Background

The University of Cincinnati (UC) is committed to providing the highest quality health care, which includes respecting the right of patients and clinical research subjects to maintain the privacy and security of their health information. The standards for protecting health information are prescribed in the federal law known as the Health Insurance Portability and Accountability Act (HIPAA). HIPAA and UC’s HIPAA policies apply to individually identifiable information on past, present or future health care or payment for health care, which HIPAA calls Protected Health Information or PHI. PHI stored electronically is called ePHI.

Because the university only uses and engages in electronic transactions involving HIPAA protected health information for a part of its operations, the university has designated itself as a hybrid entity for purposes of HIPAA compliance. UC’s policies are designed to ensure the appropriate privacy and security of all PHI or ePHI across the university comply with the law. UC's HIPAA Information Security policies apply to all faculty, staff, trainees, and students in designated health care components. The designated health care components of the university's hybrid entity subject to the specific requirements of HIPAA are the following:

1. University Health Services
2. Hoxworth Blood Center
3. College of Medicine
4. Human Resources – component administering the university’s health plans
5. Office of General Counsel
6. UC Information Technologies (UCIT) Office of Information Security (OIS)
7. Office of Research – compliance & regulatory affairs
8. Internal Audit
9. Such other components as may be required to comply with changes in the law, or that are necessary for the orderly operation of the university as determined in writing by the senior vice president for academic affairs and provost. These additional covered components include, but are not limited
to, the College of Allied Health Sciences, College of Nursing, College of Pharmacy and the Joint Center for Health Informatics.

Definitions

**Appendix A** is a limited glossary based on the original definitions in the HIPAA regulations, but edited as a convenience to help clarify for UC readers; only the definitions in the regulations are authoritative for compliance purposes.

Policy

**Required and Addressable Specifications**
The HIPAA Security Rule has both “required” and “addressable” specifications for its administrative, physical and technical safeguards. Implementation specifications described as “required” must be implemented. The concept of “addressable” specifications provides designated health care components additional flexibility with respect to compliance with the security standards. In meeting standards that contain addressable specifications, one must do one of the following for each addressable specification:

- Implement the addressable specifications;
- Implement one or more alternative security measures to accomplish the same purpose; or
- Not implement either an addressable specification or an alternative.

In all cases the designated health care component must document what it has (or has not) done to meet the standards in its policies and procedures. The rationale for the selection of an alternative, or to not implement anything at all, must be documented with particular thoroughness, including how the standard is being met via non-standard means.

**Risk Assessment**
The University of Cincinnati Information Technologies Office of Information Security (UCIT OIS), in collaboration with the Offices of Risk Management and General Counsel, shall facilitate an annual external contract to conduct an institutional security risk assessment across the designated health care components to address HIPAA requirements. The expense for this assessment will be distributed across all university designated health care components.

UCIT OIS, in collaboration with other university offices, shall facilitate system specific risk assessments of selected individual critical systems containing ePHI. These risk assessments shall be documented and shall provide a baseline for subsequent reviews. On a continuing basis, UCIT OIS shall implement a process to identify ePHI systems or categories of systems and provide procedures by which system owners responsible for ePHI-containing systems can assess compliance with security policies and procedures.
System owners who store, access, transmit or receive electronic Protected Health Information (ePHI) must review all systems and applications with ePHI for which they are responsible and evaluate their vulnerabilities to threats. Analysis must be done to determine what technical, physical and administrative safeguards are required and how best to implement those safeguards.

System Owner Responsibilities
All ePHI systems must be registered and entered into the University HIPAA System Inventory Database (See Related Links). This database is maintained by UCIT OIS, which records system owners’ or their designees’ self–assessment information for each ePHI system. UCIT OIS and Internal Audit use the HIPAA System Inventory Database to identify systems for sampling audits, and during those audits, for accuracy of the self–assessments.

System owners with responsibility for ePHI systems must:

1. Perform an annual security self-assessment of ePHI system(s).
2. Evaluate the risks to the confidentiality, integrity and availability of the ePHI.
3. Determine what physical, administrative and technical safeguards may be necessary to adequately address the identified risks, based on the annual assessment, HIPAA security policies and procedures, technical standards and other university guidance. As appropriate, system owners must develop, document, implement and test a contingency plan that includes
   a. a backup plan;
   b. an emergency mode operation plan; and
   c. a disaster recovery plan.
4. Manage ePHI system(s) in accordance with applicable university procedures including HIPAA Information Security and Data Protection policies.
5. Successfully complete the HIPAA security training offered by the university. The annual assessment completed by system owners consists of a Web-based questionnaire, the answers to which are tracked by UCIT OIS.

UC’s HIPAA security training details responsibilities and standards for maintaining security of ePHI systems and data and provides information and links to additional resources.

System owners with responsibility for any ePHI systems may contract with UCIT’s system administration services to assume system administrator responsibility or for other support for ePHI systems and applications.

Administrative, Physical and Technical Safeguards (See Related Links for more details)

Administrative Safeguards
A range of administrative safeguards is employed to protect ePHI, both at the institutional level and at the system owner level. HIPAA security training is required for
all faculty, staff, trainees, students and others in University of Cincinnati’s designated HIPAA health care components who create, access, store, transmit or receive ePHI. UCIT OIS monitors electronic information activity and university Internal Audit also audits compliance with HIPAA Information Security within the scope of their normal audit activities.

In addition, system owners with responsibility for an ePHI System must develop administrative safeguards for such systems including: (1) A contingency plan; (2) An emergency mode operation plan; and (3) A disaster recovery plan. These plans shall be developed by the responsible system owner or by a delegated, qualified IT support group. Templates for plans are available in UCIT’s business continuity system. The plans shall be consistent with university policies and procedures and shall be commensurate with the risks to confidentiality, integrity and availability of the ePHI.

Designated HIPAA health care components may permit a business associate to create, access, transmit or retain ePHI on behalf of the designated health care component only when a business associate agreement is entered into with the business associate that contains all of the requisite assurances in accordance the university’s data security contract rider. (See Business Associate Policy, Business Associate Agreement, and Data Security Contract Rider in Related Links).

**Physical Safeguards**

The university is responsible for maintaining a physical facility security plan for its university data center. The university physical facility security plan ensures that ePHI in any format (electronic, backup tapes, etc.) housed in the university data center location(s) meets HIPAA requirements for physical security. The University Architect and UCIT maintain copies of the University’s Physical Facility Security Plan.

It is the responsibility of system owners to implement safeguards such that electronic protected health information within their department is protected from physical access by unauthorized individuals and environmental safeguards are in place to protect the confidentiality, access and integrity of ePHI as commensurate with data criticality and risk assessment.

It is the responsibility of system owners to certify that electronic protected health information located at non-University of Cincinnati business locations is adequately protected from physical access by unauthorized individuals and that environmental safeguards are in place to protect the confidentiality, access and integrity of ePHI as commensurate with data criticality and risk assessment. Physical access to ePHI that is maintained at home, at a non-University of Cincinnati business location or on non-University of Cincinnati owned equipment is the responsibility of the individual.

Portable electronic devices used to store, access, transmit or receive data will be subject to special requirements designed to minimize the risk of inappropriate disclosure of ePHI through theft or accidental loss.
Procedures must be in place to ensure that the inappropriate access or viewing of the display screen of any computing device that creates, receives or distributes ePHI is minimized. Compliance is paramount in patient or research-subject areas.

Reasonable and appropriate physical security must be implemented to secure computing devices housing ePHI including:

- Privacy filters must be installed on computer screens that display ePHI and can be viewed by the public or non-clinical staff.
- A screensaver that hides the screen after 10 minutes of inactivity and requires a password to restore the display must be used.
- Whenever possible, the space must be secured through locking the room or area when a computer will be unattended for extended periods since physical access to the computer allows other methods of access to data (e.g., inserting a disk or CD with tools for hacking).
- A locking cable or equivalent physical protection (e.g., locked cabinets) for all devices when not in the user’s physical custody.
- The exact geographical locations of ePHI in local departments, data centers, or on non-University of Cincinnati property must be specified and adequate physical security implemented to ensure that individuals who have no need to access ePHI systems cannot do so. These protective measures cover all types of computing mediums such as data servers, desktop PCs, personal digital assistants (PDAs), USB devices, CDs, DVDs, diskettes, memory sticks, flash cards, smart phones and any future medium used to store ePHI – whether or not these computing media are located on University of Cincinnati property or not.
- Portable computing devices must never be left unattended and unlocked.

Technical Safeguards
System owners responsible for ePHI data systems, applications and devices are responsible for ensuring appropriate technical safeguards consistent with university policies are implemented. The adequacy of technical safeguards shall be reviewed regularly in accordance with university policies and procedures.

Laptop and Desktop Configuration Standards
All University of Cincinnati laptop and desktop computers used to store, access or transmit ePHI must follow current secure configuration standards, including:

- Whole Disk Encryption
- Automatic distribution of security and other patches via central computer management software
- Installation and update of antivirus /antispyware software
- Automatic locking and password protection of desktops after 15 minutes of inactivity
- Removal of administrative privileges
- Removal of applications that increase the vulnerability of computers such as Peer to Peer (P2P) file sharing
• Locking cables or equivalent physical protection (e.g., locked cabinets) for all devices when not in the user’s physical custody
• All new desktop and laptop computers must be purchased from University of Cincinnati managed device portfolio facilitated via UC Purchasing
• Other safeguards as they become technically feasible.

Smartphones and Other Mobile Data Devices
All faculty, staff, trainees, students and others must implement current security standards for smartphones and other mobile data devices that create, store, access, transmit or receive ePHI, whether University of Cincinnati-issued or personal, including:

• Passwords: Passwords must include a minimum of four characters. The mobile data device must be set to delete all data or lock internally after 10 unsuccessful attempts to enter a password.
• Encryption: The data on the mobile data device must be encrypted. Backups of data from one device to another device that is not encrypted (e.g., if a backup of a tablet is made using an unencrypted computer) the backup data must be encrypted.
• Message Storage Limits: No more than 200 messages or 14 days of messages may be on a mobile data device.
• Applications: Applications that create, store, access, send or receive ePHI must meet University of Cincinnati security standards. Custom developed applications used on mobile data devices must undergo a security design review and application vulnerability scan by UCIT’s Office of Information Security.
• Software must be kept up to date: You must use the most recent operating system available for your mobile data device, and you must apply available security updates for any other software (e.g., applications) in a regular and timely manner unless instructed otherwise by UCIT Office of Information Security.
• Tracking and remote deletion enrollment: A mobile data device must be capable of remote deletion and locking using the university’s mobile device management solution or the user must subscribe to a service that allows remote deletion of messages stored on the mobile data device in the event it is lost or stolen.
• No circumvention of device security: Users must not circumvent the security of any mobile data device by removing limitations designed to protect the device (jailbreaking), and tampering with a device by using unauthorized software, hardware, or other methods is prohibited.
• Safe wireless data networking:
  o Digital Cellular: Users must use University of Cincinnati’s Virtual Private Network (VPN) services if connecting to the university’s network from a cellular carrier locally, nationally or internationally.
  o For Wi-Fi networking, users may use only secure (WPA-2) Wi-Fi networks known to be secure (such as SecureWireless). If the user cannot use a WPA-2 Wi-Fi network, he/she must use a VPN connection to connect to University of Cincinnati.
  o Bluetooth®: Passwords or PINs must be used to secure Bluetooth® connections with devices and block unknown devices.
Removable or Portable Media Devices
All faculty, staff, trainees, students and others in a University of Cincinnati designated health care component may never store ePHI on thumb drives or other removable media devices unless they meet University of Cincinnati encryption standards.

Personally Owned Computers and Remote Access
University of Cincinnati faculty and staff in a University of Cincinnati designated health care component must not create, store, access, transmit or receive ePHI on personally owned computers. Faculty and staff who require remote access to on-campus systems that store ePHI must use a university provided, fully managed and encrypted device, and they must log-in via a VPN connection.

Students or trainees may use two types of computers to create, store, access, transmit, or receive ePHI:
- Clinical systems managed in a designated health care component;
- iPad or computer tablets provided through University of Cincinnati academic programs secured by a system owner/administrator in compliance with University of Cincinnati safeguards.

Students or trainees may not use any other device to create, store, access, transmit or receive ePHI. Any ePHI that is not needed for continuing work must be removed before the student or trainee leaves the University of Cincinnati.

Training
All faculty, staff, trainees, students and others in University of Cincinnati designated HIPAA health care components must complete UC’s HIPAA security training. Any of these individuals who create, access, store, transmit or receive ePHI or who access the university network must complete HIPAA security training. UCIT OIS will maintain institutional HIPAA security training records.

HIPAA security training also requires every individual review and electronically sign acknowledgement of individual responsibility to protect ePHI information. (See Related Links)

Password
All faculty, staff, trainees, students and others in University of Cincinnati HIPAA designated health care components must adhere to the university’s Password policy and password safeguards (Administrative, Physical and Technical Safeguards) in Related Links.

Removal of Electronic PHI (ePHI)
All faculty, staff, trainees, students and others in University of Cincinnati HIPAA
designated health care components must securely destroy or delete ePHI when no longer needed or when retiring computers, smartphones or other mobile devices such as thumb drives. (See Asset Disposition Policy in Related Links).

**Email Accounts**

All faculty, staff, trainees, students and others in University of Cincinnati HIPAA designated health care components must not configure UC email accounts which may receive or transmit ePHI to auto-forward messages to non-UC email accounts.

For email transmission of ePHI, implement and use only encrypted procedures permitted for electronic communication of health-related information (email, voice mail, and other electronic messaging systems). The University of Cincinnati’s central email system monitors, notifies and educates when ePHI may be distributed in an unencrypted manner. (See Email Encryption in Related Links).

**Procedure**

**Reporting Violations and Potential Information Security Incidents**

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 PHI or ePHI (for example, the loss or theft of paper PHI; 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 UCIT’s Office of Information Security at Abuse@uc.edu.

Even if it is believed that no ePHI or PHI was compromised, UCIT OIS must be notified if it is believed that any type of restricted data was compromised. The user must also promptly notify his/her immediate supervisor and administrative unit head if any University of Cincinnati physical or information asset is damaged. (See HITECH Final Rule in Related Links).

**Investigation and Enforcement Procedures**

Reported violations will be investigated by UCIT OIS and, where appropriate, referred to the HIPAA Privacy Officer or other university authorities. UCIT OIS is also authorized to investigate security concerns identified through means other than a reported violation, including routine and targeted monitoring activities. UCIT staff can also be authorized to investigate alleged violations under the direction of UCIT OIS and/or the appropriate authority.

**Disciplinary Procedures**

Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the University Rules, Faculty Handbook, Staff Personnel Policies and Procedures Manual, various student regulations (e.g., the Undergraduate Regulations for undergraduates, the
relevant manuals for graduate and professional school students), and other applicable materials.

Staff members who are members of university-recognized bargaining units will be disciplined for violations of this policy in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units.

Sanctions
Individuals found to have violated this policy may be subject to penalties provided for in other university policies dealing with the underlying conduct. Violations involving ePHI may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The applicable disciplinary authority in consultation with the systems administrator of the affected system, HIPAA Privacy Officer and UCIT Information Security Officer, shall determine the appropriate penalties.

Individuals found in violation of this policy may appeal or request consideration of any imposed sanctions in accordance with the appeals provision, if any, of the relevant disciplinary procedures. In addition to university discipline, individuals found in violation of this policy may be subject to criminal prosecution, civil liability or both.

*Organizational units may institute policies more, but not less, restrictive than this policy (9.1.10) if desired.*

**Related Links:**
- Administrative, Physical and Technical Safeguards
- Asset Disposition Policy
- Business Associate Agreement
- Business Associate Policy
- Business Continuity System
- Data Security Contract Rider
- Email Encryption
- HIPAA Regulations (See Privacy & Security Rule links for authoritative definitions)
- HIPAA System Inventory Database
- HITECH Final Rule
- Limited HIPAA Glossary (Appendix A)
- Password Policy
- Training & Acknowledgement of Individual Responsibility to Protect Restricted Information

**Phone Contacts:**
- UCIT Office of Information Security 558-4732
- UC Office of the CIO 556-2323
- HIPAA Privacy Officer 558-7155

**History**
Reviewed: 10/01/2015
**ePHI System** – A system that creates accesses, transmits or receives: 1) primary source electronically-stored Protected Health Information (ePHI); 2) ePHI critical for treatment, payment or health care operations; or 3) any form of ePHI and the host system is configured to allow access by multiple people.

Examples include:

- A personal computer with a database containing ePHI that is configured to allow access by more than one person.
- A departmental server with file shares containing ePHI.
- A computer system used to create, access, transmit or receive ePHI that is configured to allow access by a non-UC vendor/contractor.
- A clinical care system, which contains primary source ePHI.
- A billing system that is critical to clinical care operations.

**Administrative Safeguards** – Administrative actions and policies and procedures

1. to manage the selection, development, implementation, and maintenance of security measures; and
2. to protect ePHI and to manage the conduct of the designated health care components' workforce in relation to the protection of ePHI.

**Business Associate** – Generally an entity or person who performs a function involving the use or disclosure of electronic Protected Health Information (ePHI) on behalf of a covered entity (such as claims processing, case management, utilization review, quality assurance, billing) or provides services for a covered entity that require the disclosure of ePHI (such as legal, actuarial, accounting, or accreditation).

**Contingency Plan** – Sets out a course of action that is maintained for emergency response, backup operations, and post–disaster recovery. The purpose of the plan is to ensure availability of critical resources and facilitate the continuity of operations in an emergency. The plan includes procedures for performing backups, preparing critical facilities that can be used to facilitate continuity of critical operations in the event of an emergency and recovering from a disaster.

**Data Center** – a centralized repository for the storage, management, and dissemination of data and information organized around a particular area or body of knowledge (e.g., university financial and HR data, or patient scheduling, billing and medical records). At the University of Cincinnati this refers to centrally managed data centers operated by UCIT.
**Disaster Recovery Plan** – The part of a contingency plan that documents the process to restore any loss of data and to recover computer systems if a disaster occurs (e.g., fire, vandalism, natural disaster, or system failure). The document defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process to attain the stated disaster recovery goals.

**De-identification** – The process by which identifiers are removed from PHI.

**De-identification Standard** – Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. See Safe Harbor De-identification.

**Disclosure** – The release, transfer, provision of, access to, or divulging in any other manner of protected health information outside of the entity holding the information.

**Electronic Protected Heath Information (ePHI)** is PHI in electronic form.

**Emergency Mode Operation (EMO) plan** is a subset of a disaster recovery plan that documents processes that support continued operation in case of an emergency. Emergency mode operations documentation includes emergency management/crisis management guidelines and procedures to maintain the integrity, availability and confidentiality of protected health information.

**Encryption** - The process of encoding a message using an algorithmic process to transform data so that it can be read only by the sender and the intended recipient with the use of a confidential process or key. This can also be applied to data at rest (stored data), so that only the owner of that data can read the data. This includes the transmittal of texts, email messages, and file storage.

**Extranet** – An extension of the designated health care component’s intranet to users that are physically located outside of the organization for specific purposes such as research. The connection to a designated health care component’s intranet via a Virtual Private Network (VPN) is considered an extranet.

**Health Care Component** – means a component of a hybrid entity designated by the hybrid entity that functions as a health care provider, as defined by HIPAA.

**Hybrid Entity** – a single legal entity such as University of Cincinnati that is a covered entity whose business activities include both covered and non–covered functions.

**Information Security Incident** – Any activity that harms or represents a serious threat to the whole or part of UC’s computer, telephone and network–based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure,
change or deletion of ePHI, or a crime or natural disaster that destroys access to or control of these resources. Routine detection and remediation of a virus, malware or similar issue that has little impact on the day–to–day business of the university is not considered an incident under this policy.

**Non-university device** – Devices not owned or supported by the University of Cincinnati (e.g., storage, computing or communication tools, such as computers, laptops, tablets, smartphones, cell phones, personal data assistants, external hard drives, thumb drives).

**PHI – Protected Heath Information or (ePHI)** is any information, whether oral or recorded in any form or medium that is created or received by a covered entity that identifies an individual or might reasonably be used to identify an individual and relates to:

- The individual’s past, present or future physical or mental health; OR
- The provision of health care to the individual; OR
- The past, present or future payment for health care.

Information is deemed to identify an individual if it includes either the patient’s name or any other information that taken together or used with other information could enable someone to determine an individual’s identity (e.g., date of birth, medical records number, health plan beneficiary numbers, address, ZIP code, phone number, email address, fax number, IP address, license numbers, full face photographic images or Social Security number.

PHI excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act (FERPA) and employment records held by a covered entity in its role as employer.

**Physical Safeguards** – Measures, policies, and procedures to physically protect the designated health care components’ systems and related buildings and equipment that contain ePHI, from natural and environmental hazards and unauthorized intrusion.

**Portable electronic device** – Any device that supports mobile computing or communications, and has the ability to store data including, but not limited to:

- Laptops
- Smartphones, PDAs, iPhones, cellular phones
- Tablet devices (such as iPads), notebooks
- External hard drives
- Zip drives
- CDs
- DVDs
- USB thumb, flash or jump drives
- Diskettes
• Cloud services (such as Internet based file storage services)

Remote Access – Any access to a device on the University of Cincinnati data network through a non–UC managed network, device, or medium, for example by DSL, cable modem or dial–up connection.

Risk Analysis – A documented assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI, and an estimation of the security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level. Risk analysis involves determining what requires protection, what it should be protected from, and how to protect it.

Safe Harbor De-identification – The following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
   A. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   B. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including finger and voice prints
17. Full-face photographs and any comparable images
18. Any other unique identifying number, characteristic, or code. The covered entity does not have actual knowledge that the information could be used
alone or in combination with other information to identify an individual who is a subject of the information.

**System** – Any electronic computing or communications device or the applications running thereon which can create, access, transmit or receive data. Systems are typically connected to digital networks. Examples of systems include, but are not limited to:

- A computer system whether or not connected to a data network
- A database application used by an individual or a set of clients
- A computer system used to connect over a network to another computer system
- An analog or digital voice mail system
- Data network segments including wireless data networks, and
- Portable digital assistants.

**System Administrator** – the technical custodian of a system. This individual provides the technology and processes to implement the decisions of the system owner. In some circumstances, the system administrator and the system owner may be the same person. System administrators are responsible for the technical operation, maintenance, and monitoring of the system. These duties include implementing appropriate technical, physical and administrative safeguards.

**System Owner** – the authority, individual, or organization head who has final responsibility for systems which create, access, transmit or receive ePHI and including responsibility for the ePHI data. In some complex systems, the functional responsibility for the system and the responsibility for the data may lie with more than one individual. Decisions regarding who has access to the system and related ePHI data and responsibility for the risk analysis rest solely with the system owner. The system owner usually delegates responsibility for the technical management of a system to a qualified system administrator or staff who are capable of implementing appropriate technical, physical and administrative safeguards.

**Technical safeguards** – the technology, and the policy and procedures for its use that protect electronic protected health information and control access to it.