WACBD
WASHINGTON CENTER
FOR BLEEDING DISORDERS

Acceptable Use Policy	**Departments:** Pharmacy, Clinical, Billing/Contracts, Finance/ Accounting, Research, General Operations	
Origination Date: 9/14/2022	**Effective Date:** 4/19/2023	**Next Review Date:** 4/19/2024
Policy Contact: Privacy/Security Officer	**Version:** #1	

PURPOSE: The purpose of this policy is to define rules for acceptable use of WACBD Information Technology systems by WACBD employees, vendors and contractors.

SCOPE: All WACBD Information Technology Systems.

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 HIPAA policies and procedures unless specifically stated in the below policy.

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.
Information Technology Systems	A computer-based system including servers, workstations, networks, software and other components used to store, process and transmit data in electronic form.
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, 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.
Electronic Protected Health	Protected Health Information (PHI) stored, processed or transmitted electronically.

Information (ePHI)	

User Responsibilities

WACBD established this policy for the protection of WACBD information technology networks and information resources. Each authorized user is personally responsible for protecting all confidential information used and/or stored under their security access which includes: the user's logon IDs, passwords, and the hardware used to access WACBD's systems. Furthermore, users are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons.

Users of WACBD information systems and workstation assets should not expect that their workstation use is private. 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.

Workforce Security

- Only authorized users shall have access to any WACBD information systems and associated processes. Users shall not attempt to gain access to any system that they are not properly authorized to access. (Security Policy #3)
- Users shall not tamper with any computer systems. This is especially important for security systems including anti-spam/anti-malware.

Data Protection

- Access to information systems is restricted to authorized users with a need-to-know.
- Information systems users must utilize WACBD systems solely for the purposes for which they were granted access.
- Only WACBD owned devices, or devices approved in WACBD's Bring Your Own Device Policy, may be used for client related data transmission.
- All information systems users are expressly forbidden from accessing, or from attempting to access, any data or programs for which they do not have authorization or explicit consent.
- In the event that an information systems user is sent or inadvertently accesses files that contain information that the user does not have a "need to know," or authority to receive, the user is required to immediately secure the material from view and notify their supervisor.
- Patient-related files are considered as "Client Confidential." Please refer to the Data Classification Program for instructions on working with "Client Confidential" data.
- Company-related files are considered as "Company Confidential." Please refer to the Data Classification Program for instructions on working with "Company Confidential" data.
- Information systems users are forbidden from making copies of any data from any Company information system or device unless approved by management. Normal work duties, workflows, and deliverables are automatically approved by management.
- Data outside of an employee's job description may not be removed, transported, or transmitted from the Company without the specific and expressed approval of their manager or HIPAA Security Officer or Privacy Officer.
- Pictures or videos of information systems and/or data may not be taken without the specific and expressed permission of the HIPAA Security Officer or Privacy Officer.
- Do not send ePHI data via unencrypted email, unless specifically requested by patient and documented, or unless utilizing WACBD's internal encryption email domains.

User Passwords

- Information systems users are required to log in using their assigned username and password regardless of the workstation or device being used. Every user is responsible for any and all actions performed that are associated with their network or application account.
- It is important to protect login credentials from disclosure. Users must not share or disclose their user account(s), passwords, personal identification numbers (PINs), security tokens, or similar information or devices used for identification and authorization purposes.
- Users must not circumvent password entry with auto-login, embedded scripts, or hard-coded passwords in client software.
- Users must not use any WACBD password for personal applications, including email and social media accounts.
- Workforce members should be aware of the following password procedures to create and use strong passwords to protect ePHI. User Password controls must adhere to the following:
    - Minimum length of 8 characters
    - Must not use Simple passwords (Complexity) - Must contain at least 3 of the following character classes:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphabetic characters (for example, !, $, #, %)
    - Expire every 90 days
    - Disallow reuse of the previous password

Resource Management

Computer Clean Desk Requirements

Clean Desk Requirements apply to the following data classifications

- Restricted Data – HIPAA, Client Confidential
- Proprietary Data – Company Confidential

Clean Desk Requirements are assured by the following:

- Computing devices must not be left unattended without enabling a password protected screen saver, locking the workstation, or completely logging off or powering off the device. All users should log out of ePHI systems when not actively using them.
- All users must protect documents, removable storage media, and information displayed on screens in their work areas to prevent unauthorized access to information, especially when such work areas are unattended.
- All desks and cabinets are to be locked at night or the office space they reside in must be locked.

Systems Monitoring

WACBD has the right and capability to monitor electronic information created and/or communicated by system users on the WACBD computer systems and networks, including e-mail messages and usage of the Internet. It is not WACBD's policy or intent to continuously monitor all computer usage by authorized users, however, users of the systems should be aware WACBD may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and users' electronic files and messages to the extent required by regulations and what WACBD believes is necessary to ensure that the Internet and other electronic communications are being used in compliance with WACBD's polices. Please keep in mind that this includes any device connected to WACBD's Wi-Fi.

Security Training

All users must complete HIPAA and InfoSec Program training upon hire and at least annually thereafter.

Security Violation

Users who become 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. (Security Policy 1, 1.3)

Sanctions for Non-Compliance

To ensure that all workforce members fully comply with Security Policies, WACBD will appropriately discipline and sanction users and other workforce members for any violation of the HIPAA Security Policies and Procedures

Technology Systems

General Systems

The following policies on computer, the Internet and electronic mail usage shall be observed by all WACBD Users.

- Users of the Internet and e-mail are to comply with all appropriate laws, regulations and generally accepted Internet etiquette.
- Primary purpose of the Internet and e-mail is to conduct official business. Accessing the internet can increase the risk to WACBD's systems and should generally be used for business-related purposes only. All authorized users of WACBD systems should be aware of the potential risk to WACBD and should only access those sites on the internet that they have a reasonable belief to be legitimate.
- Users should identify themselves properly when using the Internet and e-mail, conduct themselves professionally, and be aware that their activities reflect on the reputation and integrity of all WACBD's Users.
- Each user is individually responsible for the content of any communication sent over or placed on the Internet and e-mail.
- All Users have a responsibility to ensure a respectful workplace. WACBD equipment must not be used to visit Internet sites that contain pornographic or sexually explicit information, pictures, or cartoons.
- Exceptions to this policy are only allowed when pre-approved by the department head and deemed necessary for official WACBD business, research or investigatory work.

The following actions are prohibited. It is unacceptable for WACBD Users to:

- Knowingly or intentionally publish, display, transmit, retrieve or store inappropriate or offensive material on any department computer system.
- Create or distribute defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material.
- View or distribute obscene, pornographic, profane, or sexually oriented material.
- Violate laws, rules, and regulations prohibiting sexual harassment.
- Place advertisements for commercial enterprises, including but not limited to, goods, services, or property.
- Download, disseminate, store, or print materials including articles and software, in violation of copyright laws.
- Download any software, including but not limited to games, screen savers, toolbars, or any other browsing tools without the permission of Managed IT Service Provider ISOutsource.
- Violate or infringe on the rights of others.
- Use company assets for personal gain.
- Communicating ePHI and other sensitive information using unsecure/unapproved methods.
- Restrict or inhibit other users from using the system or the efficiency of the computer systems.
- Cause congestion or disruption of networks or systems, including distribution of chain letters.
- Transmit incendiary statements, which might incite violence or describe or promote the use of weapons.
- Use the system for any illegal purpose or contrary to WACBD policy or business interests.
- Connect a personal computer to the WACBD network without having the computer checked by Information

Services to ensure no threatening viruses / programs infect the WACBD network. Personal devices are allowed to be connected to guest networks provided by WACBD for customer use.

- Monitor or intercept the files or electronic communications of other users or third parties.
- Hack or obtain access to systems or accounts they are not authorized to use.
- To disclose a Login ID(s) or password to anyone nor allow anyone to access any information system with someone else's Login ID(s) or passwords
- Use other people's Login ID(s) or passwords to access any information system for any reason.
- Post any patient information on social network sites, public forums, etc.
- Remove WACBD's facilities electronic media that contains Protected Health Information (PHI) or confidential or proprietary WACBD information unless such removal is authorized by a user's supervisor and the user signs out the media in accordance with the WACBD HIPAA Security Device and Media Controls Policy.

Application Security

- Before an application can be installed on any of the WACBD systems or employees/contracted employees work devices, the application must be evaluated and approved by the Managed IT Service Provider - ISOutsource or designee to ensure that it meets minimum security requirements.
- Applications must be able to support access privileges adequate for the classification level of the information being handled.
- Applications, upgrades, and enhancements to be installed on information systems must follow the WACBD change control process.
- Information systems users must not make unauthorized copies of copyrighted software.

Workstation Security

- For the purposes of this policy, the term "Workstation" applies broadly to all laptops, desktops, and similar computing devices.
- All workstations must use encrypted storage (e.g. Hard Drive).
- All workstations must be set to lock the screen after no more than fifteen minutes of idle time.
- All workstations must have firewalls enabled and configured to prevent unauthorized access.
- All workstations must be running up to date and active antivirus and antimalware protection.
- All workstations must be running and have active the WACBD's standard remote monitoring and management application.
- All computers will run anti-virus/anti-malware software.
- Only use company systems (Outlook, Teams, or similar) to communicate electronically with the customer.
- Changes to the operating systems (other than regular updates) will not be allowed.
- Patient or company data may not be stored or transported on non-approved removable media, such as CDs, DVDs, USB or other portable drives.
- No Restricted Data (HIPAA, Client Confidential) or Proprietary Data (Company Confidential) information shall be stored on mobile device See WACBD's Bring Your Own Device Policy for more information.

Remote Access for the Microsoft M365 Environment Security

- All users are granted access to the Microsoft Office 365 environment.
- Only company owned equipment (desktops, laptops, mobile devices) are authorized to access Microsoft 365 environment.

Remote Access to CPR+

- Remote access users must be authorized by the Pharmacy Director.
- Only authorized equipment (desktops, laptops, mobile devices) can access CPR+.

Use of mobile devices for access to WACBD systems

- See WACBD's Bring Your Own Device Policy for more information.

Mobile Devices Security

- Mobile device users are subject to all Acceptable Use requirements contained herein.
- All mobile devices must be kept current on the latest 2 versions of its operating system.
- Mobile device locks must be protected by a four-digit pin or stronger and/or biometric controls.
- Mobile devices will be configured with screen savers or screen locks that protect the screen after 2 minutes.
- Mobile device users are responsible for ensuring the devices are secured and properly stored at all times.
- Lost or stolen portable devices must be reported to the HR and Managed IT Service Provider - ISOutsource immediately.
- All mobile devices shall always run the standard Mobile Device Management software.
- Mobile devices must use authorized messaging apps.
- Mobile devices must not be "rooted", "jailbroken", or running custom or modified operating systems, ROMs, Firmware, or Bootloader.

Telecommuter/Mobile Device Policy

- Telecommuters and users of company issued mobile devices and approved mobile devices, are required to keep their laptops and other work devices secured at all times.

Use of Wireless Networks for Remote Access to WACBD Systems

- Only trusted wireless networks are authorized to be used for access to any WACBD system, including access via VPN.
- Users must not access the VPN from networks not controlled by WACBD or other trusted entity, including home wireless networks.
- Public hotspots (e.g. hotel or airport Wi-Fi) that are not password protected are not considered trusted and must not be used for access to any WACBD systems.
- When no trusted Wireless network is available, users can use their cell phone, or company Hotspot to connect to the Internet via cable or by enabling WiFi hotspot on their cell phone.
- These requirements are subject to regular auditing, both of the remote computer's configuration and of session activity, time, and duration at the central location.

Incident Detection and Reporting

- Information systems users should immediately notify their supervisor, the COO, and Managed IT Service Provider - ISOutsource if there is any suspicion or cause for concern about the safety and security of customer or Company information or information systems.
- In the event malware is suspected:
  - Immediately contact a member of the Information Technology team.
  - Do not continue to use the device
  - Do not turn off the device
  - Make no attempt to remove the malware

- Any Users who abuse the privilege of their access to e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.
- Any Users will immediately report to the WACBD Privacy Officer of any activity that violates this agreement.

RELEVANT REFERENCES:

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

APPROVING COMMITTEE(S):

Policy and Compliance Committee (PCC)
ISOutsource

REVISION HISTORY

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