

URMC/Strong Health HIPAA Security Training Module

POLICY SUMMARY: 0S1

(for full policy, refer to <http://intranet.urmc.rochester.edu/policy/HIPAA/>)

HIPAA Security Compliance

The University of Rochester Medical Center/Strong Health (URMC/SH) will maintain the security of electronic protected health information (ePHI) in the manner set forth in the URMC/SH HIPAA Security policies. URMC/SH will adhere to all applicable general requirements, approaches, standards, implementation specifications, and maintenance requirements of the Security Rule in developing and maintaining policies and procedures for security standards for the protection of electronic protected health information. Whenever there is a change in law that necessitates a change to URMC/SH Security policies and procedures, URMC/SH will promptly document and implement the revised policies and procedures.

Who needs to follow this policy?

Any member of the URMC/Strong health workforce who is responsible for the use and disclosure of ePHI and/or works with business associates who have access to ePHI.

What are the general requirements for compliance?

URMC/Strong Health is required to take reasonable steps to:

- Ensure all ePHI that is created, received, maintained or transmitted by URMC/Strong Health is kept secure.
- Create and maintain protection against reasonably anticipated threats (those things we think might happen) to the security and integrity (information is not damaged in any way) of ePHI, including inappropriate use and disclosure.
- Educate workforce members in the Security Rule and monitor compliance of those members.

How will the level of security that is needed be determined?

URMC/Strong Health will follow all standards to comply with the Security Rule by taking reasonable steps to reduce or eliminate unauthorized access to ePHI. Appropriate security measures will be determined by reviewing each covered entity's physical structure, software security capabilities, and the cost to create security measures as well as the potential risk to ePHI at each entity.

What policies, procedures and documentation does URMC/Strong Health need to have in place?

URMC/Strong Health will:

- Create and implement reasonable policies and procedures to comply with the Security Rule.
- Maintain the policies and procedures in written (electronic) form that are easily accessible to all members of the workforce.
- Document any action, security incident, or assessment that is required by the Rule and maintain that documentation for 6 years or from the last update, whichever is later.
- Periodically review all HIPAA Security policies and procedures to ensure they continue to provide security of ePHI as determined by the URMC/Strong Health Chief Security Official.

What are my responsibilities under the Security Rule?

As a workforce member, your responsibilities are to know:

- Which of the policies pertain to your work role.
- Who your Security Official is for your organization.
- When and how to contact your Security Official.
- What to look for regarding security incidents.
- How to report a security incident.

SAMPLE SCENARIO

As part of a hospital unit redesign, new computers have been installed that are used to access ePHI. How does the unit manager know that ePHI is protected according to the Security Rule?

- As part of the redesign, the physical and technical aspects of the unit were reviewed by the Access Administrator and Systems Administrator to determine what safeguards were needed to be put in place to ensure protection of ePHI.

The unit manager must ensure that all workforce members who are now assigned to the unit have read and understand the HIPAA security policies/procedures, and implement them as appropriate for their job.

URMC/Strong Health HIPAA Security Training Module



POLICY SUMMARY: OS2

(for full policy, refer to <http://intranet.urmc.rochester.edu/policy/Hipaa/>)

Disposal of Media Containing PHI

URMC/Strong Health will properly dispose of Protected Health Information (PHI) recorded on any physical medium, whenever that medium will no longer be under the physical control of those who are authorized to access, store, or transport it.

Who needs to follow this policy?

Anyone who handles any kind of media that contains PHI and is responsible for disposal of that information.

What kinds of objects might contain PHI and have to be disposed?

- Paper records
- Tapes, diskettes, cartridges, compact disks, external disc drives, etc.
- Internal hard disk drives or solid-state memory chips.
- Film, including X-rays, infrared, etc.
- Video tapes
- Patient wrist bands
- Medication containers
- IV bags

What about computers?

Any device that may contain digital information such as computers, servers, laptops or patient bedside monitors, needs to be disposed of appropriately. PDAs (e.g. Palm Pilots), digital cameras and cell phones may also contain PHI, all of which must be disposed of properly.

Who is responsible for ensuring all PHI has been appropriately removed from the computers and digital media noted above?

Each URMC/Strong Health workforce member who plans to dispose of computers or digital media, must arrange to have the PHI rendered unreadable and unrecoverable. Typically, workforce members arrange for their information technology (IT) support staff or an outside IT contractor to perform this task.

What if computers or media that contain PHI may be left unattended or otherwise accessible by those who do not have authorization to view that information?

The computers and media should not be left unattended, but if there is a possibility that they may be accessible by unauthorized persons, the PHI should be password protected or encrypted.

How do I know if the PHI has been properly erased/disposed of before I discard the item?

You must be sure the PHI is not in any way readable or able to be reconstructed and read/used.

What about recycling? How do we know PHI will not be recovered from those paper items once they are in the bin?

General blue recycle bins should NOT be used for any item that contains PHI. Each department must have a procedure that ensures paper containing PHI is either shredded (crosscut shredding preferred) or locked in a bin until picked up by a business associate for proper disposal.

What if a patient asks us to remove their wristband and wants to throw it away while still in our care?

Explain to them, using language like, “For your protection and safety, we ask that you continue to wear your wristband until after you have left the facility. If it is uncomfortable, we can move it to your other wrist.”

What if a computer, for example, is being sent to another department within Strong? Do I have to be sure the PHI is erased?

Yes, it is each department’s responsibility to ensure PHI on the hard drive is completely unreadable before that computer is transferred to another department.

How do I know I’ve really ‘cleaned’ the hard drive?

Remember that ‘deleting’ a file does not properly dispose of the PHI. Follow the Procedural Guidelines that accompany Policy OS2 on the intranet site for specifics on how to properly dispose of all PHI, or call the ISD Help Desk at 275-3200 for assistance.

What if we are donating computers to a local school? Or the computers or other equipment are just being thrown out?

In both cases, follow the procedures to ensure all PHI has been erased and is not recoverable. Also, remember to follow internal disposal policies as well as environmental policies when discarding computers or other electronic equipment.

Who can I contact if I have questions on how to discard something?

If your question is related to computers or other electronic media, call the ISD Help Desk at 275-3200 for assistance. For other media, contact your HIPAA Security or Privacy Officer.

SAMPLE SCENARIOS

Nick, a patient on the surgical unit, has needed several IV bag changes after surgery. He has heard about the new HIPAA regulations and wants to know what is being done about his information on the used bags and how they are thrown out. What should the surgical staff on the unit do to ensure his information is not read by anyone who should not have access to it?

- The used IV bags can be disposed of in the regular trash, *as long as the information on the bag is no longer readable*. Options:
 - Use a permanent black marker to *cross out* the information,
 - Place an opaque, non-removable *label over* the information, or
- At URMC, the used IV bag, with all easily disconnected tubing removed, may be placed in the red bag trash for autoclaving.

Sarah is a Home Health Nurse who receives faxed PHI in her home. When she has seen her patient and no longer needs the info, she throws it out at home. Is this a safe way to dispose of PHI?

- Unless Sarah owns a crosscut shredder to assure nothing could be read, she should NOT dispose of PHI at home. Alternatively, Sarah could maintain continuous physical control over the unwanted paper fax until she could bring it to the VNS office for proper disposal.

Pediatrics is getting new computers and the staff have decided to put one of the old computers in the children's play area. What has to be done to be sure there is no PHI on the computer?

- Special software to multi-pass overwrite the hard drive must be used. Examples are BC Wipe and PGP Wipe for Windows machines. The staff should refer to the Procedural Guidelines on the policy intranet site for complete instructions.

Department Q is cleaning out old files and has come across X-rays from 1962. It's doubtful that anyone will care what information is on 40-year-old films, so they decide to just toss them in the regular trash. A housekeeper discovers them that evening and brings them to her supervisor. What should the supervisor do?

- First, congratulate the housekeeper on remembering her HIPAA training! Then properly dispose of the X-rays per that facility's procedures. Third, the housekeeping supervisor needs to talk to either the Department Head about proper disposal procedures, or call the HIPAA Security or Privacy Officer for assistance.



URMC/Strong Health HIPAA Security Training Module

POLICY SUMMARY: 0S4

(for full policy, refer to <http://intranet.urmc.rochester.edu/policy/HIPAA/>)

HIPAA Security Office

As a covered entity, URMC/Strong Health must designate a Security Official with the overall responsibility for the security of the health system's electronic protected health information (ePHI).

URMC/Strong Health is considered a 'covered entity' under the HIPAA Security Rule. As such, URMC/Strong Health has designated a HIPAA Chief Security Official.

In addition, URMC/Strong Health has designated other HIPAA Security Officials who have oversight for their own locations/units (HH, the Highlands, VNS, etc.) that are part of URMC/Strong Health.

What are the responsibilities of HIPAA Security Officials?

HIPAA Security Officials are responsible for overseeing and coordinating the:

- Review of URMC/Strong Health's business policies to ensure that protection of ePHI is a part of those business policies, when appropriate.
- Performance of risk assessments, audits and reviews of relevant information systems to ensure they are adequately protected.
- Establishment and use of appropriate forms, materials, processes and procedures when using ePHI.
- Implementation of policies and procedures to control electronic access to ePHI.
- Purchase of information security products, and their implementation plans and schedules.
- Creation of Business Associate Agreements (as necessary) in coordination with the URMC/Strong Health Privacy Officers.
- Establishment of an incident response team to investigate and document electronic information security breaches (pertaining to computers, hand-held personal devices, digital cameras) and to prevent future incidences.
- Response to security violations, in cooperation with Human Resources, Administration and the Office of Counsel.

- Review of information security plans to ensure URM/Strong Health practices remain in place.
- Awareness of current state and federal security and privacy laws; conducting routine assessments of URM/Strong Health to ensure compliance.
- Supporting a culture that includes security of ePHI and other information into daily practices.
- Development and implementation of security policies and procedures, standards and guidelines to maintain the ongoing security of information.
- Development of training material for security policies and procedures.

HIPAA Security Officials

Please go to the HIPAA website for HIPAA Security Official information.

<http://intranet.urmc.rochester.edu/policy/HIPAA/FAQsResources/Officers.asp#Security>

SAMPLE SCENARIOS

Juan suspects that someone has used his computer and that patient information has been accessed. He always logs off when he goes home, but when he logged in this morning, he noticed some recent patient files had been opened and he is sure that he was not in those files the day before. What should he do?

- Juan should first go to his supervisor and tell him/her what he has found. It may be that another person used Juan's computer in the evening, with appropriate permissions and using their own login. However, if Juan suspects that his computer was used inappropriately; his supervisor needs to call the Security Official or the Area Administrator so that the incident response team can be called in to begin an investigation.

A doctor's office is researching new online billing system to replace the old one they've been using for years. Their vendor of choice offers the service of setting up the new system for them and teaching he staff how to us it. What steps do they need to take to ensure that the system will protect ePHI as outlined in the URM/Strong Health policies and procedures?

- The doctor's office needs to contact their HIPAA Privacy Officer to ensure that a Business Associate Agreement is in place with the vendor before they are given access to ePHI. The doctor's office should also speak to their HIPAA Security Official for assistance in assuring the implementation of the new system includes appropriate security measures.



URMC/Strong Health HIPAA Security Training Module

POLICY SUMMARY: 0S5

(for full policy, refer to <http://intranet.urmc.rochester.edu/policy/HIPAA/>)

Sanctions

URMC/Strong Health will review all reported violations of URMC/Strong Health's security policies or the HIPAA security regulation and will impose sanctions on responsible members of the workforce as indicated.

Who needs to follow this policy?

Any member of the workforce (staff, volunteers or students) who works under the URMC/Strong Health covered entity, whether or not they are paid for that work.

Who determines what sanctions are appropriate?

The HIPAA Security Official will work with Human Resources, the Medical Director, the Associate Dean for Graduate Medical Education, Office of Counsel and/or senior leadership, whomever is the appropriate contact, when HIPAA security violations arise. The Privacy Officer must also be consulted if the security violation involves a privacy breach.

What types of sanctions will be imposed?

The level of sanction will correspond to the seriousness of the violation and may include, but is not limited to:

1. Termination
2. Loss of medical staff or practice privileges

Other disciplinary actions may include counseling, probation, focused auditing or reporting to legal or regulatory authorities.

What is taken into consideration when a violation is reported?

The HIPAA Security Official and URMC/Strong Health management may consider, among other things, whether or not the violation:

1. Is the first violation or a repeated incident.
2. Was committed with willful intent to do harm.

How will the HIPAA Security sanction be documented?

The HIPAA Security Official will maintain relevant documentation on security sanctions for six years.

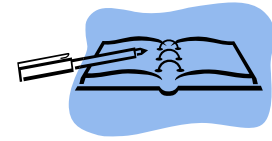
SAMPLE SCENARIOS

Anita is a nurse whose job responsibilities require her to travel between different clinical sites and document patient information on her laptop computer. While Anita ran in to drop off some paperwork at one of her clinical sites, she left her laptop in her car on the front seat. When she returned, she found that her car window had been broken and her laptop had been taken. Anita and her manager notify both their entity Privacy Officer due to the loss/theft of PHI and their HIPAA Security Official since this theft also involved a device containing electronic PHI. What is the proper sanction?

- Upon investigation by the Privacy Officer and HIPAA Security Official, it was determined that Anita did not maintain proper control of her laptop containing PHI by leaving it in plain sight in her car. In addition, she had not password protected her computer as her department had instructed. The HIPAA officers will coordinate with Anita's manager and Human Resources on an appropriate sanction in accordance with this policy.

Chris, a researcher who accesses ePHI as part of his job, decides that he is going to download pictures and music from a number of Internet sites onto his work computer. Chris' actions result in a server crashing, causing a portion of the network to no longer be available to access ePHI to care providers. An investigation by the HIPAA Security Official determines that by downloading this information, Chris was the direct cause of making the system unavailable to get to online patient information. What sanction, if any, should be taken against Chris?

- The HIPAA Security Official, together with Chris' department head/manager and Human Resources will determine an appropriate sanction based on this policy.



URMC/Strong Health HIPAA Security Training Module

POLICY: 0S6

(for full policy, refer to <http://intranet.urmc.rochester.edu/policy/HIPAA/>)

HIPAA Security Training

URMC/Strong Health will implement a security and awareness training program for all workforce members including management. Workforce members will be trained on the HIPAA security policies that pertain to their position. All members of the workforce affected by any material change in relevant policies and procedures will be trained in those changes within a reasonable time after they become effective.

Who needs to follow this policy?

Any member of the workforce (staff, volunteers or students) who works under the URMC/Strong Health covered entity, whether or not they are paid for that work.

What is included in the training?

The Strong Health Security Official has determined that all workforce members are required to read those security training modules that provide a general understanding of the policies for all workforce members. Department heads/managers are required to determine which of the other security training modules are pertinent to their faculty, staff, students and volunteers to be able to perform their daily work.

What is necessary to be in compliance regarding the training?

All workforce members are expected to complete and understand general policies and those policies relating to their job responsibilities and when done, to notify their supervisor for record keeping purposes.

What additional training will be needed?

Additional job-specific training beyond what's developed for those with technical responsibilities will be determined by supervisors who will direct staff to an appropriate resource.

What kind of documentation is needed to show compliance?

Upon completion of the training, documentation by the supervisor/manager for the department must be sent to the appropriate office/department within their organization for tracking and can be kept in paper or electronic format, or in combination, for each entity. All documentation must be kept for six years. (See chart on next page for each entity's process for maintaining documentation.)

Entity	Documentation should be:
SMH, SMD, SON, UHS, Mt. Hope Family Center, Purchasing, EH&S, Audit	Entered into the HRMS system.
Eastman Dental Center	Sent to Senior Operations Administrator, Box 683
Highland Hospital	Entered into the online compliance system.
Highlands of Brighton	Sent to the Staff Development Office
Highlands of Pittsford	Sent to the Education Department
Visiting Nurse Service	Sent to the Education Department

SAMPLE SCENARIOS

Laura is a contractor who works on-site 5 days a week, accessing electronic patient records as well as having direct contact with some patients. What training does she need in addition to HIPAA Privacy training?

- Even though she is a contractor, Laura is considered a member of the workforce and must undergo the same HIPAA Security training as employees in the department in which she works.

Sam is a dishwasher and never has any direct contact with patients or their electronic records. What HIPAA Security training does he need?

- Sam should read the security training modules designed for the general workforce to ensure he has a basic understanding of security policies and procedures, in addition to Privacy training.

Jose is a medical resident who uses his Personal Digital Assistant (PDA) to document patient care. What training does he need?

- Because Jose personally owns the PDA, he is responsible for configuring his system and adding or deleting software programs in a safe manner. Unless Jose has a URMC/Strong Health system administrator who has agreed to maintain the PDA, Jose is the system administrator. He needs to read and understand the HIPAA Security training modules for system administrators in addition to the Security modules for the general workforce.

URMC/Strong Health HIPAA Security Training Module



POLICY SUMMARY: 0S7

(for full policy, refer to <http://intranet.urmc.rochester.edu/policy/HIPAA/>)

Incident Response

URMC/Strong Health workforce members will identify, respond to, and report known or suspected security incidents involving systems that contain or access electronic protected health information (ePHI). Security incidents resulting in harmful effects known to URMC/Strong Health will be mitigated to the extent practical.

Who needs to follow this policy?

All URMC/Strong Health workforce members who access, use, and disclose electronic protected health information (ePHI).

What is a security incident?

An attempt by anyone to inappropriately access, use, disclose, modify, or destroy ePHI is considered a security incident. Additionally, an incident can also be defined as anyone attempting to interfere with the operation of any information system that uses or stores ePHI. A few examples of security incidents are (but are not limited to) -

A person:

- Trying to enter an area where ePHI is stored without having a work-related reason to be in that area.
- Using a shared password to access ePHI.
- Attempting to reconfigure a computer's information system files or purposely installing a virus or 'spyware' on any computer that would result in problems for authorized users.
- Showing/using false identification to gain access to ePHI or to a network or system that stores ePHI.
- Trying to view, modify or destroy ePHI without appropriate access/permission.
- Removing computers or media containing ePHI from the facility without authorization to do so.
- Damaging computers or media so that data confidentiality, integrity or availability is threatened

What are some actions I should take to help minimize the impact of a security incident?

- If it appears there has been unauthorized access to a physical location that contains ePHI, immediately notify the facility's Security Services (public safety staff) or local police if the location is not on a main campus.
- If it appears that a workstation has been compromised, take reasonable steps to contain the incident (for example, shutting down the computer).
- Notify appropriate persons that an incident has occurred (i.e., immediate supervisor/manager, the System Administrator and the entity's HIPAA Security Official and Privacy Officer).

When a security incident is reported, what are the responsibilities of the person who receives the report of the incident?

The manager who receives the report of the incident becomes the *Security Incident Manager* for that incident and is responsible for coordinating communication and documentation of that incident while it is being investigated, until that incident is brought to the next level of authority. *Generally, a workforce member who reports the incident to their supervisor/manager is not the Security Incident Manager; the supervisor assumes the role.*

If the incident needs to be brought to the next level of authority, the original Security Incident Manager no longer fills that role; the person at the next level of authority becomes the Incident Manager. Determination of the level of authority needed is based on the type of incident and the impact it has on the area or system.

Is there anything else the Security Incident Manager needs to do?

He or she is involved on some level in the resolution of the problem and participates in the analysis afterward of why and how the incident occurred so that it does not happen again. He or she is also responsible for documenting their actions and providing the documentation to the next level of authority.

HIPAA Security Officials will be involved in all security incidents, working closely with the Security Incident Manager to determine whether or not the entity's Security Incident Response Team (SIRT) needs to be activated, (the Team is brought in when the event has a significant business impact or is a high threat level).

Please see the Procedural Guidelines for OS7 for full instructions regarding a security incident.

SAMPLE SCENARIOS

A doctor's office has a procedure manual next to the computer used to access patient records. In the manual is a User ID and password for everyone to use to access their patients' information. Is this an acceptable method for accessing ePHI?

- No; everyone needs to access ePHI under their own User ID and password per the regulations. Additionally, leaving a User ID and password out in the open for anyone to see could result in an unauthorized person accessing the information. This incident needs to be reported and the correct procedure for accessing ePHI needs to be put in place.

A computer has been stolen from a nonclinical area. What does the supervisor/manager need to do regarding a security incident?

- In this scenario, since the computer does not contain ePHI, the supervisor needs to follow those procedures that pertain to stolen property. This is not an incident where the HIPAA Security Official would be involved.

A researcher who does not ever access ePHI notices that her computer seems to have been tampered with; does she need to contact the HIPAA Security Official, since this computer is not used to access ePHI?

- Since the computer is connected to the network, the researcher needs to notify her immediate supervisor/manager so that appropriate steps can be taken to determine whether or not the computer has been used to access systems that contain ePHI.

Angela begins to notice the electronic files she routinely accesses for patient record information are either missing or seem to be locked, and she can not gain access to them. She reviews this for several patients and sees that this seems consistent with her search. She becomes suspicious about the record access and availability; what should she do?

- Angela took some initial steps to validate her concerns about being able to access files and became concerned that this could potentially be a security incident impacting ePHI. She needs to report her suspicions to her supervisor immediately.

Michael regularly accesses a locked room in his area that has systems containing ePHI. Michael confirms backups have completed successfully or that media is prepared for data copies that need to be made. While going through his routine, Michael becomes aware that some of the media files seem to be missing. What should he do?

- Michael should notify his supervisor of the missing media files. His supervisor will contact Security Services (public safety staff) or local police because of a possible theft, as well as their HIPAA Security Official and Privacy Officer because the media that is missing contains ePHI.

Carl begins receiving numerous e-mails from unrecognizable e-mail addresses. He suspects that this may be the result of an e-mail Spam attack or a virus. He takes some

initial preventive measures to try to stop the attack by turning off his computer and notifies his supervisor who instructs him to report the incident to their Help Desk.

- The Help Desk person who receives the call receives the details from Carl and becomes the Incident Manager. Carl took a reasonable, immediate action by trying to contain the incident or to minimize impact by turning off his computer. The incident was properly handled, reported, and sent to the next level of authority.