Applies to: All OSUWMC Workforce

## Overview of Policy

Information in any of its forms, as well as supporting processes, systems and networks, are valuable business assets that are essential to OSUWMC. As such, adequate mechanisms must be in place to protect them from a variety of threats and to facilitate the continuity of operations, minimize business risk, and maximize return on investments and business opportunities. The purpose of this document is to establish the policies by which OSUWMC follows in order to help ensure the confidentiality, integrity and availability of information.

## Definitions

| Term | Definition |
|---|---|
| **OSUWMC** | All hospitals of The Ohio State University, all hospital-based Ambulatory Clinics and all OSU Wexner Medical Center locations (located on or off the main Medical Center campus). |
| **Personal** | Explicitly belonging to the individual; not purchased using OSUWMC funds or grants awarded. Including but not limited to BYOD (Bring Your Own Device), smart devices, IoT (Internet of Things) devices. |
| **OSUWMC Data; data** | Any information in electronic format stored, transmitted or received by OSUWMC |
| **Information Assets** | Devices and systems used to store, transmit or receive OSUWMC data; assets include but are not limited to: servers, workstations, laptops, portable hard drives and USB drives, tablets, smartphones, etc. |
| **Workforce** | Employees, faculty, staff, students, consultants, volunteers, trainees, affiliates, and other persons whose conduct, in the performance of work for the Health System, is under the direct control of the Health System, whether or not they are paid by the Health System. |
| **Third Party** | Persons and/or vendors performing work duties on behalf of the Medical Center, whether or not they are paid by OSUWMC; Persons performing work duties for any entity that, under written agreement between the entity and OSUWMC, has access to OSUWMC data. |
| **Restricted Data** | Data protected or regulated by law or critical to university operations including sensitive personal information such as intellectual property, protected health information, student records, and credit card numbers |
| **Two-factor authentication** | Authentication that takes into account two of the following three aspects: (i) something only the user knows, e.g. static password, code, personal identification number; (ii) something only the user possesses,e.g.token, smart card, mobile phone; (iii) something the user is, e.g. biometric characteristic, such as a fingerprint. |
| **Privileged User Accounts** | System user accounts that allow additional access and/or functionality beyond what a normal end user receives; Typically includes system administration functions and/or access to expanded datasets |

## Policy Details

The detailed policy statements below define The Ohio State University Wexner Medical Center position and exceptions regarding information security. Where a standard exists that supports policy details, compliance with the policy will be measured by compliance with the standard. Unless otherwise noted in this policy, OSUWMC is to follow OSU Information Security Control Requirements as defined in the Information Risk Management Framework.

1) Acceptable Use Details
   a) Any information created, disseminated or stored using OSUWMC information systems is the property of OSUWMC

1) There is no right to privacy and employees should not have an expectation of privacy regarding such information

b) OSUWMC reserves the right to, at any time and without notice, access, read, review, monitor and copy all messages and files on its computer systems, as it deems necessary
c) OSUWMC may, as it deems necessary, disclose information from its computer system to law enforcement or other third parties without the employee's consent
d) OSUWMC Information systems prohibits engaging in any illegal activity or knowingly violate any laws and regulations
e) Any storage, dissemination, use or transmission of OSUWMC data requires prior approval
   i) Approval may be in the form of organizationally approved standard processes and technologies or ad hoc requests to the identified data owners.

2) Management Security
   a) The OSUWMC Chief Information Security Officer is designated as the official to be responsible for the development, implementation and maintenance of the OSUWMC Information Security Program including information security policies, standards and other supporting documentation.
   b) OSUWMC must have defined governance and operational processes that facilitate the effective, consistent and on-going management of information security risks.
      i) Governance
         1) OSUWMC must establish a governance structure that oversees the management of information security risk.
         2) OSUWMC must establish criteria to clearly define acceptable levels of risk and expectations for the appropriate treatment of the risk.
         3) Risk Acceptance
            (a) The acceptance of risk and corresponding rationale must be documented and periodically reviewed to ensure accuracy and applicability as relevant changes in the environment or organization occur.
      ii) Information Risk Management
         1) OSUWMC must establish processes to accurately and thoroughly assess the potential risks to the confidentiality, integrity and availability of information.
         2) Risk assessments must be performed regularly and as needed based on changes to the environment including the addition of new systems and applications and changes to those systems.
      iii) Compliance Management
         1) OSUWMC must develop measures to monitor and ensure compliance with information security policies and standards. OSUWMC Workforce members, business processes, information systems, and system access must be regularly checked for compliance with security implementation standards.
      iv) Third Party Risk Management
         1) Any Third Party or Partner with whom OSUWMC may potentially exchange data or allow connectivity to OSUWMC infrastructure must be assessed for risk, and the risk effectively managed to an acceptable level.
         2) Third Party or Partner risk must be continuously managed by providing adequate and consistent processes and controls for risk assessment, monitoring, treatment and acceptance.
            (a) Information Security requirements for third parties and partners must be included in contract language.

3) Legal, Regulatory and Contract Security
   a) OSUWMC must comply with all relevant statutory, regulatory and contractual requirements related to the security of information. OSUWMC must explicitly define, document and maintain its compliance approach.

4) Human Resources Security
   a) OSUWMC must develop, maintain, and enforce standards to ensure that Workforce members are adequately vetted prior to obtaining access to Information Assets.

5) Facilities Security

a) Building Security
   i) OSUWMC must provide physically and environmentally secure environments to house and protect Information Assets, including systems and information, from hostile external influence by establishing multiple physical and environmental security perimeters. These environments, or secure areas, must prevent unauthorized physical access, damage and interference to the organization's premises and information.
b) Workspace Security
   i) OSUWMC must protect Information Assets, onsite and offsite, by establishing standards and procedures to mitigate the risks associated with unauthorized physical access, loss or damage from physical or environmental causes.

6) Disaster-Related Security
   a) OSUWMC must create and document a disaster recovery plan(s) to recover its information systems if they are impacted by a disaster. The plan(s) must be reviewed regularly and revised as necessary.

7) Network Access
   a) OSUWMC must implement appropriate security measures on network devices and systems. Access to and across the network, both internally and externally, must be appropriately controlled, monitored and segregated.
      i) Only authorized users must deploy or modify network equipment
   b) Remote Access
      i) OSUWMC must develop and enforce remote access management processes and technologies which facilitate secure system access from external networks. Remote access will be reviewed and granted as required by the business.
      ii) Remote access to systems containing Restricted Data must require strong authentication (e.g., two-factor or other OSUWMC-approved authentication).

8) Identity-Related Security
   a) User Access Management
      i) OSUWMC must develop and enforce formal user access management procedures that, at a minimum:
         1) Uniquely identify users;
         2) grant and maintain access on a need-to-know basis, and;
         3) remove access in a timely manner when no longer needed.
   b) Authentication and Passwords
      i) OSUWMC must require users to authenticate when accessing OSUWMC systems, information, infrastructure or other Information Assets.
      ii) OSUWMC passwords must not be shared with anyone other than to whom they were assigned.
      iii) Use of another individual's account and password is prohibited.
      iv) Passwords must meet minimum password complexity requirements for strong passwords.
   c) Privileged User Accounts
      i) OSUWMC must develop and enforce formal procedures to manage privileged user accounts.
      ii) Privileged access is only granted to authorized users and must only be used for authorized functions.

9) Threat and Vulnerability Management
   a) OSUWMC must develop processes and implement systems that enable the prevention, timely identification, and remediation of vulnerabilities to Information Assets, including but not limited to: malware, patching, intrusion detection/prevention systems, and vulnerability scanning.

10) Segregation of Duties
   a) Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized access, modification, or misuse of OSUWMC assets.

11) Development Process-Related Security
   a) OSUWMC must develop and enforce formal systems development life cycle processes to address the confidentiality, availability and integrity of information.

b) Development environments must be maintained separately from production environments and must not contain Restricted Data
c) OSUWMC developers must receive formal secure software training on a regular basis.

12) Information Asset Management
a) OSUWMC must achieve and maintain protection of its Information Assets by assigning responsibility to appropriate owners. The responsibilities of an asset owner include the inventory and protection of assets.
b) Inventory
All Information Assets must be clearly identified and monitored.

13) Institutional Data-Related Security
a) Encryption
i) All Computing Devices or Media, connecting to or storing data from the OSUWMC network, must be encrypted with an enterprise managed solution or other OSUWMC approved strong encryption product.
ii) All OSUWMC Private and Restricted Data must be encrypted when transmitted over the Internet, Wireless Networks or other NON-OSUWMC Trusted networks
b) Information Classification
i) OSUWMC must have documented information classification standards that define approved data owners with authority to approve data usage requests.
ii) OSUWMC must have documented information handling and protection standards that define acceptable handling and protection controls specific to the classification of the information.

14) Security Incident Management
a) Incident Management
i) OSUWMC must have defined operational processes that facilitate quick, effective and orderly management of incidents based on their nature and severity.

15) Logging and Monitoring
a) OSUWMC must develop and enforce formal logging and monitoring processes to comply with all relevant business, statutory, regulatory, and contractual requirements related to information and security

16) Media Handling
a) OSUWMC must develop and enforce standards for the handling of media, in all its forms (e.g. mass storage, portable devices, paper) to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

17) Messaging of PHI or Restricted Data
a) Instant Messaging (IM) and Text Messaging
i) Only approved IM and text messaging apps and applications may be used to transmit PHI and other Restricted Data.
b) Email
i) OSUWMC Workforce members must use their OSUWMC email account to conduct OSUWMC business.
ii) OSUWMC email accounts should be used for OSUWMC for business purposes only and not for personal use.
iii) OSUWMC email may not be systematically redirected to other email systems.
iv) Emailing PHI or other Private / Restsricted Data to external persons or organizations must be secured and sent using an approved secure email service.

18) Personal or Unmanaged Devices
a) Personal or unmanaged devices must not connect to OSUWMC information systems (such as servers, computers and networks) without prior authorization and acceptance of required terms, conditions and agreements associated with the connection.
b) Employees must be made aware that personal privacy may not be possible based on the nature of the connection to or managed by OSUWMC equipment or networks.

c) Storage of OSUWMC information on unmanaged devices is prohibited.
d) Under no circumstances does OSUWMC assume liability for damage to personal devices.

19) User Security Education and Awareness
a) OSUWMC must implement an information security education and awareness program in order to ensure that all Workforce members are aware of information security threats and concerns as well as their own responsibilities and liabilities as it relates to information security.
b) All Workforce members must receive appropriate education, training, and regular updates regarding information security policies, standards, and best practices, specific to their job function.

## User Roles and Responsibilities

Unless explicitly stated otherwise, the following user terms and conditions apply to all OSUWMC users:

1) User agrees to immediately report to his/her manager and the IT department any incident involving the loss of or unauthorized access to OSUWMC data, including potential loss or unauthorized access related to lost and stolen personal devices. Any security incidents involving ePHI must be reported immediately to the Chief Information Security Officer (CISO) or one of his/her designees at ISSecurity@osumc.edu.

2) User acknowledges and agrees to surrender an OSUWMC provided device upon request by HR, Legal, IT Security, OSU Police or other authorized agent to assist in investigation of OSUWMC ePHI data or application that may have been accessed by the device.

## Exception Process

When compliance is not possible due to business requirements or system limitations, the following exception request process must be followed (see Information Security Exception Submissions):

1) Executive leadership, the dean or vice-president (or one of his/her designees) of the unit requesting the exception must review the exception request, the justification why the unit cannot comply, and is responsible for assumption of risk and potential impact of non-compliance. If the exception is approved by unit senior leadership, the OSUWMC information security governance group will review the request and make a final determination as to whether or not the exception request is granted. At a minimum, this includes approval by the OSUWMC CISO. Depending on the risk of the exception, the review and approval may also include the HIPAA Security & Privacy Committee and/or HIPAA Steering.

2) Exception approvals will be valid up to a maximum of one year for the specified device, system or process, at which point the exception request will need to be re-submitted.

3) Exceptions are subject to review by the OSUWMC Chief Information Security Officer (CISO) or one of his/her designees. Responses may include requests for additional information or justification.

## Sanctions

Unless explicitly stated otherwise, or unless a formal exception has been granted, Workforce members are required to comply with this policy and associated standards.

Those who fail to comply with this policy and associated standards are subject to sanctions and/or corrective action up to and including termination in accordance with Human Resources policy and procedures regarding discipline and termination.

## Resources

Applies to: All OSUWMC Workforce

OSU Institutional Data Policy (OSU IDP)
OSU Information Security Standard (OSU ISS)
OSU Information Security Control Requirements (OSU ISCR)
OSUWMC Information Security Exception Submission SOP

## Contacts

| Office | Telephone |
|---|---|
| CISO, Director IT Information Security | 614-293-7672 |

## History

Issued: March 31, 2014
Revised: August 7, 2018
Submitted by: HIPAA Steering Committee
Approved by: HIPAA Steering Committee
Approval date: August 14, 2018