University of Cincinnati
HIPAA Administrative, Physical and Technical Safeguards

Your information security role in protecting HIPAA information

Effective Date: 7/1/2014
Prior Effective Date: 10/1/2013
INTRODUCTION

It is the legal and ethical responsibility of all individuals to use electronic protected health information in accordance with the law, and University of Cincinnati policies, and to preserve and protect the privacy rights of the subjects of the information. The HIPAA Administrative, Physical and Technical Safeguards set forth in this document describe the responsibility of protecting HIPAA data required by everyone that uses, stores, or comes in contact with electronic protected health information (ePHI).

GENERAL

1. General

1.1. The University of Cincinnati is committed to maintaining the integrity and security of its information. Information security core principles include:

- Confidentiality: Preventing the disclosure of information to unauthorized individuals, systems, or processes. This means ePHI is accessible only by authorized people and processes.
- Integrity: Maintaining and assuring the accuracy and consistency of the data over its entire life cycle. This means ePHI must be protected from unauthorized alteration, faulty processing, destruction, and/or loss.
- Availability: Ensuring ePHI information is accessible and useable when needed by an authorized user.

1.2. The university defines roles and responsibilities for protecting restricted information in its Data Protection policy. HIPAA data or ePHI is classified as restricted data or information. Data trustees, stewards, custodians and users are required to ensure these HIPAA Administrative, Physical and Technical Safeguards are implemented. See Roles and Responsibilities in the Data Protection Policy found in the Related Links section.

2. Safeguards

2.1. Prohibited personal uses: Personal use of restricted information is prohibited. For example, use for personal commercial gain, charitable solicitations, and political activities. Criminal use of restricted information will be prosecuted to the full extent of the law.

2.2. Unauthorized disclosure: The intentional or unintentional disclosure of restricted information to an unauthorized user or for an unauthorized use is prohibited.

2.3. Unauthorized use: University of Cincinnati information systems are provided for the sole use of authorized users. Use by others is prohibited.
2.4. **Storage of restricted information:** ("data at rest"): Each user is responsible for adequately safeguarding restricted information. For a definition of restricted information related to policy, see the Data Classification and Data Types in the Data Protection Policy. Therefore:

2.4.1. Restricted information must be stored on network drives secured by user name and password or in other approved encrypted storage/applications.

2.4.2. In the event that restricted information must be stored on any other portable or non-portable device or service, said device or service must be reviewed by the IT@UC Office of Information Security to ensure security safeguards and regulations are met. Following approval, the user is responsible for adequately protecting that restricted information, including ensuring that physical protections are in place and the device or service is password protected and encrypted.

2.4.3. The storage of restricted information in external services/systems such as Internet cloud services (e.g., Google documents, Dropbox, or backup systems) is prohibited. IT@UC’s Office of Information Security should be contacted for further information on alternative options.

2.4.4. IT@UC’s Office of Information Security and Office of General Counsel must review the use of externally hosted applications. A data security rider is required for any agreement with an external application service provider. IT@UC’s Office of Information Security may be contacted for information.

2.5. **Logging in/out:** Users must either secure/lock or log out of systems (e.g., computers, VPN or Extranet) and log off of applications (e.g., People Admin, UC Flex or Epic) when not in use.

2.6. **Modification or removal of safeguards:** Any system that uses, stores, or comes in contact with electronic protected health information must have safeguards as part of the standard installation. These safeguards include: anti-malware programs, encryption software, and timeout periods. These safeguards must not be removed, disabled, or altered in any way.

2.7. **Business Associates:** Third parties requiring access to information systems or restricted information or electronic Protected Health Information (ePHI), require a written agreement. For ePHI from university operated clinical systems, a Business Associate Agreement (BAA) will be required with review and approval by the University of Cincinnati’s Office of General Counsel.

2.8. **Information security incident of ePHI:** All faculty, staff, trainees, students and others in University of Cincinnati’s HIPAA designated health care components must immediately report violations of this policy and/or information security incidents that may involve the loss of, improper disclosure of, or improper
access to ePHI (e.g., the loss or theft of a computer, smartphone, or thumb drive storing ePHI; or an electronic intrusion into a computer storing ePHI). Reports should be made to the IT@UC’s Office of Information Security at Abuse@uc.edu.

2.9. The University of Cincinnati reserves the right to suspend access to information systems for suspected violations, pending investigation and resolution. The University of Cincinnati reserves the right to terminate access to any user found in violation of its policies, procedures or safeguards.

PORTABLE DEVICE MANAGEMENT

1.0 General

1.1. Theft, loss, and/or misuse of portable devices are one of the most common information security incidents of restricted information across industries. While portability has obvious advantages, the increased risks require that users of portable devices take extra precautions. The risks associated with the use and/or loss of portable devices may result in increased costs associated with replacement of the device, lost productivity, legal liability, federal reporting obligations, the fines and penalties to the institution, loss of reputation and/or negative publicity.

1.2. Portable devices include all devices or services that support mobile computing or communications, including, but not limited to the following device types:

1.2.1. Portable Computers
   - Laptops
   - Notebooks
   - Netbooks

1.2.2. Mobile Devices
   - Smartphones (e.g., iPhone)
   - Cellular phones
   - PDAs
   - Tablet devices (e.g., iPad)

1.2.3. External Data Storage
   - USB flash drives
   - SD Cards
   - Connected external hard disk drives
   - Any removable media (e.g., diskettes, Zip drives, CDs, DVDs etc.)

1.2.4. Cloud/Internet based file storage services
   - UC FileSpace
   - Dropbox
• Microsoft SkyDrive

2.0 Safeguards

2.1. Users are responsible for ensuring security of portable devices (regardless of device ownership) that access information systems, transmit or store restricted information. IT@UC’s Office of Information Security will determine the type of device being used and the protections that must be implemented, and can provide additional information about devices. Protections that may be required in order to acquire and manage restricted information include:

• Using a password or other user authentication
• Installing and enabling encryption
• Installing and activating remote wiping and/or remote disabling
• Installing and enabling a firewall
• Installing and enabling security software
• Keeping security software up to date
• Researching mobile applications before downloading
• Maintaining physical control (protect against loss)
• Using adequate security to send or receive ePHI over public Wi-Fi networks
• Deleting all stored information before discarding or reusing the mobile device

2.2. Reporting: Users must immediately report any loss or theft of portable devices containing ePHI or restricted information to IT@UC’s Office of Information Security at Abuse@uc.edu.

2.3. Portable devices are prohibited from accessing the secure network of the designated health care component unless the system owner approves access.

2.4. If a user chooses to access information systems of the designated health care component using portable devices (regardless of who owns the device), it is the user’s responsibility to ensure that the device is properly secured and protected. Users are required to know the properties of each device and ensure optimum security of information systems and restricted information by use of password protection and encryption. Portable devices used for access to the designated health care component must be registered with the system owner.

2.5. Users must not store access credentials to information systems on portable devices (e.g., user IDs, passwords).

2.6. Physical security: It is each user’s responsibility to maintain the physical security of portable devices in his/her possession at all times. Physical security includes the use of physical and technical safeguards to protect the device from loss, natural and environmental hazards and unauthorized intrusion. This includes,
but is not limited to, ensuring that it is either physically within the user’s control or locked in an area where unauthorized users cannot access it.

2.7. **Destruction, retiring, recycling:** Users are responsible for adequately destroying, erasing, or retiring portable devices that have been used to access and/or transmit restricted information. Users should contact University of Cincinnati’s Asset Management unit to arrange for the appropriate disposal of portable devices, which will be in accordance with Federal National Institute of Standards in Technology (NIST) guideline SP 800-88.

**PHYSICAL & ENVIRONMENTAL SECURITY**

1.0 **General**

Physical and environmental safeguards are an important part of protecting information systems and restricted information.

2.0 **Safeguards**

2.1. Servers, data storage devices, and other IT equipment that manages ePHI must be kept within secure areas with appropriate access or entry controls. Security controls include installing the appropriate level of physical (e.g., key/ID badge access, surveillance monitoring) and environmental controls (e.g., fire suppression, uninterruptible/back-up power supplies) to protect these resources, as well as managing access to these resources.

2.2. **Physical Security:**

2.2.1. A clear desk and clear screen reduce the risk of unauthorized access or damage to information systems and restricted information. This includes ensuring that restricted information is not visible in an unattended work area or on an unattended system, logging off of systems after access, not posting passwords and user ids in visible areas around the work area, not tampering with the automated screen savers, and locking cabinets and rooms containing systems that can access or store restricted information.

2.2.2. Protection of equipment (including computer equipment that is used off- site) is necessary to reduce the risk of unauthorized access to information systems and to protect against loss or damage. Depending on the size of the system or device, physical access to areas where systems reside must be restricted to personnel specifically authorized to operate or maintain the systems or as authorized by the system owner.

2.3. **Environmental Security:**

2.3.1. Environmental control systems must be established to maintain
temperature, humidity, and electrical values that support a stable computing environment. Special controls are required to protect against hazards or unauthorized network access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure. Backup facilities for environmental control systems must be part of an approach to ensuring system integrity and availability.

ACCOUNT MANAGEMENT

1.0 General

1.1. Access to information systems and restricted information are controlled and accessible only on a need-to-know basis. Access to information systems will be granted only when specifically authorized and warranted based on job function.

1.2. Users are responsible for ensuring that they only have access to the resources they need to fulfill their responsibilities.

1.3. System owners are responsible for immediately updating user account and access privileges upon changes to job responsibilities and employment status such as employment termination, promotion, or internal transfer or any other occurrence or event that warrants such change.

2.0 Safeguards

2.1. Account set-up:

2.1.1. System owners must establish a specific process in place to setup accounts for users on information systems who require access to restricted information including:

- UC employees
- Students
- Non-employees
- Vendors, contractors
- All others

2.2. Account transfers:

2.2.1. Users should ensure they only have access to those resources required for their current job. Users must contact the system owner to remove access to resources from a previous position / department.

2.2.2. System owners must develop a system access form for their designated health care component. Outgoing and incoming managers of a transferred employee or badged non-employee must complete the system access
form within 48 hours of the transfer. This form includes information about the resources from which access is removed and the resources to which access is to be granted.

2.2.3. Outgoing managers must work with incoming managers and the system owner to confirm that access to applications and resources that need to follow an employee remain in place and that access to applications and resources that do not need to follow an employee are removed.

2.3. **Account termination:**

2.3.1. Managers must immediately submit the system access form for voluntary and non-voluntary terminations.

2.3.2. Managers must regularly review organizational management in UC Flex to ensure that terminated or transferred employees no longer display in their organizational center.

**ACCOUNT CREDENTIALS: USER IDS & PASSWORDS**

1.0 **General**

1.1. Users who have been assigned user IDs/passwords to work with systems that generate, store or manage restricted information bear the responsibility for preserving the confidentiality and integrity of their credentials to ensure against unauthorized use by any other person.

1.2. Employees who negligently or intentionally share their system passwords or accounts with anyone else for any reason will be held responsible for resulting misuse of the system by others.

1.3. Users who have any reason to believe or suspect that someone else is using their unique credentials must immediately notify their supervisor and IT@UC’s Office of Information Security.

2.0 **Safeguards**

2.1. Users are prohibited from sharing individual account credentials or from logging into information systems with their unique credentials and then permitting another person to access information in those databases and/or systems.

2.2. Users must access only those resources to which they have been explicitly authorized access.

2.3. Users must not have more than one account on any given system or resource.
Exceptions will be made on an individual basis. These exceptions will be documented and reviewed annually during the risk assessment process.

2.4. Users who have become locked out of an application as a result of too many incorrect username/password attempts must notify the appropriate service desk promptly so the event can be logged as a user error, rather than as an unauthorized access attempt. The service desk/application administrator must not reset any such accounts until the identity of the user can be positively established. Where technically supported, user IDs will be automatically disabled (i.e., locked out) as a result of entering too many consecutively incorrect user ID/password combinations.

2.5. When prompted to remember a password by a browser, program, or application (e.g., Internet Explorer, Google, etc.), users should always select “no”. Passwords must not be hard-coded (whether readable or not) into applications and programs.

2.6. User IDs:

2.6.1. User IDs will be created only once approved by the system owner and established by the system administrator through an established system account setup process for each designated health care component.

2.6.2. User IDs should only be disclosed when required to support an application in the troubleshooting process.

2.6.3. Access to information systems may require additional (i.e., multi-factor) authentication requirements as determined by system owners.

2.6.4. Authentication devices (e.g., SecurID tokens/key fobs) must be managed to ensure their security. It is the user's responsibility to maintain the physical security of key fobs in their possession. This includes ensuring that it is either physically within their control or locked in an area where it cannot be accessed by unauthorized users.

2.7. Passwords:

2.7.1. Users are individually responsible for maintaining the confidentiality, security and integrity of their chosen passwords.

2.7.2. Under no circumstances should users share a password. No legitimate activity will require or request that a user communicate a password.

2.7.3. If a user has forgotten his/her password, they should contact the appropriate service desk to reset the password. Only service desk personnel and system administrators shall have the privileges to reset
passwords. They do not need the current password in order to reset a password.

2.7.4. Users are required to change their password every 90 days. Reminders will be sent in advance of the 90-day expiration.

2.7.5. Where technically feasible, the system owner will control and regulate the use of temporary passwords (i.e., upon first use, a user will be forced to change their password). Where this is not technically feasible, users will be instructed to change these passwords as soon as possible. Users must immediately change the default passwords of any newly assigned or reset accounts.

2.7.6. Users who suspect that their passwords have been compromised must immediately report the suspected compromise to IT@UC’s Office of Information Security and must change or reset all passwords in question.

2.7.7. Passwords must not be stored in freeware/shareware password vaults, whether encrypted or not.

2.7.8. Passwords must comply with current standards to ensure appropriate strength of password and have the following characteristics (where supported by the application):

- Passwords must not be the same as a user’s previous five passwords.
- Passwords must be at least 8 characters in length.
- Passwords must contain at least one alpha character and one numeric character.
- Passwords must not be based on easily guessed, readily identifiable/available information (e.g., the same as the user name, Social Security number, names of children, spouse, pets, etc.).

REMOTE ACCESS

1.0 General

1.1. Remote access to information systems must be managed and protected.

1.1.1. Personnel who have been issued an employee id, user id and badge are provided extranet access.

1.1.2. Other users must go through an approved system access process to receive extranet access.

1.1.3. Other remote access options, VPN, require specific authorization to
remotely access systems and information from the system owner.

1.2. Users must follow the standards described in this document when remotely accessing information systems from networks other than those managed by the University of Cincinnati.

2.0 Safeguards

2.1. Extranet: Access is granted by using network user name and password.

2.2. VPN: Access will only be granted following submission of a completed remote access request form that has been approved by the system owner. Gateway-to-gateway VPN connections (semi-permanent) will require the explicit approval of the system owner and IT@UC Office of Information Security.

2.3. Remote users are prohibited from transferring any protected data from a university system to their home/personnel device of any kind.

MALWARE, SPAM, AND SOCIAL ENGINEERING

1.0 General

1.1. Malicious software, social engineering acts and hoaxes are designed to disrupt computer systems, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources.

2.0 Safeguards

2.1. Information Systems must have an automated anti-malware management system. Disabling, altering, deleting, or preventing these programs or other security settings from updating is strictly prohibited. The system owner and IT@UC Office of Information Security may grant exceptions to this when alternate methods of risk mitigation are available.

2.2. The deliberate creation, use, storage, distribution, and/or possession of malware is expressly prohibited. The intentional storage, distribution, and/or possession of malware may be construed as failure to safeguard information systems.

2.3. Removal of unauthorized software: Unauthorized, malicious or nuisance software can be installed on a computer without the knowledge of the user. If unauthorized software is discovered to be or suspected to be installed on any system, IT@UC’s Office of Information Security must be contacted immediately.

2.4. System administrators may remove, with or without prior notification any malicious or unauthorized software.

2.5. Spam or bulk mail: Users shall not use information systems to send unsolicited
or bulk advertisements or commercial messages.

2.6 Social engineering: Users of information systems must recognize and avoid social engineering links. Users should not engage in requested actions, whether that is a human or electronic request, without scrutinizing the requested information and the person making the request. IT@UC’s Office of Information Security can advise.

2.7 Hoax messages: Creation or forwarding of hoax messages is expressly prohibited. Users who receive virus-related warnings from sources other than the University of Cincinnati shall contact the IT@UC Service Desk for further clarification and/or guidance.

2.8 Users shall take due care when opening suspicious or unexpected email with attachments from unknown users. When uncertain, users shall contact the IT@UC Service Desk for assistance and/or guidance.

SOFTWARE & HARDWARE: REQUESTS & INSTALLATION

1.0 General

1.1 The system owner provides standard hardware and software to support overall functions for technology hardware and software needs. The system owner usually delegates responsibility for the technical management of a system’s hardware and software to a qualified system administrator or staff who are capable of implementing appropriate technical, physical and administrative safeguards.

1.2 Additional hardware and software for individual users may be requested via an established documented project request process defined by the system administrator and approved by the system owner. Requests for enterprise-wide, departmental, or area-specific hardware or software solutions should follow this same process. This includes custom-built applications. These requests may be subject to additional costs.

2.0 Safeguards

2.1 All software and hardware purchases must receive pre-approval from the system owner and follow a consistent documented project request process.

2.2 Installation of unauthorized software: Only properly licensed, obtained and approved software may be installed on computers that use, store, or come in contact with electronic protected health information (ePHI).

2.3 Any non-standard software not purchased or distributed by a system owner approved vendor is prohibited.
2.4. Unauthorized duplication or distribution of university-licensed software is prohibited.

2.5. System owners must approve use of custom-built applications.

SAFEGUARDS FOR NON-UNIVERSITY DEVICES

1.0 General

1.1. University of Cincinnati policies, procedures, and standards apply when information systems and restricted information, including ePHI, is accessed from devices not owned or supported by the university (e.g., storage, computing or communication tools, such as computers, laptops, tablets, smartphones, cell phones, personal data assistants, external hard drives, thumb drives).

1.2. It is each user’s responsibility to ensure that information systems and restricted information of the university, including ePHI, is protected from unauthorized access, use, disclosure, modification, and/or loss, including when such systems or information is accessed from non-university devices.

2.0 Safeguards

2.1. Access to or use of information systems and restricted information residing on the university’s network using non-university devices shall be either through an extranet or VPN. The appropriate university system owner must approve access.

2.2. The university makes some applications/websites available externally. Where applicable, access to these applications is controlled through approved system access processes.

2.3. If using a non-university device to access information systems of the university or while working with restricted information of the university, users are responsible for the actions of non-university users (e.g., household members, collaborators in other organizations).

2.4. Each user is responsible for implementing appropriate security measures on non-university devices used to access information systems and/or restricted information of the university. This includes, but is not limited to:

- Installation and automatic updating of anti-malware detection programs and vendor security patches
- Immediately logging off when finished accessing information systems or restricted information from the university (e.g., VPN)
- Physical security measures, such as using locks and not leaving non-university devices visible in public places
• Implementing separate user profiles and password protecting and using encryption on the device itself
• Maintaining current operating system and browser configurations.