the Privacy Officer or other specifically designated authority. Such release will prevent a serious threat to public safety or to the safety of another. Such releases shall be limited to the minimum amount of PHI necessary to address known or suspected serious threats to public safety or the safety of another.
Avert Serious Threat to Safety GOVERNING REGULATION 45 CFR 164.512(j) - 45 CFR 164.512(j)(ii)	Standard: Uses and disclosures to avert a serious threat to health or safety. 1. Permitted disclosures- A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure: a. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

	b. Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or c. Is necessary for law enforcement authorities to identify or apprehend an individual
Internal Procedures	1. If, in the professional opinion of WACBD's Privacy Officer or specifically designated authority, it is determined that it is necessary to release PHI to avert a threat to safety, an evaluation will be conducted and, if appropriate, the PHI will be released to the appropriate party which includes: a. Public health Official b. Law enforcement Official or Officer c. Community mental health Official d. The courts (in the event civil commitment is deemed appropriate) 2. The Privacy Officer or designated authority will compile the necessary data and said data about a patient will be released following minimum necessary standards. 3. Such a release shall be made only to the appropriate individual or entity. 4. Following release, the release of PHI shall be documented a. in the patient's file and in the disclosure record to be included in the event the patient requests an accounting of disclosure; and b. In a log of reportable disclosures maintained in the Privacy or Compliance office or by electronic means. 5. Any information regarding the release shall be retained for ten years. 6. Follow up PHI releases for the same incident shall be evaluated to meet minimum necessary standards and documented in the same way as the original release. Such release shall only be related to the release to avert an identified danger to the safety to the public or others.

Procedure 17- Release of PHI in Psychotherapy Notes	
Statement	It is the policy of WACBD to comply with HIPAA (and any appropriate state law or regulation), and with a few limited exceptions, to obtain from the patient a separate and distinct authorization to use and disclose psychotherapy notes for any purpose. Most WACBD psychosocial assessments during comprehensive visits are not considered a psychotherapy notes.
Psychotherapy Notes	When WACBD receives a request for release of psychotherapy notes, the request will be forwarded to the Privacy Officer or designated authority. 1. The Privacy Officer or designee shall review the request and, if it meets all of the criteria cited in this policy, approve release. 2. Such release will not be made if patient authorization is required prior to release until such authorization is received by WACBD. 3. If the patient requests a copy of his/her psychotherapy notes, the Privacy Officer or designee shall consult with the appropriate mental health professional.

	4. Any release to the patient shall only be made if the mental health professional, in his/her professional judgment, does not consider such a release to the patient to be a danger to the patient or others. 5. Denial of access to the patient may be appealed to another designated mental health professional. 6. The decision to release or deny the release of psychotherapy notes to the patient by the designated mental health professional shall be binding on WACBD and the patient. 7. Releases for legal purposes shall be reviewed by the Privacy Officer, as well as and Legal Department as appropriate, prior to release.
Exceptions	A separate and distinct authorization is not required to carry out the following treatment, payment, or health care operations: 1. The person who created the psychotherapy notes may use the notes for treatment purposes, but not for payment or health care operations purposes; 2. WACBD workforce members may use and disclose psychotherapy notes to conduct WACBD's own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; 3. WACBD workforce members may use or disclose psychotherapy notes to defend a legal action or other proceeding brought by the patient. a. NOTE: This category of disclosure allows release of information to WACBD's attorney to defend against the action or proceeding and must be reviewed and approved by the Privacy Officer prior to disclosure. 4. WACBD workforce members may disclose psychotherapy notes to avert a serious threat to health or safety. 5. WACBD workforce members may disclose psychotherapy notes to the subject of the notes. 6. WACBD workforce members may disclose psychotherapy notes as required by law. 7. WACBD workforce members may disclose psychotherapy notes to a health oversight agency for oversight of the note's originator. 8. WACBD workforce members may disclose psychotherapy notes regarding a decedent to coroners, medical examiners and funeral directors for identification purposes, to determine cause of death, or to allow such person to carry out their duties with respect to the decedent. 9. WACBD workforce members may disclose psychotherapy notes to the patient only if the mental health professional creating the notes does not consider such release to be a danger to the patient or others.

RELEVANT REFERENCES:

- RCW 70.20
- 45 CFR 164.512(b)
- 45 CFR 164.512(d)
- 45 CFR 164.512(i)
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY:

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Request for Confidential Communications	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 10/10/2022	**Effective Date:** 10/19/2022	**Next Review Date:** 10/19/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance to Washington Center for Bleeding Disorders (WACBD) workforce members regarding the handling of requests by the patient for confidential communications or communication to an alternate party.

WACBD must permit patients to request alternative means or location for receiving communications of PHI by means other than those that the covered entity typically employs. For example, a patient may request that the provider communicate with the patient through a designated address or phone number. WACBD must accommodate reasonable requests if the patient indicates that the disclosure of all or part of the protected health information could endanger the patient. WACBD shall not question the patient's statement of endangerment.

SCOPE: The scope of this policy applies to WACBD and its patients.

POLICY STATEMENT: It is the policy of WACBD to identify alternative means when a request from a patient is received asking to communicate confidentially by some alternative means or location. WACBD will determine the reasonableness of the request based on administrative capability of complying and, if the request is reasonable, communicate with the patient in the requested manner.

DEFINITIONS:

Term	Definition
Confidential	Confidentiality in the medical setting refers to "the principle of keeping secure and secret from others, information given by or about an individual in the course of a professional relationship," and it is the right of every patient, even after death. Maintaining confidentiality is part of the "good faith" that exists between doctor and patient. Ignoring patients' rights to confidentiality would lose their trust and might prevent people from seeking help when needed. Confidentiality preserves individual dignity, prevents information misuse, and protects autonomous decision making by the patient.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- Patient Confidential Communications Request	
Patient Confidential	1. All requests must be on the Patient Request for Confidential Communications

Communications Request	Form. (Appendix 4) 2. WACBD will review the patient request for confidential communication and determine if the request is administratively feasible. 3. If it is not administratively feasible WACBD will: a. Contact the patient and inform them of this. b. Attempt to work with the patient to establish a method of communication that is administratively feasible c. Document the agreed upon methods of communication on a new Form and have the patient sign the updated form. 4. Communicate with the patient in the requested manner if the request is reasonable and accepted by WACBD

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2323098/#:~:text=Confidentiality%20in%20the%20medical%20setting,every%20patient%2C%20even%20after%20death.

APPROVING COMMITTEE(S):

Policy and Compliance Committee

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Request to Amend Patient Record	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 10/17/2022	**Effective Date:** 10/26/2022	**Next Review Date:** 10/26/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: Provide guidance to Washington Center for Bleeding Disorders regarding requests by patients or authorized patient representatives to amend personal health information (PHI) in their health care record.

SCOPE: The scope of this policy applies to WACBD and its patients.

POLICY STATEMENT: It is the policy of WACBD to maintain a process to accept or deny requests from patients and authorized patient representatives to amend PHI in their health care records, that all requests will be carefully evaluated, and that the patient or authorized patient representatives will be notified of any decision within 60 days of receipt of the request.

DEFINITIONS:

Term	Definition
Amend	To alter, modify, rephrase, or add to or subtract from
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

PROCEDURES:

Procedure 1- Patient Request to Amend Record	
WACBD	WACBD will require patients and/or authorized patient representatives make requests for amendment in writing. 1. A member of WACBD's workforce designated to review such requests, or the appropriate physician will evaluate the request to determine if amendment is appropriate and will make a determination to grant the amendment request, deny the request or partially deny the request.
Acceptance of Amendment Request	If the request for amendment is accepted, A member of WACBD's workforce or the appropriate physician will: 1. make the appropriate amendment; 2. identify the records that are affected by the amendment, and append or otherwise provide a link to the location of the amendment in the affected records; 3. inform the patient or plan member the amendment request has been accepted using an acceptance of denial on letterhead.

Denial of Amendment Request	If the request for amendment is denied, a member of WACBD's workforce, or appropriate physician will: 1. base denial of amendment on the determination that the PHI (that is the subject of the request for amendment): a. Was not created by WACBD; b. Is not part of the individual's designated record set; c. Is accurate and complete; d. Would not be accessible to the individual for the reasons under WACBD's Policy "Patient Right to Access PHI" 2. Inform the patient the amendment request has been denied in writing. 3. Ensure patient is notified of rights following a denial, including: a. Right to submit a written statement disagreeing with the denial b. Right to file a formal complaint with WACBD c. Right to file a formal complaint with the Secretary of DHHS If the patient submits a written statement disagreeing with the denial, WACBD may reasonably limit the length of the statement of disagreement and, if appropriate, prepare a written rebuttal to the individual's statement. If a member of WACBD's workforce prepares a rebuttal, a copy will be provided to the patient. A member of WACBD's workforce will respond with a denial on letterhead. The denial may include the following: a. The patient's request for amendment b. WACBD's denial of the request c. The patient's statement of disagreement (if any) d. WACBD's rebuttal (if any) If the amendment is denied and the patient or plan member submits a written statement of disagreement, the statement, WACBD's rebuttal, and the written denial, or an accurate summary of these items, must be included with any subsequent disclosure of the PHI to which the disagreement relates. If the patient does not submit a written statement of disagreement, a member of WACBD's workforce will include the statement, rebuttal, and form only if the individual requests that WACBD do so.

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):
Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Requests for Restriction	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 10/20/2022	**Effective Date:** 10/26/2022	**Next Review Date:** 10/26/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: Provide guidance to Washington Center for Bleeding Disorders (WACBD) regarding patient requests for restriction to access their protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

SCOPE: The scope of this policy applies to WACBD and its patients.

POLICY STATEMENT: It is the policy of WACBD to allow patients to exercise their right to request restrictions of release of PHI, that all requests for restrictions will be carefully reviewed and that the patient will be notified, in writing, of all decisions made by WACBD related to the request.

DEFINITIONS:

Term	Definition
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

PROCEDURES:

Procedure 1- Restriction Request	
Patient Restriction Request	1. If a patient wishes to request a restriction on WACBD's use or disclosure of PHI, the patient will be asked to send a written request. 2. WACBD or an appropriate department manager will review the request to determine if the requested restriction would interfere with treatment, payment, and operations. 3. WACBD will attempt to honor a request for a restriction of disclosures for carrying out payment or operations that are not otherwise required by law. 4. WACBD is not required to agree with any other requests for restrictions, if the request interferes with treatment, payment or operations, the request may be denied and the patient will be notified in writing of such decision, in writing. 5. If WACBD agrees to the requested restriction, an appropriate department manager will document any restrictions agreed upon in writing. The documentation will be retained for ten years from the date it was last in effect. In addition: a. The patient must be notified in writing b. The restriction must be communicated in a manner as to assure that anyone accessing the information in the record, whether paper or

	electronic, becomes aware of the restriction. 6. WACBD will use and disclose information consistent with any agreed-upon restrictions and the above policy unless the use or disclosure is required by law. 7. WACBD may terminate a restriction with the patient's written agreement. 8. If WACBD wishes to terminate a restriction without the patient's agreement, the termination will only apply to PHI created or received after WACBD has informed the patient of the termination. The restriction continues to apply to PHI created or received prior to informing the patient of the termination. 9. If the restriction request is terminated, WACBD will note the date the restriction is terminated ("End Date") in writing. 10. If a patient requests WACBD restrict the disclosure of PHI, WACBD must comply with the requested restriction: a. Except as otherwise required by law, the disclosure is for purposes of payment or operations.

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Required PHI Disclosures	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 10/19/2022	**Effective Date:** 11/02/2022	**Next Review Date:** 11/2/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy to alert the workforce members that WACBD is required to disclose PHI to an individual when requested or the Secretary of Health and Human Services (HHS) to investigate or determine WACBD's compliance with the HIPAA privacy provisions.

SCOPE: The scope of this policy applies to WACBD and its patients.

POLICY STATEMENT: It is the policy of WACBD to safely release protected health information to the patient and/or the patient's authorized representative upon request and as required by law under 45 CFR 164.512 and 164.502(a)(2).

DEFINITIONS:

Term	Definition
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Minimum Necessary	The minimum necessary standard is a key protection of the HIPAA privacy rule. It is based on the practice that protected health care information should not be used or disclosed when it is not necessary to satisfy a particular purpose. This standard requires healthcare entities to limit unnecessary or inappropriate access to and disclosure of protected health information.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- Required PHI Disclosures	

Required PHI Disclosures	• WACBD is required to disclose PHI to an individual patient and/or patient authorized representative when requested or required to meet the individual's right to access, inspect and obtain a copy of the individual's PHI,
	  ○ When WACBD receives a request for PHI from a patient and/or patient authorized representative to whom the PHI pertains, the Privacy Officer or designee will follow the Patient Right to Access policy.
	  ○ Release of PHI to the individual is required with limited exceptions and is not subject to minimum necessary.
	• WACBD is required to disclose PHI when required by the Secretary of Health and Human Services (HHS) to investigate or determine WACBD's

	compliance with the HIPAA privacy provisions. o If the Privacy Officer receives a request to release PHI to the Secretary of HHS for compliance review, the Privacy Officer or designee will work with the appropriate departments to compile the necessary data in a timely manner. o Upon notification, release of PHI to the Secretary of HHS is required and all information requested must be provided. • WACBD is also required to release PHI when required by state or federal law. Such releases shall be limited to the minimum amount of PHI necessary to meet the legal requirements of the law. o If the Privacy Officer receives a request to release PHI as required by state or federal law, the Privacy Officer or designated member of the workforce will review the request and work with the appropriate departments to compile the necessary data. o Release of PHI when required by state or federal law is required and all information required by law must be provided. • Following any PHI release, the release of PHI shall be documented o in the patient's file and in the disclosure record to be included in the event the patient requests an accounting of disclosures; and • Any information regarding each release shall be retained for a minimum of ten years.

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- 45 CFR 164.512 and 164.502(a)(2)

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Training Requirements	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 10/20/2022	**Effective Date:** 11/2/2022	**Next Review Date:** 11/2/2025
Policy Contact: Privacy Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance regarding workforce member training related to all policies, procedures, and regulations about patient privacy and security in accordance with the Health Insurance and Portability Act of 1996 (HIPAA).

SCOPE: The scope of this policy applies to WACBD and its staff.

POLICY STATEMENT: WACBD will provide HIPAA privacy and security training to its workforce. The workforce includes employees. For contracted employees, WACBD will verify the completion of HIPAA training with the contracted organization. All workforce members are required to complete HIPAA privacy and security training within 60 days of employment. Following initial hired training, additional training must be conducted at least annually and may consist of class training, Internet based training, or other informational announcements, etc.

DEFINITIONS:

Term	Definition
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Minimum Necessary	The minimum necessary standard is a key protection of the HIPAA privacy rule. It is based on the practice that protected health care information should not be used or disclosed when it is not necessary to satisfy a particular purpose. This standard requires healthcare entities to limit unnecessary or inappropriate access to and disclosure of protected health information.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient

PROCEDURES:

Procedure 1- HIPAA Training	
HIPAA Training	Training will cover all aspects of HIPAA requirements including (not inclusive): Notice of Privacy Practices Patient rights Appropriate exchange of PHI for treatment, payment, and healthcare operations Authorizations and consents Minimum necessary standards Sanctions HIPAA Privacy and Security policies and procedures

	Additional training may be provided for special classes of the workforce such as IT department staff, privacy/compliance/legal workforce members, health records management staff, etc. WACBD utilizes training software to provide new workforce member training and annual trainings on HIPAA. The training report showing completion shall be held by Human Resources Department. All workforce members shall be required to review and sign WACBD's confidentiality agreement annually. All training materials shall be retained for at least ten years from the date last used.

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Workforce Sanctions for HIPAA Violations	Department: Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 11/01/2022	**Effective Date:** 11/9/2022	**Next Review Date:** 11/9/2025
Policy Contact: Privacy Officer, HR	**Version:** #1	

PURPOSE: The purpose of this policy is to provide guidance on possible appropriate sanctions against workforce members who fail to comply with Washington Center for Bleeding Disorder's (WACBD) privacy and security policies, procedures and practices or states or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The sanctions shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of protected health information (PHI), and similar factors. Sanctions against WACBD workforce members may include but are not limited to verbal counseling, written counseling, suspension, demotion, transfer and termination of employment, contract penalties and contract termination.

SCOPE: The scope of this policy applies to WACBD workforce members

POLICY STATEMENT: In accordance with any disciplinary action policy in force through Human Resources or Administration, WACBD will apply appropriate sanctions against members of its workforce who fail to comply with the privacy and security policies and procedures. WACBD will, when appropriate, refer all violations of state and federal law to appropriate external agencies for further investigation and/or prosecution. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), penalties for misuse or misappropriation of PHI include both civil monetary penalties and criminal penalties.

DEFINITIONS:

Term	Definition
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Privacy Officer	Oversees and investigates all ongoing activities related to the development, implementation, and maintenance of the organization's Privacy Policies and Procedures in accordance with applicable federal and state laws
Sanctions	Civil, criminal, and/or internal company penalties as a result of violating HIPAA law
Whistleblower	A person who informs on a person or organization engaged in an illicit activity

PROCEDURES:

Procedure 1- WACBD Internal Sanctions	
WACBD Internal Sanctions	• In collaboration with the HIPAA Privacy Officer/ Security Officer, Human Resources will have the responsibility of reviewing and authorizing the

	appropriate sanctions for substantiated violations committed by members of WACBD's workforce.
	• All sanctioning of workforce members will be documented and retained for a period of at least ten years from the date of its creation or the date when it was last in effect, whichever is later. Documentation shall include but is not limited to:
	  ○ The name of workforce member.
	  ○ The violation that has occurred.
	  ○ The date of violation.
	  ○ Documentation substantiating the violation (e.g., Privacy Officer investigation summary)
	  ○ The sanction authorized.
	• Sanctioning documentation will be maintained by the HIPAA Privacy Officer/ Security Officer for all privacy and security violations of all such actions for HIPAA-related violations.
	• Sanctioning/disciplinary action taken against the workforce member will include a notice if
	  ○ civil or criminal penalties for misuse or misappropriation of health information is suspected or has occurred.
	  ○ the violation may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations.

Procedure 2- Exceptions	

Exceptions	This policy does not apply to workforce members who exercise their right to:
	• File a complaint with the Department of Health and Human Services
	• Testify, assist, or participate in an investigation, compliance review, proceeding
	• Oppose any act made unlawful by the HIPAA privacy and security rules; provided the individual or person has a "good faith" belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA privacy and/or security rules
	• Disclose PHI as a whistleblower provided that:
	  ○ The workforce member or business associate believes in good faith that WACBD has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, service, or conditions provided by WACBD potentially endangers one or more patients, workers, or the public
	  ○ The disclosure is to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or condition of the covered entity or to an

	appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by WACBD or an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to whistleblower activity; and, o An employee who is a victim of a criminal act and discloses PHI to a law enforcement official, provided that the PHI is about a suspected perpetrator of the criminal act; and is limited to permitted disclosures pursuant to WACBD's policies and procedures.

RELEVANT REFERENCES:

- WACBD Confidentiality Agreement
- HIPAA Final Privacy Rule, 45 CFR Parts 160 and 164, Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system.
- HIPAA Omnibus Rule, revisions to 45 CFR Parts 160, and 164, Department of Health and Human Services, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #1 **Administrative Safeguards** **Security Management Policy**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 8/30/2022	**Effective Date: 1/11/2022**	**Next Review Date: 1/11/2024**
Policy Contact: Security Officer	**Version: # 1**	

Purpose: The purpose of the policy is to develop a risk management process for the selection and implementation of security safeguards to reduce the risks to electronic Protected Health Information (ePHI) to reasonable and manageable levels

Scope: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

Statement of Policy: Washington Center for Bleeding Disorders (WACBD) is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required and will comply with safeguarding electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

Delegation of Responsibilities: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

Definitions:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient.
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

1. Security Management Policy

IMPLIMENTATION TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(1)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to prevent, detect, contain and correct security violations."

WACBD will protect the confidentiality, integrity, and availability of ePHI by maintaining appropriate safeguards for the networks and systems that handle ePHI. WACBD will implement policies and procedures to prevent, detect, contain, and correct security violations.

WACBD will comply with the policies and procedures where possible and will ensure appropriate policies and procedures for protecting ePHI.

1.1 Risk Analysis

SAFEGUARD: Administrative

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(1)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity."

1. WACBD acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI.
2. WACBD acknowledges the potential vulnerabilities associated with storing ePHI, transmitting ePHI locally and transmitting ePHI outside of WACBD.
3. To appropriately assess such potential vulnerabilities, WACBD shall perform a Risk Assessment which:

i. Identify and document all ePHI repositories
ii. Identify and document potential threats and vulnerabilities to each repository
iii. Assess current security measures
iv. Determine the likeliness of threat occurrence
v. Determine the potential impact of threat occurrence
vi. Determine the level of risk
vii. Determine additional security measures needed to lower level of risk
viii. Document the findings of the Risk Assessment

Procedure

1. Document all ePHI repositories

i. Identify and document where ePHI is stored, received, maintained, or transmitted.

1. ePHI may be identified through surveys, questionnaires, interviews, review of documentation, automated scans, or other data gathering methods.

ii. The output of this process should be documentation of all repositories/systems that contain ePHI in an organization.

2. Identify and document potential threats and vulnerabilities to each repository

i. Identify and document all reasonably anticipated threats to ePHI. Examples of Threats include:

1. Data entry error
2. Theft of a laptop
3. Power outage

ii. Identify and document all vulnerabilities to each ePHI repository.

iii. The output of this process should be documentation of all reasonably anticipated threats and vulnerabilities to each repository/system that contains ePHI within an organization.

3. Assess current security measures

i. Review the current security measures (safeguards / controls) that are currently in place that are used to mitigate identified risks. Examples of current safeguards include:

1. User awareness training
2. Backup procedures
3. Disaster Recovery procedures
4. Employee termination procedures

ii. The output of this process should be documentation of current security measures to protect any repositories/systems within the organization.

4. Determine the likeliness of threat occurrence

i. For each threat and vulnerability to ePHI that has been identified in step 2 of the Risk Assessment procedure, calculate the likelihood of the threat occurring.

ii. The likeliness or probability of a threat occurring is usually measured in (low, medium, or high) or expressed as a number of times a threat is likely to occur in a given year.

iii. Existing security measures as identified in step 3 of the Risk Assessment procedure may lower the likeliness of a threat.

iv. Existing vulnerabilities as identified in step 2 of the Risk Assessment procedure may raise the likeliness of a threat.

v. Examples of a likeliness of a threat includes:

1. If there have been issues with power outages in the past, then the threat of a power outage may be assessed as ***High***. Additionally, if a backup generator has been previously installed (current security measure) then the likeliness of a threat of a power outage may be reduced to ***Medium*** or ***Low***.
2. If there have been no issues with flooding in the past 5 years, then the threat from flooding may be assessed as ***Low***.

vi. The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability, and integrity of ePHI of an organization.

5. Determine the potential impact of threat occurrence

i. For each threat and vulnerability to ePHI, calculate the associated impact of the threat.

ii. Examples of threat impact include:

i. A fire in the computer room that contains all ePHI repositories / systems would have a ***High*** impact. The fire may affect the availability of ePHI repositories / systems.

iii. The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability, and integrity of ePHI within an organization.

6. Determine the level of risk

i. For each threat and vulnerability to ePHI, calculate the level of risk of the associated threat.

ii. The level of risk is calculated by using the likeliness of a threat, as calculated in step 4 of the Risk Assessment procedure and the resulting impact of a threat, as calculated in step 5 of the Risk Assessment procedure.

iii. An example of calculating the level of risk for a threat include:

1. If the threat of a flood has been calculated with a likeliness of **High** and the impact of a flood has been calculated as **High,** then the associated level of risk would then be **High**.
2. If the threat of a power outage has been calculated as **Low** and the impact of a power outage has been calculated as **Medium,** then the associate risk level would be **Low**.

iv. The output of this process should be documentation of the level of risk associated with each threat and impact to the confidentiality, availability and integrity of ePHI within an organization.

7. Determine additional security measures needed to lower the level of risk

i. Based on the determination of the level of risk as defined in step 6 of the Risk Assessment procedure, additional security measures (safeguards / controls) may be needed to lower the risk.

ii. Examples of additional security measures needed include:

1. If the threat of a power outage has been calculated as **High** and the impact of a power outage has been calculated as **Medium,** then the associate risk level would be **High**. An additional security measure that may be implemented would be the installation of a backup generator to lower the likeliness of a power outage impacting any systems containing ePHI.

iii. The output of this process should be documentation of any additional security measures that are needed to lower the level of risk associated with each threat and impact to the confidentiality, availability, and integrity of ePHI within an organization.

8. Document the findings of the Risk Assessment

i. The final step in the Risk Assessment process is to document and publish all of the findings in each of the steps of the Risk Assessment procedure.

1.2 Risk Management

SAFEGUARD: Administrative
IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(1)(ii)(B)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 (a) [Risk analysis]."

1. WACBD shall implement security measures and safeguards for each ePHI repository sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. The level, complexity and cost of such security measures and safeguards must be commensurate with the risk classification of each such ePHI repository.

2. WACBD will reassess the potential risks and vulnerabilities of an ePHI repository as part of a periodic review; it must update the security measures and safeguards for such ePHI repository to reflect any changes in the risks and vulnerabilities assessment. At a minimum, the risk management process will include the following:

i. Assessment and prioritization, on the basis of risks, of each ePHI repository.
ii. Selection and implementation of reasonable, appropriate, and cost-effective security measures to manage, mitigate, or accept identified risks.
iii. Security training and awareness on implemented security measures to workforce members.
iv. Periodic evaluation and revision, as necessary, of the security measures.

Procedure

1. The Risk Management process will be based on the following steps
i. Risk Analysis – A Risk Analysis will be performed based on Risk Analysis policy (1.1).
ii. Risk Prioritization - Using information from the risk analysis, risks will be ranked on a scale (from high to low) based on the potential impact to information systems containing ePHI and the probability of occurrence.
iii. Cost-benefit analysis – An analysis shall identify and define the costs and benefits of implementing or not implementing the identified security methods.
iv. Safeguard selection – Safeguards shall be selected that are the most appropriate security methods to mitigate or manage identified risks to critical information systems and ePHI. Such selections will be based on the nature of specific risks and the feasibility, effectiveness, and cost of specific safeguards.
v. Assignment of responsibility – Appropriate workforce members will be identified and assigned responsibility for implementing and managing selected safeguards.
vi. Security method evaluation - Selected security safeguards will be regularly evaluated and revised, as necessary.
vii. The results of each of the above steps will be formally documented.

1.3 Sanctions for Noncompliance

SAFEGUARD: Administrative

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(1)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

1. WACBD acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI.
2. To ensure that all workforce members fully comply with Security Policies, WACBD will appropriately discipline and sanction employees and other workforce members for any violation of the HIPAA Security Policies and Procedures

Procedure

1. Security Violations that Prompt Consideration of Disciplinary Action
   i. Human Resources or a department / person with similar responsibilities may discipline a workforce member, who violates the HIPAA Security Rule
   ii. Human Resources or a department / person with similar responsibilities may also discipline managers or supervisors if their lack of diligence or lack of supervision contributes to a subordinate's Security Violation.

2. Investigation of Security Violation
   i. A workforce member who becomes aware of a Security Violation shall promptly communicate the report to the HIPAA Security Officer and his or her supervisor or Human Resources or a department / person with similar responsibilities.
   ii. After receiving a reported Security Violation, the HIPAA Security Officer or someone designated by him or her shall determine the facts and circumstances surrounding the violation and report the findings to Human Resources or a department / person with similar responsibilities.

3. Imposition of Discipline
   i. Human Resources or a department / person with similar responsibilities shall impose sanctions for a Security Violation in accordance with Human Resources policies.

4. Reporting of Security Violations
   i. The failure to report a known Security Violation could lead to discipline because each workforce member has an obligation to report any Security Violation of which the workforce member becomes aware to the HIPAA Security Officer and to his or her supervisor or the Human Resources Department or a department / person with similar responsibilities.

1.4 Information System Activity Review

SAFEGUARD: Administrative
IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(1)(ii)(D)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports."

1. Internal audit procedures shall be implemented to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
2. To ensure that system activity for all systems that contain ePHI is appropriately monitored and reviewed, the following procedures outlined below should be implemented.
   i. An internal audit procedure should be established and implemented to regularly review records of system activity. The internal audit procedure may utilize audit logs, activity reports, or other mechanisms to document and manage system activity.

1. Audit logs, activity reports, or other mechanisms to document and manage system activity should be reviewed at intervals commensurate with the associated risk of the information system or the ePHI repositories contained on each information system. The interval of the system activity review should not exceed, but may be less than, 90 days.

ii. An Audit Control and Review Plan should be created and approved by the HIPAA Security Officer. This plan should include:

1. Systems and Applications to be logged
2. Information to be logged for each system
3. Procedures to review all audit logs and activity reports
4. Security incidents such as activity exceptions and unauthorized access attempts should be detected, logged and reported immediately to the appropriate system management and HIPAA Security Officer in accordance with the HIPAA Security Policy #6 – Security Incident Procedures

3. A Risk Analysis as defined in Section 1.1 of the WACBD HIPAA Security Policy #1 - Security Management Policy should be performed annually but not more than every two years.

RELEVANT REFERENCES:

- HIPAA privacy rule:
  Privacy | HHS.gov
- HITECH Act:
  Health IT Legislation | HealthIT.gov

APPROVING COMMITTEE(S):

- Policy and Compliance Committee
- ISOutsource
-

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #2 **Administrative Safeguards** **Security Officer Policy**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 1/11/2023	**Next Review Date:** 1/11/2024
Policy contact: Privacy/ Security Officer	**Version: # 1**	

PURPOSE: Under the HIPAA Security Regulations, WACBD is required to designate a security official who is responsible for the development and implementation of its security policies and procedures.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI)

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such,* **WACBD** is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect **WACBD**'s commitment to complying with such Regulations. **WACBD** will comply with documented HIPAA policies and procedures unless specifically stated in the below policy**.**

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

2.1 Assigned Security Responsibility

SAFEGUARD: Administrative
TYPE: Standard
HIPAA HEADING: REFERENCE: 45 CFR 164.308(a)(2)
SECURITY REGULATION STANDARDS LANGUAGE:
" Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

1. WACBD acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI.
2. An individual will be assigned to assume responsibility for developing, implementing, maintaining, and monitoring adherence to WACBD security policies and procedures. This role is called the **HIPAA Security Officer.**

Procedure

1. The HIPAA Security Officer is responsible for:
   i. Ensuring that appropriate security measures and standards are implemented and enforced with regard to ePHI. The security measures implemented should be based on the criticality, sensitivity, and public or private nature of the data.
   ii. Review rights of authorized users of ePHI on a regular basis.
   iii. Review access and system logs for systems that contain ePHI.
   iv. Investigate and report on security problems and issues and refer such matters to the appropriate officials.
   v. Develop conditions of use or authorized use procedures for ePHI.
   vi. Provide training to regularly remind workers about their obligations with respect to information and ePHI security.
   vii.

APPROVING COMMITTEE(S):
Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #3 **Administrative Safeguards** **Workforce Security Policy**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 1/11/2023	**Next Review Date:** 1/11/2024
Policy contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of the policy is to ensure that all workforce members who need access to electronic Protected Health Information (ePHI) have the appropriate access while preventing all others from obtaining access to ePHI.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI)

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.
Safeguard	Defend, protect, shield, guard, safeguard as a means to keep secure from danger or against attack

Policy

3 Workforce Security Policy

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(3)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) [Information access management] of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information."

1. WACBD will ensure that only properly authorized workforce members shall have access to ePHI Systems. Workforce members shall not attempt to gain access to any ePHI that they are not properly authorized to access. WACBD shall train its workforce members on proper and appropriate use of access rights.
2. WACBD shall take reasonable and appropriate steps to ensure that workforce members who work with or have the ability to access ePHI are properly authorized and/or supervised.
3. WACBD workforce members shall be screened, as appropriate, during the hiring process.
4. WACBD shall implement a documented process for terminating access to ePHI when employment of workforce members ends or when access is no longer appropriate.

3.1 Authorization and Supervision

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(3)(ii)(A)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."

1. WACBD will take reasonable and appropriate steps to ensure that workforce members who have the ability to access ePHI or work in areas where ePHI might be accessed shall be properly authorized and/or supervised. WACBD will use a Minimum Necessary Policy, which is one of its HIPAA Privacy policies, and other policies as appropriate, as the basis for the type and extent of authorized access to ePHI.

Procedure

1. WACBD will implement procedures to ensure that only workforce members with a need to access ePHI are granted access to ePHI. No unauthorized access to ePHI will be allowed. (See HIPAA Privacy Policy Minimum Necessary)
2. WACBD shall maintain documentation detailing each workforce member's role and responsibilities, why such workforce member requires access to ePHI and the specific levels of ePHI access required by such workforce member.
3. WACBD shall ensure that all workforce members who work with ePHI are supervised so that unauthorized access to ePHI is avoided. (See HIPAA Security Policy #4 – Information Access Management).
4. ePHI data and sensitive labeled data shall be controlled by enrollment in security groups.

3.2 Workforce Clearance Procedure

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(3)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures to determine that the access of a workforce member to Electronic Protected Health Information (EPHI) is appropriate."

1. WACBD shall develop and implement procedures to ensure that the ePHI access of its workforce members is appropriate when granted and continues to be appropriate on an on-going basis. WACBD shall maintain documentation detailing each workforce member's current role and responsibilities and the ePHI access required for such role and responsibilities. (See HIPAA Security Policy #4 -- Information Access Management).

Procedure

1. Each WACBD supervisor will act as a system manager (person who is responsible for the access levels and permissions of a system) and shall perform an initial review for each system that uses ePHI to ensure that the current user list as well as the level of access for each user is appropriate. Each WACBD system manager should perform a subsequent review at least annually.
2. Each supervisor shall make appropriate changes when a workforce member's role changes so that the workforce member's access level can be adjusted promptly.
3. WACBD shall review prospective workforce members' backgrounds during the hiring process and, as appropriate, shall perform verification checks on prospective workforce members. WACBD shall analyze prospective workforce members' access to and expected abilities to modify or change ePHI as one of the bases for the type and number of verification checks conducted. Verification checks may include:

i. Confirmation of claimed academic and professional qualification
ii. Professional license validation
iii. Criminal background check
iv. Other state or federal database checks

3.3 Termination Procedure

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(3)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedure] of this section."

1. WACBD shall develop and implement procedures for terminating access to ePHI when the workforce member's employment ends or when the access granted is determined to be no longer appropriate. (See HIPAA Security Policy #4 – Information Access Management).

Procedure

1. The termination procedures should include the following steps:

i. A notification mechanism to ensure that the appropriate personnel are made aware that the workforce member's access to ePHI is no longer required.
ii. Recovery of all forms of access to PHI and ePHI that was granted or assigned to that workforce member. Examples include, but are not limited to, keys, remote access tokens, and identification badges.
iii. Disabling the workforce member's accounts on networks and system.
iv. Disabling remote access to networks and systems
v. Changing administrative or other shared passwords of which the workforce member has been made aware.

APPROVING COMMITTEE(S):

Policy and Compliance Committee

ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #4 **Administrative Safeguards** **Information Access Management**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 1/11/2023	**Next Review Date:** 1/11/2024
Policy contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of the policy is to describe the procedures that WACBD should establish and implement to ensure that access to ePHI is assigned and managed in a manner commensurate with the role of each workforce member.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy**.**

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Health Information Technology for Economic and Clinical Health Act (HITECH)	The HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009 is legislation that was created to stimulate the adoption of electronic health records (EHR) and the supporting technology in the United States. It is a part of the American Recovery and Reinvestment Act of 2009 (ARRA). Other than stimulating EHR adoption in the United States, the HITECH Act was passed to further expand data breach notifications and the protection of electronic protected health information (ePHI)
Minimum Necessary	The minimum necessary standard is a key protection of the HIPAA privacy rule. It is

	based on the practice that protected health care information should not be used or disclosed when it is not necessary to satisfy a particular purpose. This standard requires healthcare entities to limit unnecessary or inappropriate access to and disclosure of protected health information.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.
Safeguard	Defend, protect, shield, guard, safeguard as a means to keep secure from danger or against attack

Policy

WACBD acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI. §164.308(a)(4)(ii)(A) Isolating health care clearinghouse functions (Required).

4. Information Access Management Policy

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(4)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part."

Policy

WACBD ensures that users requiring access to ePHI have appropriate access and provides procedural safeguards to ensure that access to ePHI is properly restricted.

Standard

1. Procedures for Access Authorization should include the following:

i. Users must be authorized for the appropriate level of access that their position requires.

ii. Access to ePHI and systems that store or process ePHI requires a valid and authorized user account and password.

iii. Users are required to authenticate themselves to these systems using their unique user accounts.

4.1 Access Authorization

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(4)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."

Policy

WACBD implements procedures to establish, document, periodically review and modify if appropriate each users' rights to access ePHI.

Standards

1. Procedures for Access Authorization should include the following:

i. Each supervisor or manager is responsible for authorizing access to systems and networks containing ePHI for his or her subordinates. Users are not permitted to authorize their own access to ePHI or be granted authorization from another supervisor.

ii. Each supervisor or manager is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.

iii. Each supervisor or manager is responsible for periodically reviewing the access to ePHI granted to each of his or her subordinates and for modifying such access if appropriate.

4.2 Access Establishment and Modification

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(4)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."

Policy

WACBD follows documented process for establishing, documenting, reviewing, and modifying access to ePHI.

Standards

1. Procedures for Access Establishment and Modification include:

i. WACBD shall implement a procedure for establishing and documenting different access levels to ePHI. System managers must define access levels for accessing ePHI. These access levels must be communicated to all supervisors of workforce members.

ii. WACBD shall implement a procedure for documenting establishment of access to ePHI. All requests for access or modification of access must be done in writing (or electronic) and copies of the request must be kept for at least 6 years

iii. WACBD shall implement a procedure for reviewing on a regular basis workforce members' access privilege to ePHI.

iv. WACBD shall implement a procedure for modifying the access privileges of workforce members to ePHI, as appropriate, based on the periodic reviews.

APPROVING COMMITTEE(S):

Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #5 **Administrative Safeguards** **Security Awareness and Training**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 1/11/2023	**Next Review Date:** 1/11/2024
Policy contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of the policy is to develop a security awareness program that will train WACBD workforce members on how to reasonably protect and safeguard ePHI while allowing them to perform their job functions.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.
Safeguard	Defend, protect, shield, guard, safeguard as a means to keep secure from danger or against attack

Policy

5 Security Awareness and Training

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(5)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement a security awareness and training program for all members of its workforce including management."

1. All WACBD workforce members must receive security training on how to protect the confidentiality, integrity, and availability of ePHI. Workforce members will not be allowed to access ePHI until they are properly trained on how to protect and safeguard the ePHI. The security and awareness program will include the following:

i. Security reminders
ii. Procedures for guarding against, detecting and reporting malicious software
iii. Procedures for monitoring log-in attempts and reporting
iv. Procedures for creating, changing and safeguarding passwords

2. The WACBD Human Resources (HR) Manager will assign each workforce member required training upon hire and annually. The HR Manager will keep a log containing the name of the workforce member, job classification, training level required, date the training was completed and date the training log was last reviewed for that employee. The HR Manager will continually track workforce members' training in the log to ensure that training is completed in a timely manner and to reevaluate training needs when a workforce member's job function changes.

5.1 Security Reminders

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(5)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Periodic security updates."

1. WACBD must develop and implement procedures to ensure that periodic security updates are issued to the workforce on reminders of or changes to WACBD's HIPAA Security Policies.
2. WACBD must develop and implement procedures to ensure that warnings are issued to the workforce of potential, discovered, or reported threats, breaches, vulnerabilities, or other HIPAA security incidents. (See HIPAA Security Policy #6 -- Incident Response and Reporting).

Procedure

1. WACBD will periodically provide Security updates and reminders to its workforce on how to protect and safeguard ePHI.
2. Security updates and reminders may be in the form of emails, videos, face to face presentations, posters, or other methods to distribute the updates and reminders.
3. WACBD will provide Security updates when any of the following occur:

i. Significant changes to WACBD's HIPAA Security Policies and Procedures.
ii. Significant changes to safeguards or controls to protect ePHI.
iii. Substantial risks to systems that contain ePHI.

5.2 Protection from Malicious Software

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(5)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Procedures for guarding against, detecting, and reporting malicious software."

1. WACBD must develop and implement procedures for guarding against, detecting, and reporting to the appropriate persons, new and potential threats from malicious software such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

Procedure

1. WACBD will ensure that all systems will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions.
2. WACBD shall train its workforce members to identify and protect against malicious software. Periodic Security updates will be provided to all workforce members on how to identify and avoid malicious software.
3. WACBD shall notify its workforce members of new and potential threats from malicious software designed to interfere with the normal operation of a system or its contents and procedures.
4. WACBD's workforce members shall not try to bypass or disable the anti-virus / anti-malware software.

5.3 Log-in Monitoring
IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(5)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Procedures for monitoring log-in attempts and reporting discrepancies."

1. WACBD shall train its workforce members on monitoring Log-in attempts and reporting discrepancies that the workforce member becomes aware of.

Procedure

1. WACBD's workforce members should expect that all activity on systems that contain ePHI will be logged and recorded. In addition, all changes made to ePHI will be logged and recorded.
2. WACBD's workforce members should be trained on how to identify and report suspicious access activity on their workstations.
3. WACBD's workforce members should be trained on any limitations on the number of failed login attempts that are permitted. In addition, workforce members should be trained that failed Log-in attempts will be logged and recorded.

5.4 Password Management
IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(5)(ii)(D)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Procedures for creating, changing, and safeguarding passwords."

1. WACBD must train its workforce members on creating, changing, and safeguarding passwords in accordance with HIPAA Security Policy #14 - Access Control.

Procedure

1. WACBD workforce members should receive training on the password policy that is defined in HIPAA Security Policy #14 - Access Control.
2. WACBD workforce members should receive training on how to protect and safeguard passwords.

APPROVING COMMITTEE(S):

Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #6 **Administrative Safeguards** **Privacy and Security Incident Procedures**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 1/11/2023	**Next Review Date:** 1/11/2024
Policy Contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of the policy is to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

STATEMENT OF POLICY: Washington Center for Bleeding Disorders (WACBD) is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

6 Privacy and Security Incident Procedures

TYPE: Standard

REFERENCE: 45 CFR 164.308(a)(6)(i)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to address security incidents."

1. WACBD will develop and document a procedure for identifying, responding to and reporting of all privacy and security incidents against ePHI or other critical systems.

6.1 Reporting and Response

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(6)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

1. WACBD acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI.
2. WACBD will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of ePHI will be reported and responded to.
3. WACBD shall have a Privacy and Security Incident Response Team ("IRT") charged with the responsibility of identifying, evaluating, and responding to privacy and security incidents. The HIPAA Privacy and Security Officers shall oversee the activities of the IRT.

Procedure

1. WACBD will maintain an Incident Response Plan to achieve requirements set forth in this policy.
2. WACBD IRT will be responsible for investigating all known or suspected privacy and security incidents to systems containing ePHI or other critical systems.
3. WACBD will document a procedure for all workforce members to follow to report security incidents. See **Security Incident Response Log.**
4. WACBD will ensure that all workforce members receive training on how to identify and report privacy and security incidents.
5. All workforce members must follow the documented procedure to report privacy and security incidents. In addition, workforce members must report all known or suspected privacy and security incidents.
6. All workforce members must assist the IRT with any privacy or security incident investigations.

6.2 Breach Determination

The Privacy and Security Incident Response Teams (IRT) will investigate all reported and suspected privacy and security breaches. The following guidelines will help determine if a privacy or security incident would be considered a breach as defined by the HIPAA Privacy, Security and Omnibus rules:

1. An acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy or Security rules is presumed to be a breach unless WACBD or a business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
iii. Whether the protected health information was actually acquired or viewed; and
iv. The extent to which the risk to the PHI has been mitigated.

6.3 Breach Notification

Following the discovery of a breach of unsecured PHI, WACBD will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

I. Date of discovery

A breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

II. Timeliness of notification

WACBD will provide the required notifications without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

III. Content of notification

A notification will be provided to each individual affected by the discovered breach. The notification should include the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps patients should take to protect themselves from potential harm resulting from the breach;
- A brief description of what WACBD is doing to investigate the breach, to mitigate harm to patients, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
- The notification should be written in plain language.

IV. Methods of notification

The following methods should be used to notify individuals affected by the discovered breach:

i. Written notice

Written notification by first-class mail to the patient at the last known address of the individual or, via e-mail if the patient agrees to e-mail notice. The notification may be provided in one or more mailings as information is available.

If the patient is deceased notifications will be sent to next of kin or personal representative

ii. Substitute notice

If contact information is out of date and written notification cannot be made, a substitute notification can be used.

- If contact information is out of date for fewer than 10 individuals, the substitute notification may be provided by an alternative form of written notice, telephone, or other means.
- If contact information is out of date for more than 10 individuals, the substitute notification may be in the form of either a conspicuous posting for a period of 90 days on the home page of WACBD's Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The notice should include a toll-free contact phone number that remains active for at least 90 days.
- In any case deemed to require urgency because of possible imminent misuse of unsecured PHI, notification may be provided to individuals by telephone or other means, as appropriate, in addition to notice defined above.

V. Notification to media

In addition to notifying individuals of a known breach, a notification to the media is required if the breach involves more than 500 residents of a State or jurisdiction. The notification should occur no later than 60 days after the breach discovery.

VI. Notification to Health and Human Services (HHS)

WACBD will notify HHS of a discovery of a known breach. The timing of the notification will be the following:

- For breaches involving 500 or more individuals a notification to HHS will occur no later than 60 days after the date of discovery.

- For breaches involving fewer than 500 individuals a notification to HHS will occur no later than 60 days after the end of each calendar year. All breaches involving fewer than 500 individuals in the calendar year will be reported to HHS 60 days after the end of each calendar year.

  HHS has given guidance to breach notification on their website:
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

VII. Notification by business associates

Breaches discovered by business associates will be reported to a covered entity without delay and no later than 60 calendar days after discovery of the breach.

6.4 Testing

The contingency procedures outlined in the Incident Response plan. shall be tested on a periodic basis.

Security Incident Response Log

Incident Identification Information	
Name:	
Phone:	
Email:	
Date/Time Detected:	
System / Application Affected:	
Incident Summary	
Type of Incident Detected: (Denial of Service, Malicious Code, Unauthorized Access, Unauthorized Use / Disclosure, Unplanned System Downtime, Other)	
Description of Incident:	
Names of Others Involved:	
Incident Notification	
How Was This Notified? (Security Office, IT Personnel, Human Resources, Other)	
Response Actions Include Start and Stop times	
Identification Measures (Incident Verified, Accessed, Options Evaluated):	
Containment Measures:	
Evidence Collected (Systems Logs, etc.):	

APPROVING COMMITTEE(S):

Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision

Revision			
Revision			

HIPAA Security Policy #7 **Administrative Safeguards** **Contingency Plan**	**Department:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of the policy is to plan for operational contingencies in the event of a disaster or emergency and to ensure that ePHI is protected during the disaster or emergency.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

7 Contingency Plan

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(7)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."

1. WACBD must develop documented procedures to respond in the event an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including:

i. Data Backup Plan
ii. Disaster Recovery Planning
iii. Emergency mode operation plan
iv. Testing and Revision Procedures

7.1 Data Backup Plan

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(7)(ii)(A)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

1. WACBD shall establish and implement Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all ePHI that is stored on all WACBD computer systems.
2. The Data Backup Plan will apply to all systems that contain ePHI that WACBD has operational control of.
3. The Data Backup Plan shall apply to all files, records, images, voice or video files that may contain ePHI.
4. The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
5. If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement shall be used to ensure that the Business Associate or Contractor will safeguard the ePHI in an appropriate manner.
6. Data backup procedures outlined in the Data Backup Plan shall be tested on a periodic basis to ensure that exact copies of ePHI can be retrieved and made available.

Procedure

1. WACBD will develop and implement procedures to ensure that daily backups and exact and retrievable copies are made of all systems that contain ePHI.
2. The Data Backup Plan will apply to all systems that contain ePHI that WACBD has operational control of.
3. WACBD will develop a list of systems that contain ePHI or that contain critical information and ensure that each of the systems are included in the daily backup.
4. WACBD will ensure that periodic tests are performed to ensure the daily backups are valid, contain retrievable information and can be restored in the event of a disaster or emergency.
5. WACBD will develop and implement a procedure to define restoration steps in the event data needs to be restored from backup.
6. WACBD will ensure that any media used for the daily backup will be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
7. Data encryption should be used to safeguard any ePHI on the daily backups.

7.2 Disaster Recovery Plan

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.308(a)(7)(ii)(B)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish procedures to restore any loss of data.

1. To ensure that WACBD can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing ePHI, WACBD shall establish and implement Disaster Recovery Plan pursuant to which it can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner.
2. The Disaster Recovery Plan will apply to all systems that contain ePHI that WACBD has operational control of.
3. The Disaster Recovery Plan should include training and security reminders to all workforce members.

Procedure

1. The Disaster Recovery Plan should include procedures to restore ePHI from data backups in the case of a disaster causing data loss.
2. The Disaster Recovery Plan should include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.
3. The Disaster Recovery Plan shall always be documented and easily available to the necessary personnel.

7.3 Emergency Mode Operation Plan

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.308(a)(7)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."

1. WACBD shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
2. The Emergency Mode Operation Plan will apply to all systems / processes that WACBD has operational control of.

Procedure

1. WACBD will define what constitutes and triggers an Emergency that would require an Emergency Mode Operation Plan.
2. The Emergency Mode Operation Plan will apply to all systems / processes that WACBD has operational control of.
3. The Emergency Mode Operation Plan shall include detailed steps on how workforce members will react to emergencies that impact the confidentiality, integrity, and availability of ePHI.
4. The Emergency Mode Operation Plan shall include steps that outline security processes and controls to ensure the confidentiality, integrity, and availability of ePHI.
5. The Emergency Mode Operation Plan shall be documented and easily available to the necessary personnel at all times.
6. The Emergency Mode Operation Plan should include training and security reminders to all workforce members.

7.4 Testing and Revision Procedures

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(7)(ii)(D)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures for periodic testing and revision of contingency plans."

1. The Contingency procedures outlined in the Disaster Recovery and Emergency Operations Plans (Contingency Plan) shall be tested on a periodic basis.
2. Any necessary revisions or updates to the Contingency Plans shall be made.

Procedure

1. Testing of Contingency Plan should be performed at least annually.
2. Any necessary revisions that are identified during the Contingency Plan testing will be made to the Contingency Plans.

7.5 Application and Data Criticality Analysis

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.308(a)(7)(ii)(E)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Assess the relative criticality of specific applications and data in support of other contingency plan components.

1. WACBD shall assess the relative criticality of specific applications and data for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.
2. The Application and Data Criticality Analysis will apply to all systems / processes that WACBD has operational control of.
3. The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Procedure

1. WACBD will, at least annually, identify the relative criticality of each system that may or may not contain ePHI in relation to patient care.
2. The list of critical systems will be used to prioritize which systems to concentrate on when implementing the Contingency Plan.

APPROVING COMMITTEE(S):

Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #8 **Administrative Safeguards** **Evaluation of Security Policies and Procedures**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of the policy is to define the procedures that will ensure that each Security Policy adopted by WACBD is periodically evaluated for technical and non-technical viability**.**

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

STATEMENT OF POLICY: Washington Center for Bleeding Disorders (WACBD) is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, **WACBD** is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect **WACBD**'s commitment to complying with such Regulations. **WACBD** will comply and periodically evaluate documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy
8 Evaluation

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(8)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

1. WACBD acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI.
2. WACBD Policies initially should be evaluated to determine its compliance with the HIPAA Security Rule. Once compliance with the HIPAA Security Rule is established, the WACBD Security Policies should be evaluated on a periodic basis to assure continued viability in light of technological, environmental, operational or regulatory changes that could affect the security of ePHI.

Procedure

1. WACBD HIPAA Security Officer shall periodically (at least annually) evaluate its HIPAA Security Procedures to ensure that such Procedures maintain their technical and non-technical viability and continue to comply with any Regulatory Policies.
2. The results of the periodic security evaluation shall be documented and retained through a self-assessment workbook.
3. In the event that one or more of the following events occur, the policy evaluation process should be triggered:

i. Changes in the HIPAA Security Regulations or Privacy Regulations.
ii. New federal, state, or local laws or regulations affecting the privacy or security of PHI or ePHI.
iii. Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Security Procedures.
iv. A serious security violation, breach, or other security incident occurs.

4. Any changes to Security Policies or Procedures shall be communicated to all workforce members.

APPROVING COMMITTEE(S):
Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #9 **Administrative Safeguards** **Business Associate Contracts**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/13/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of the policy is to cover all Business Associates that create, receive, maintain, or transmit ePHI on WACBD's behalf. WACBD will develop and implement contracts that ensure the Business Associate will appropriately safeguard the information in compliance with the HIPAA Security Rule.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

9 Business Associate Contracts

TYPE: Standard

REFERENCE: 45 CFR 164.308(b)(1); 45 CFR 164.308(b)(4)

SECURITY REGULATION STANDARDS LANGUAGE:

"A covered entity, in accordance with § 164.306 [Security standard: General rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a)[Business Associate contracts and other arrangements] that that the business associate will appropriately safeguard the information."

1. WACBD acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI.
2. At times ePHI may be disclosed to and used by Business Associates (BA) or subcontractor as necessary to allow the BA or subcontractor to carry out a healthcare related function or activity on behalf of WACBD or to provide services to WACBD. A BA or subcontractor must sign a Business Associates Agreement (BAA) with WACBD, in order to access, use or disclose ePHI. The BAA must be in writing and must contain the requirements of the Security Rule and authorized signatures.

Procedure

1. The HIPAA Security Officer shall ensure that all Business Associates or subcontractors enter into Business Associate Agreements that contain the requirements of the Security Rule.
2. Each Business Associate Agreement shall state that the Business Associate will:

i. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on WACBD's behalf.

ii. Ensure that any agent, including a subcontractor to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it.

iii. Report to WACBD any security incident of which it becomes aware.

iv. Authorize the termination of the Business Associate Agreement by WACBD if WACBD determines that the Business Associate has violated a material term of the contract.

APPROVING COMMITTEE(S):

Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #10 **Physical Safeguards** **Facility Access Controls**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to define the procedures that will limit physical access to electronic information systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorder (WACBD) is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures in regards to physical and electronic access to its facilities unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

10 Facility Access Controls

TYPE: Standard

REFERENCE: 45 CFR 164.310(a)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

1. WACBD shall create and maintain a Facility Security Plan that outlines and documents its procedures to safeguard all facilities, systems, and equipment used to store ePHI against unauthorized physical access, tampering, or theft. The Facility Security Plan will include:

i. Contingency Operations Plans
ii. Facility Security Plans
iii. Access Control and Validation Plans
iv. Maintenance Records

10.1 Contingency Operations

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(i)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency."

1. WACBD will create procedures that ensure access to facilities by appropriate personnel during Disasters or Emergency Operations. These procedures will be incorporated into the respective Contingency Operations Plan (See HIPAA Security Policy#7 – Contingency Plan)
2. The Contingency Operations Plan will apply to all systems / processes that WACBD has operational control of.

Procedure

1. WACBD shall implement procedures to allow facility access in the event of an emergency, disaster, or other occurrence resulting in lost data:

i. WACBD will take reasonable and appropriate steps to secure any location that contains PHI or ePHI. WACBD workforce members will take reasonable and appropriate steps to continue to protect PHI and ePHI.
ii. WACBD will permit access to all workforce members involved in the repair of electronic information systems and in the restoration of lost data in accordance with the Emergency Mode Operation Procedures and Disaster Recovery Procedures (see HIPAA Security Policy #7 -Contingency Plan)
iii. WACBD Management and/or HIPAA Security Officer shall see that WACBD'S workforce members involved in Emergency Mode Operation Procedures and Disaster Recovery Procedures (see HIPAA Security Policy #7 - Contingency Plan) have access to rooms and areas containing any back-up data stored on-site or off-site.

10.2 Facility Security Plan

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."

1. WACBD will implement procedures to safeguard facilities and equipment from unauthorized physical access, tampering, and theft.
2. The Facility Security Plan will apply to all systems / processes that WACBD has operational control of.

Procedure

1. WACBD shall ensure that all network servers, application servers, routers, database systems, device management system hardware, and other servers are located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.
2. WACBD will ensure that only appropriate and authorized personnel have access to facilities housing operations related systems.
3. Any other workforce members requiring access to facilities housing WACBD operations-related electronic information systems shall request and receive permission from the HIPAA Security Officer.

i. Such access shall only be granted on a need-to-know basis.
ii. The HIPAA Security Officer shall log the names of personnel who have requested and been granted access to the facilities containing WACBD electronic information systems.

10.3 Access Control and Validation Procedures

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(iii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."

1. WACBD will take reasonable and appropriate steps to control and validate physical access to facilities containing ePHI Systems.
2. The Access Control and Validation Procedures will apply to all facilities that WACBD has operational control of.

Procedure

1. WACBD will implement procedures to control and validate a person's access to facilities based on their role or function:

i. Access to highly sensitive areas that contain ePHI will only be granted on a need-to-know basis and based on a legitimate business need.
ii. All access to areas that house systems that contain ePHI will be tracked and logged. Logs will contain at a minimum: person's name, company, date of entry, time of entry, duration, and reason for entry.
iii. Guests of WACBD should not be given access to areas that house systems that contain ePHI.
iv. Patients should only be permitted in common areas and should not be given access to areas that house systems that contain ePHI.

10.4 Maintenance Records

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.310(a)(2)(iv)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)."

1. WACBD management will be responsible for overseeing those repairs and modifications to the physical components of the facility, which are related to security (for example, hardware, walls, doors and locks), are completed and documented with WACBD Executive Management and the Landlord. Documented information should include the following:

i. The equipment or component where maintenance has been performed
ii. The date maintenance was performed
iii. A description of the Maintenance performed
iv. The WACBD'S workforce member(s) or contractor who performed the maintenance.

2. Maintenance Records Procedures will apply to all facilities that WACBD has operational control of.

APPROVING COMMITTEE(S):

Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Appendix: Facility Security Plan (FS Plan being finalized per actual procedures performed by WACBD & ISO)

HIPAA Security Policy #11 **Physical Safeguards** **Workstation Use and Workstation Security**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to provide policies and specifications on workstation use that include documented instructions and procedures defining the proper functions to be performed and the manner in which those functions are to be performed in order to maximize the security of ePHI. As well as to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store ePHI to ensure that appropriate security is maintained, and that access is restricted to authorized workforce members.

SCOPE: The Scope of this policy applies to all WACBD employees both in office and including remote locations.

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information	Protected Health Information (PHI) stored, processed or transmitted electronically.

(ePHI)	

Policy

11 Workstation Use

TYPE: Standard

REFERENCE: 45 CFR 164.310(b)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected health information.

1. To ensure that workstations, smartphones, and other computer systems that may be used to send, receive, store or access ePHI are only used in a secure and legitimate manner, all workforce members must comply with the WACBD Acceptable Use Policy that includes the Computer Use Policy.
2. WACBD will provide workstations and other computer systems to workforce members for the purpose of performing their job functions for WACBD. Workforce members shall be responsible for using workstations appropriately in conformance with this Policy.
3. When an employee retires, resigns, or is terminated, WACBD will remove or deactivate any workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.
4. Workforce members must be assigned and use a unique User Identification and Password (See HIPAA Security Policy #14 - Access Control)
5. Workforce members that use WACBD' information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, WACBD may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information system assets

Procedure

1. Create acceptable use policy that specifies proper computer usage per HIPAA regulations.

APPROVING COMMITTEE(S):

Policy and Compliance Committee
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #12 **Physical Safeguards** **Workstation Security**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store ePHI to ensure that appropriate security is maintained and that access is restricted to authorized workforce members.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

12 Workstation Security

TYPE: Standard

REFERENCE: 45 CFR 164.310(c)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."

1. WACBD will implement a Workstation Security Plan for all systems that store, access or transmit ePHI that WACBD has operational control of.

Procedures

1. WACBD will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices including laptops, smartphones, CD-ROMs, DVDs, USB Drives, etc. that store or access ePHI.
   i. Workstations and laptops that are in common areas that store or access ePHI should be physically placed with the monitor so that it prohibits unauthorized people from viewing confidential information such as logins, passwords or ePHI.
   ii. Workstations and laptops that are in common areas that store or access ePHI should utilize privacy screens to prevent unauthorized access to ePHI.
   iii. Portable devices and media including laptops, smartphones, CD-ROMs, DVDs, USB Drives, data backup tapes, etc. that contains ePHI should utilize encryption to protect the ePHI.
   iv. Portable devices and media should be concealed when from view when offsite to prevent theft.
   v. All network servers, application servers, routers, database systems, device management system hardware, and other servers should be located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel. (See HIPAA Security Policy #10 – Facility Access Controls).
   vi. All workstations, servers and portable devices will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions. Workforce members must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Workforce members must not disable these tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.
   vii. All workstations, servers and portable devices, where feasible, must implement a security patch and update procedure to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
2. WACBD will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices from misuse and physical damage, vandalism, power surges, electrostatic discharge, magnetic fields, water, overheating and other physical threats.
   i. Workstations must not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions should also be taken to ensure that workstations cannot be affected by problems caused by utilities, such as water, sewer and/or steam lines that pass through the facility.
   ii. All facilities that store systems that contain ePHI, should have appropriate smoke and/or fire detection devices, sprinklers, or other approved fire suppression systems, and working fire extinguishers in easily accessible locations throughout the facility.
   iii. All servers that contain ePHI, should be connected to an Uninterrupted Power Supply (UPS) to prevent server crashes during power outages or spikes. Servers should be configured to shut down in a controlled manner if the power outage is for an extended period of time.
   iv. All systems should be connected to surge protectors, where feasible, to protect against power spikes and surges.
3. A user identification and password authentication mechanism shall be implemented to control user access to the system. (See HIPAA Security Policy #14 - Access Control).
4. Workforce members suspecting any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to the HIPAA Security Officer.

APPROVING COMMITTEE(S):

Policy and Compliance Committee

ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #13 **Physical Safeguards** **Device and Media Controls**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy Contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to define the policy and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility; and the movement ePHI within the facility; and to implement methods to properly dispose of ePHI.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

13 Device and Media Controls

TYPE: Standard

REFERENCE: 45 CFR 164.310(d)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility."

1. WACBD will develop policies and procedures that govern receipt, removal, movement and disposal of hardware and electronic media containing ePHI within the facility. The policies and procedures will address device and media controls relating to:

i. Disposal
ii. Media Re-use
iii. Accountability
iv. Data Backup and Storage

13.1 Disposal

IMPLEMENTATION TYPE: Required

REFERENCE: 45 CFR 164.310(d)(2)(i)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

1. WACBD must take reasonable and appropriate steps to dispose of portable devices and media that contain ePHI. Removal steps must ensure that ePHI is properly copied off of the device and that destruction of ePHI prevents unauthorized access to the ePHI.
7. The Media Disposal procedure will apply to all systems that contain ePHI that WACBD has operational control of.

Procedure

1. Prior to destroying or disposing of any portable device or media, care must be taken to ensure that the device or media does not contain ePHI.
2. If the portable device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to disposal.
3. If the portable device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data. Note that a data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI.
3. HIPAA Security Officer or delegate will notify the Information Technology (IT) department/company/individual of equipment that needs to be disposed of.
4. HIPAA Security Officer or delegate will determine data sensitivity of data to be disposed of. (See Data Classification Table below)
5. IT will assess the condition of the equipment, they will:

a. IT will track the disposal of the device (type of hardware, serial number, etc). See Appendix
b. IT will run approved wiping software on all devices to make sure all patient information is removed from the device. This may include physical destruction (See Methods of Destruction below)
c. IT will verify the hardware's data has been removed
d. IT will dispose of the hardware

6. HIPAA Security Officer or delegate / IT will document the destruction of the asset and keep a record. See Appendix C: Media Disposal Log
7. If taken to outside facility - The media shall be taken to an approved, certified facility for erasure or destruction. A letter of certification regarding date and time of erasure/destruction shall be obtained.

Data Classification Table:

1. **Low (Unclassified)** - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.

- Basic operating system, personal files,

2. **Medium (Sensitive)** - Erase the data using any means such as reformatting or degaussing.

- Business related information that does not contain patient information (ePHI).

3. **High (Confidential)** - The data must be erased using an approved technology to make sure it is not readable using special technology techniques. (See method of destruction below)

- Media contains patient information (ePHI).

Examples of hardware devices include:

- Workstation
- Laptop
- Tablet (iPad/Android)
- Smartphones
- Server hard drives
- Memory stick (USB drives)
- CD ROM disk / DVD ROM
- Storage / Backup tape(s)
- Hard drives
- Copiers / Scanners / Fax machines
- X-Rays / Ultrasound / Diagnostic Machines
- Any other hardware that contains ePHI

Methods of Destruction Table:

Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. A data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI. Overwriting cannot be used for media that are damaged or not rewriteable.)
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. Disintegration, Pulverization, Melting, and Incineration. These sanitization

	methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm).

13.2 Media Re-use

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.310(d)(2)(ii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."

1. WACBD must take reasonable and appropriate steps to ensure that portable device and media do not contain ePHI prior to re-use the device or media. If the device or media does contain ePHI then steps must be taken to ensure that the ePHI is properly destroyed prior to re-use of the device or media.
2. The Media Re-use procedure will apply to all systems that contain ePHI that WACBD has operational control of.

Procedure

1. Prior to making a portable device or media available for reuse, care must be taken to ensure that the device or media does not contain ePHI.
2. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to reuse.
3. If the portable device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse. A typical reformat is not sufficient as it does not overwrite the data. Note that a data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI
4. The use of a data destruction tool before reuse is not required if the media is used for system or data backup, as long as the media is stored and transported in a secured environment.

13.3 Accountability

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.310(d)(2)(iii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

1. When using portable devices or media to transport ePHI, a procedure must be developed to track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.
2. The Media Accountability procedure will apply to all systems that contain ePHI that WACBD has operational

control of.

Procedure

1. A log should be maintained of any hardware containing ePHI that has been received into or removed from WACBD's facilities. The log should note the workforce member receiving or removing the equipment, the date of receipt or removal, the person approving the receipt or removal, and the date the hardware was returned. (See Appendix A Receipt of Hardware or Electronic Media Containing ePHI Log and Appendix B Removal of Hardware or Electronic Media Containing ePHI Log).

13.4 Data Backup and Storage

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.310(d)(2)(iv)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

1. Before moving any systems that contain ePHI, a procedure must be developed to ensure that the ePHI is properly backed up and secured prior to moving.
2. The Media Data Backup procedure will apply to all systems that contain ePHI that WACBD has operational control of.

Procedure

1. If a system contains ePHI, all files containing ePHI must be backed up to a computer, tape, USB drive, CD-ROM, disk, or other storage media before equipment is moved within or outside of WACBD facilities.
2. The backed-up data should be stored in a secure area until it is placed on different equipment or restored to the original equipment from which it was removed.

APPROVING COMMITTEE(S):
Policy and Compliance Committee (PCC)
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #14 **Technical Safeguards** **Access Control**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy Contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to assure that systems containing ePHI are accessed only by those persons or software programs that have been granted access rights under the HIPAA Security Policy #4 – Information Access Management.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

14 Access Control

TYPE: Standard
REFERENCE: 45 CFR 164.312(a)(1)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

WACBD ensures that access to ePHI is only permitted to authorized persons for the duration and purpose to complete required data management.

Standard

1. All workforce members must be assigned a unique user identifier (i.e. userid) that allows for workforce member identification and tracking of access to ePHI.
2. Emergency access procedures that enable authorized workforce members to obtain access to necessary ePHI during a disaster or other emergency.
3. Automatic Logoff procedures protect ePHI from unauthorized access while workforce members are utilizing systems that access ePHI.
4. The use of encryption where it is reasonable and appropriate to protect ePHI.
5. All networks that contain systems that access or store ePHI should be protected by a network firewall.

14.1 Unique User Identification

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.312(a)(2)(i)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Assign a unique name and/or number for identifying and tracking user identity."

Policy

WACBD tracks all activities for all ePHI systems via unique user identity.

Standard

1. Workforce members will be assigned a unique user identification (i.e. user id) in order to access any system or application that transmits, receives or stores ePHI.
2. Each workforce member must ensure that their assigned user identification is appropriately protected and only used for legitimate access to systems or applications.
3. If a workforce member believes their user identification has been comprised, they must report the security incident. (See HIPAA Security Policy #6-- Incident Response).
4. Workforce members should be aware of the following password procedures to create and use strong passwords to protect ePHI. The passwords requirements are stated in the InfoSec Handbook
5. Workforce members should be aware of the following procedures to protect passwords:

i. Passwords should not be written down
ii. Passwords should not be shared with other workforce members
iii. If a workforce member suspects that their passwords has been compromised, they should report the incident immediately

6. Passwords should be changed at least every 90 days

7. After a number of failed password attempts, the workforce member's account should be disabled (e.g. 3 or 5 failed attempts)
8. Multi-Factor (MFA) shall be implemented as much as possible on all systems.
9. Multi-Factor (MFA) shall be implemented for remote access, administrators, and third parties.
10. All terminated/separated workforce members will have access revoked immediately.
11. All third-party must be disabled when not in use and only enabled as necessary.

14.2 Emergency Access Procedure
IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 164.312(a)(2)(ii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Establish procedures for obtaining necessary electronic protected health information during an emergency."

Standard

1. WACBD ensures that the Disaster Recovery and Emergency Operations plans include steps to enable authorized workforce members to obtain access to necessary ePHI during a disaster or other emergency. (See HIPAA Security Policy#7 – Contingency Planning)
2. WACBD trains workforce members on the Disaster Recovery and Emergency Operations Plan (See HIPAA Security Policy#7 – Contingency Planning)

14.3 Automatic Logoff
IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.312(a)(2)(iii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

Standard

1. Systems that access or store ePHI implement an automatic logoff after a determined 10 minutes of inactivity. Users need to be identified and authenticated again to regain access and continue the session.

2. Users are trained that when leaving a server, workstation, or other computer system un-attended, they must lock or activate the system's automatic logoff mechanism (e.g. CTRL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing ePHI.

14.4 Encryption and Decryption
IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.312(a)(2)(iv)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement a mechanism to encrypt and decrypt electronic protected health information.

Policy

WACBD encrypts data when possible to protect and safeguard ePHI.

Standard

1. Workforce members are trained on the use of encryption to protect ePHI when ePHI is being transmitted outside of WACBD.

2. All portable devices and media that contain ePHI are encrypted to protect ePHI in the event that they are lost or stolen.
3. All backup tapes and media that contain ePHI are encrypted to protect ePHI.
4. WACBD implements secure encrypted remote access procedures to protect systems that access or store ePHI
   i. Authentication and encryption mechanisms should be required for all remote access sessions to networks containing ePHI. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and encrypted Citrix client access.
5. WACBD implements secure encrypted wireless access procedures to protect systems that access or store ePHI.
   i. All wireless access to WACBD networks should utilize encryption mechanisms.
   ii. All encryption mechanisms implemented to comply with this policy should support a minimum of 128-bit encryption.

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #15 **Technical Safeguards** **Audit Controls Policy**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to define the hardware, software and/or procedural mechanisms that will be implemented by WACBD to record and examine activity in information systems that contain or use ePHI.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

15 Audit Controls

TYPE: Standard

REFERENCE: 45 CFR 164.312(b)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

1. WACBD should implement audit mechanisms to track and audit access to systems that contain or use ePHI.
   i. Each system containing ePHI shall utilize a mechanism to log and store system activity.
   ii. Each system's audit log shall include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.
   iii. System audit logs shall be reviewed on a regular basis. (See HIPAA Security Policy #1 – Security Management).
   iv. Security incidents such as activity exceptions and unauthorized access attempts should be detected, logged, and reported immediately to the appropriate systems management and the HIPAA Security Officer in accordance with the HIPAA Security Policy #6 - Security Incident Procedures.
2. The Audit Control procedure will apply to all systems that contain ePHI that WACBD has operational control of.

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #16 **Technical Safeguards** **Integrity Policy**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to define the appropriate data authentication measures that WACBD shall implement to ensure that ePHI is not improperly altered or destroyed.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

16 Integrity

TYPE: Standard

REFERENCE: 45 CFR 164.312(c)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

1. WACBD will implement procedures to ensure that ePHI is not improperly altered or destroyed.
2. The Integrity procedure will apply to all systems that contain ePHI that WACBD has operational control of.

Procedure

1. WACBD will implement mechanisms to protect ePHI from alteration or destruction by Malicious Software such as a virus or malware. (See HIPAA Policy#11 – Workstation Security).
2. WACBD will implement mechanisms to protect ePHI integrity during storage and use, including the use of data redundancy (i.e., Redundant Arrays of Inexpensive Disks [RAID] configurations) and error-correcting memory.

16.1 Mechanism to Authenticate ePHI

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(c)(2)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."

1. WACBD must implement mechanisms to validate that ePHI has not been altered or destroyed in an unauthorized manner.

Procedure

1. WACBD will take steps to ensure that, when reasonable and appropriate, electronic mechanisms are implemented to validate the integrity of ePHI by proving that it has not been improperly altered or destroyed. Examples of electronic mechanisms that are capable of detecting and reporting unauthorized alteration or destruction of ePHI include:
   i. Checksum
   ii. Hash values
   iii. Digital signatures
   iv. Encryption
   v. Disk redundancy (such as Redundant Arrays of Inexpensive Disks or "RAID").
2. The use of electronic mechanisms to ensure that ePHI has not been altered or destroyed will be determined by the HIPAA Security Officer

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			

Revision			

HIPAA Security Policy #17 **Technical Safeguards** **Person or Entity Authentication Policy**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy Contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to define the procedures to be implemented by WACBD to verify that a person or entity seeking access to ePHI is the person or entity claimed.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

17 Person or Entity Authentication

TYPE: Standard
REFERENCE: 45 CFR 164.312(d)
SECURITY REGULATION STANDARDS LANGUAGE:

"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

3. WACBD will implement authentication mechanisms to ensure the authenticity of a person or entity prior to granting access to ePHI.

Procedure

1. All workforce members of WACBD are provided a unique username and password for all systems containing ePHI. (See WACBD HIPAA Security Policy #14 - Access Control Policy*)*.
2. Workforce members will select a password in accordance with WACBD HIPAA Security Policy #14 - Access Control Policy.
3. Workforce members of WACBD must not use another person's account to access any system. If a workforce member requires access to a system, they must gain access using an account in their own name. If new or additional access to a system is required, the procedures outlined in WACBD HIPAA Security Policy #4 - Information Access Management must be followed.
4. If a workforce member becomes aware that someone has improperly obtained his or her username and password or has improperly accessed WACBD electronic system through the use of the username and password, the workforce member shall immediately report the incident (See HIPAA Security Policy #6 – Security Incident Procedures).
5. Elevated or Privileged accounts are created for users requiring administrative access to all system. This includes configurations, restricted utilities, and systems management.
6. Least privilege access will be enforced.
7.

APPROVING COMMITTEE(S):
Policy and Compliance Committee (PCC)
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

HIPAA Security Policy #18 **Technical Safeguards** **Transmission Security Policy**	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 09/15/2022	**Effective Date:** 01/18/2023	**Next Review Date:** 01/18/2024
Policy Contact: Privacy/Security Officer	**Version:** # 1	

PURPOSE: The purpose of the policy is to define the technical security measures that WACBD will implement to guard against unauthorized access to or modification of ePHI that is being transmitted over an electronic communications network or via any form of removable media.

SCOPE: The scope of this policy applies to all WACBD employees, business processes and systems that store, process or transmit Electronic Protected Health Information (ePHI).

POLICY STATEMENT: Washington Center for Bleeding Disorders (WACBD) is a *Covered Entity* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, WACBD is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect WACBD's commitment to complying with such Regulations. WACBD will comply with documented HIPAA policies and procedures unless specifically stated in the below policy.

DELEGATION OF RESPONSIBILITIES: WACBD can delegate some or all of its responsibilities under this policy to ISOutsource, WACBD's IT Managed Services Provider.

DEFINITIONS:

Term	Definition
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entity	Any health plan, healthcare clearinghouse, or any healthcare provider who transmits Protected Health Information (or PHI as per the standards developed by the Department of Health & Human Services) in electronic form.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.
Healthcare Insurance Portability and Accountability Act (HIPAA)	A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.
Protected Health Information (PHI)	Individually identifiable health information (IIHI) held or transmitted by a covered entity or business associate in any form or media including electronic, paper, and oral, that identifies the patient or could reasonably be used to identify the patient
Electronic Protected Health Information (ePHI)	Protected Health Information (PHI) stored, processed or transmitted electronically.

Policy

18 Transmission Security Policy

TYPE: Standard

REFERENCE: 45 CFR 164.312(e)(1)

SECURITY REGULATION STANDARDS LANGUAGE:

"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

1. WACBD will implement procedures to reasonable protect ePHI against unauthorized access while being transmitted over an electronic communications network. Measures to protect ePHI include:

i. Implementing Integrity Controls

ii. Data Encryption

18.1 Integrity Controls

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(e)(2)(i)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

1. WACBD will implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

Procedure

1. The use of Secure Sockets Layer (SSL) should be utilized when accessing or transmitting ePHI to or from any website.
2. Transmission of ePHI via other methods should use secure and encrypted mechanisms to safeguard and protect ePHI.

18.2 Encryption

IMPLEMENTATION TYPE: Addressable

REFERENCE: 45 CFR 164.312(e)(2)(ii)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement a mechanism to encrypt protected health information whenever deemed appropriate."

1. WACBD will implement data encryption procedures where it is reasonable to protect and safeguard ePHI. Encryption should be utilized when:

i. Transmitting ePHI to outside entities

ii. Stored on Portable Devices and Media

iii. Sent via Email or messaging systems

iv. Sent over wireless networks

Procedure

1. WACBD will utilize encryption to protect and safeguard ePHI when sending to entities that are outside of the WACBD's network. The file, document, or folder containing ePHI should be encrypted before transmission.
2. WACBD should utilize encryption when transmitting ePHI on Portable Devices or Media. Portable Devices and Media include but are not limited to Laptops, Tablets, USB Drives, CD-ROMs, DVDs, Floppy Drives and (Backup) Tapes.
3. WACBD will utilize encryption when sending ePHI via email or messaging systems.

i. WACBD should not send ePHI via email or messaging systems if encryption has not been implemented.

4. WACBD will utilize secure encrypted wireless networks to transmit ePHI.

i. WACBD'S workforce members should not access ePHI when using public non-encrypted wireless networks.

ii.

APPROVING COMMITTEE(S):
Policy and Compliance Committee (PCC)
ISOutsource

REVISION HISTORY

	Final Approval by	Date	Brief description of change/revision
Revision			
Revision			

Appendix 1

About this Notice

This Notice of Privacy Practices is NOT an authorization. This Notice of Privacy Practices describes how we, our Business Associates, and our Business Associates' subcontractors, may use and disclose your protected health information (PHI) to carry out treatment, payment, or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information.

"Protected Health Information" is information about you, including demographic information, that may identify you and that relates to your past, present, or future physical or mental health condition and related health care services.

We are required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and other applicable laws to maintain the privacy of your health information, to provide individuals with this Notice of our legal duties and privacy practices with respect to such information, and to abide by the terms of this Notice. We are also required by law to notify affected individuals following a breach of their unsecured health information.

WACBD safeguards the privacy of the comprehensive health care services provided to all patients receiving care, including interactions with payors, clearinghouses, partners, business associates and other healthcare professionals.

WACBD's practice is to protect the privacy of all medical information about a patient or identifying a patient. WACBD reserves the right to change its privacy practices and apply the revised practices to PHI previously created or received and has described how it will provide individuals with a revised notice.

Medical information is defined as: medical services provided to a patient, payment information, and information about a patient's past, present and future, medical history and/or condition.

Grievance (Complaints):

Any patient has the right to file a complaint if they believe WACBD have violated HIPAA. Any patient or representative on patient's behalf may submit a written or verbal complaint to the privacy officer regarding breach of a patient's privacy at WACBD without fear of jeopardizing their care. Patients will not suffer retaliation of any kind for filing a complaint.

Electronic correspondence should be sent to PG@wacbd.org or verbally by calling 206-614-1200 and speaking with the Privacy Officer.

Patients also have the right to file a complaint with the OCR

Patients have the options of:

- The OCR Complaint Poral at: U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)
- By Mail Print and mail the completed complaint and consent forms (found at HIPAA Complaint Process | HHS.gov) to:
  Centralized Case Management Operations
  U.S. Department of Health and Human Services 200 Independence Avenue, S.W.
  Room 509F HHH Bldg.
  Washington, D.C. 20201
- By email to OCRComplaint@hhs.gov

Effective: 09/28/2022

WACBD, at the Washington Institute for Coagulation

Notice of Privacy Practices

THIS NOTICE OF PRIVACY PRACTICES ("NOTICE"), DESCRIBES HOW WE MAY USE OR DISCLOSE YOUR PROTECTED HEALTH INFORMATION AND HOW YOU MAY ACCESS TO SUCH INFORMATION. PLEASE READ CAREFULLY.

Contact Information:
701 Pike Street, Suite 1900 Seattle WA, 98101
Phone: (206) 614-1200

Contacting Patients

WACBD intends to contact individuals for:

- providing appointment and refill reminders,
- for treatment, case management, care coordination
- communicate about a drug or biologic currently prescribed
- describing or recommending treatment alternatives, providing information about health-related benefits, products and services that may be of interest to the individual,
- describing plan benefits

Patient Rights

Patients have the right to the following concerning their privacy:

- Right to a copy of this Notice
- Right to review and receive a copy of medical information
- Right to request disclosures WACBD has made up to 6 years prior
- Right to request restrictions on disclosures
  - WACBD is not required to agree to a requested restriction EXCEPT when a disclosure to a health plan is for 1) carrying out payment or health care operations and is not otherwise required by law, and 2) the PHI pertains solely to a health care item or service.
- The right to receive confidential communications of PHI
- Right to request an alternative method of communication
- Right to notification of breach of medical information

WACBD Engagement

WACBD intends to engage in:

- A health plan or health insurance issuer if PHI may be disclosed to a plan sponsor, with the exception of disclosing PHI that is genetic information for such purposes
- fundraising communications, with the right to opt out.

Use of Appropriate Disclosure:

- WACBD may disclose medical information about a patient internally and to an outside healthcare professional to provide treatment and to coordinate or manage healthcare services provided.
- WACBD may disclose medical information to obtain payment for healthcare services provided. Meaning, we may use medical information to arrange payment, prepare bills, and to manage accounts. We may also disclose medical information about you to others, such as insurers.
- WACBD may disclose medical information as required by law to do so. There are federal, state, and local laws requiring the disclosure of medical information. This disclosure includes worker's compensation.
- WACBD may disclose information about you when performing business activities for the improvement of quality of care, such as:
  - Reviewing and evaluating the skills, qualifications, and performance of healthcare providers taking care of you.
  - Providing training programs for fellows, other healthcare providers or non-healthcare professionals for practice and professional development.
  - Compliance with outside organizations and government agencies that evaluate, certify or license healthcare providers, staff, or facilities.
  - Reviewing and improving the quality and efficiency of care provided to patients.
  - Planning for our organization's future operations.
  - Resolving grievances within WACBD.
  - Reviewing activities and using or disclosing medical information to make significant changes for the benefit of patients.
  - Working with outside entities such as attorneys, accountants and other providers who assist WACBD with compliance of this notice and other applicable laws.
  - Right to notification of breach of medical information.

WACBD
WASHINGTON CENTER FOR BLEEDING DISORDERS

Other Permitted and Required Uses and Disclosures That May Be Made Without Your Authorization. These situations include:

Public Health: We may disclose your protected health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. For example, a disclosure may be made for the purpose of preventing or controlling disease, injury, or disability.

Communicable Diseases: We may disclose your protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Legal Proceedings: We may disclose protected health information during any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), or in certain conditions in response to a subpoena, discovery request or other lawful process.

Law Enforcement: We may also disclose protected health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of our practice, and (6) medical emergency (not on our practice's premises) and it is likely that a crime has occurred.

Appendix 2

Authorization to Release Personal Health Information (PHI)

This form is for use when such authorization is required and complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Standards.

Patient Information:

Print Name of Patient: _____
(Include all other name changes, e.g., maiden, etc.)

Date of Birth: _____

Street Address: _____

City, State, Zip Code: _____

Home/Cell Phone: _____

Email Address: _____

Release Information to or Discuss Information with:

Health Care Provider/Facility/Family Member or Friend:

_____

Street Address: _____

City, State, Zip Code: _____

Phone: _____

Email Address: _____

Send a copy of released records either by U.S. Mail, Fax, or Encrypted Email

Please send all medical records including lab reports from the most recent two years or date range specified, or specify exactly what information is to be shared below.

_____

_____

_____

Date Range: _____ to _____

Patient Authorization

Information released may include information regarding the testing or diagnosis of HIV/AIDS or sexually transmitted diseases. I hereby give my authorization for this information to be released.

I authorize the Washington Center for Bleeding Disorders to release information regarding my patient history diagnosis or treatment to the organization or person listed above.

I have the right to revoke my authorization at any time in writing to the Washington Center for Bleeding Disorders' Medical Director. Signed authorizations will expire 1 year from the date of signing.

Once disclosed, this medical health information may be subject to re-disclosure by the recipient and may no longer be protected under health information privacy laws.

Signature – Patient/Guardian/Authorized Representative Date

(*Documentation may be required to verify signature authority*)

Form Submission

Please submit the signed form via the following ways:

- ○ U.S. Mail to the Washington Center for Bleeding Disorders, 701 Pike Street, Ste. 1900, Seattle, WA 98101
- ○ Fax to (206) 614-1178
- ○ Email to info@wacbd.org

If you have any inquiries, please call the Washington Center for Bleeding Disorders' Office at (206) 614-1200

Appendix 3
Data Use Agreement for Disclosures of Limited Data Sets

This Data Use Agreement ("Agreement") is between ORGANIZATION, ("Covered Entity") and _____ ("Recipient"). This Agreement is effective on _____ (date).

WHEREAS, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its associated regulations at 45 C.F.R. Part 160 and 164 (Privacy Rule) requires a Data Use Agreement in connection with the disclosure of a limited data set (LDS) by Covered Entity to Recipient;

WHEREAS, Recipient conducts research, performs public health activities, or performs health care operations using protected health information (PHI) in a LDS as defined by the HIPAA Privacy Rule regulations at 45 C.F.R. 164.514(e);

WHEREAS, Covered Entity wishes to provide to Recipient PHI in a LDS for the purposes of research, public health activities, or health care operations;

THEREFORE, in consideration of the above requirements, the parties agree:

1. RESPONSIBILITIES OF RECIPIENT

   a. Recipient shall use or disclose the LDS from Covered Entity only for purposes of: _____.

   b. Recipient represents and warrants that only the following individuals or groups will use or disclose the LDS received from Covered Entity for purposes described above:
   _____
   _____
   _____

   c. Recipient agrees that any agents, including any subcontractor, to whom it provides the LDS shall agree to the same restrictions and conditions contained in this Agreement for its use of the LDS.
   d. Recipient shall use appropriate safeguards to prevent any use or disclosure of the LDS not specified by this Agreement.

   e. Recipient agrees not to perform any of the following actions:

      i. Attempting to identify or contact any individual whose health information is included in the LDS.
      ii. Using or further disclosing the information in the LDS for any purpose other than the purpose specified in section 1.a of this Agreement or as otherwise permitted by law.
      iii. Publishing or otherwise disclosing information that identifies the individuals whose health information is included in the LDS.

   f. Recipient agrees not to use or permit others to use information from the LDS that identifies an entity or individual health care provider for any of the following purposes:

      i. To compete commercially against an entity.
      ii. To determine the rights, benefits, or privileges of an entity or individual health care provider.
      iii. To report, through any medium, information that identifies an entity or individual health care

provider.

g. Recipient agrees not to use, or permit others to use, information from the LDS for purposes not specified by this Agreement in Section 1.a.
h. Recipient shall report to Covered Entity any use or disclosure of the LDS that is not specified by this Agreement.

2. RESPONSIBILITIES OF COVERED ENTITY

a. Covered Entity shall provide PHI to Recipient as a LDS in the following format and medium: _____.
b. Covered Entity shall include in its Notice of Privacy Practices that it may disclose PHI for the purposes of research, public health activities, and health care operations.

3. GENERAL

a. This Agreement may be terminated:

i. By Covered Entity on material breach by Recipient, provided:
1. Covered Entity gives Recipient written notice of the breach, and
2. Recipient fails to cure the breach within thirty (30) days of receipt of such written notice. Covered Entity may agree to extend the time for Recipient's cure of the breach.
ii. By either party upon thirty (30) days written notice to the other, or
iii. In a written agreement signed by both parties.

b. The responsibilities of Recipient described in Section 1 of this Agreement shall survive termination of this Agreement.

c. This Agreement shall be governed and interpreted in accordance with the laws of the State of _____.

d. This Agreement may not be assigned by Recipient without the prior express written consent of the Covered Entity.

e. None of the terms of this Agreement are intended to create, nor shall be construed to create, any relationship between the parties other than that of independent entities contracting with each other solely for the purpose of transferring an LDS.

IN WITNESS WHEREOF, the parties have executed this Agreement on the effective date stated above.

Recipient

Signed by: _____ Date _____

Print or Type Name: _____

Title: _____

Organization: _____

Address: _____

City: _____ State: _____ Zip: _____

Covered Entity

Signed by: _____ Date _____

Print or Type Name: _____

Title: _____

Organization: _____

Address: _____

City: _____ State: _____ Zip: _____

Appendix 4
Patient Request for Confidential Communications

Patient Name: _____ Birth Date: _____ /_____/_____

Telephone Number: _____ E-mail: _____

I understand I have the right to request that WACBD communicate with me in an alternative manner and/or location regarding my protected health information as defined in the Health Insurance Portability and Accountability Act of 1996. I understand that WACBD will accommodate my request if:

1. The request is reasonable.
2. The request clearly states that a failure to honor could endanger me (the patient);
3. The request provides reasonable alternative means or location for communications; and
4. The request provides a satisfactory explanation of how any payments (if applicable) will be addressed using the alternative means or location.

This is a: _____ New Request _____ Change to Prior Request_____ Withdrawal of Prior Request

I request that WACBD accommodate the request for confidential communications for the following specific health information:

_____

_____

_____

I request that WACBD use the following methods/means of communication and locations for contact:

_____ Delivery Address: _____

_____ Telephone: _____

_____ Other: (Specify) _____

By signing this form, I am confirming that it accurately reflects my wishes.

_____ _____/_____/_____
Signature Date

If signed by personal representative:

Name of personal representative: _____

Relationship to participant or nature of authority: _____

_____ _____/_____/_____
Signature of Personal Representative Date