UPMC

Privacy and Security Awareness

Self-Directed Learning Course for All UPMC Staff

Table of Contents

1 - Privacy and Security Awareness Introduction 2

2 - Safeguarding Information 4

3 - Protecting Privacy 6

4 - Protecting Electronic Information 10

5 - UPMC Privacy and Security Policy Overview 17

6 - Reporting Suspected Problems 23

7 - "Red Flag Rules": Reporting Suspected Identity Theft 24

8 - Privacy and Security Glossary 25

This self-directed learning course was developed to meet the training requirement under federal privacy and security laws that apply to, among others, health care providers.

1.0 Privacy and Security Awareness Introduction

Numerous federal and state laws require that UPMC protect information that UPMC creates or collects for a variety of purposes, including patient care, employment, and retail transactions. Education and training are key elements of an effective compliance program. The Privacy and Security Awareness training is an example of UPMC's commitment to educate and promote a culture that encourages ethical conduct and compliance with applicable laws.

After completing this course you should be able to explain:

- your obligations regarding privacy
- your responsibilities for protecting information
- what you should do in the event that you suspect that a breach may have occurred

Additionally, you should become familiar with the UPMC policies that discuss these subject matters. All policies that are mentioned in this guide will be reviewed from time to time and may change. It is your responsibility to periodically check these and become familiar with any changes or updates.

1.1 What is Privacy and Security?

Privacy is UPMC's obligation to limit access to information on a need-to-know basis to individuals or organizations so that they can perform a specific function for or on behalf of UPMC. This includes verbal, written, and electronic information.

- Security — ensure that only those who need to have access to information can access the information. Security also includes ensuring the availability and integrity of information.
- Need-to-know basis — information should only be provided to those who need it to perform their assigned job responsibilities.

1.2 Complying with UPMC Privacy and Security Policies

As an employee, you are to comply with UPMC's privacy and security policies and procedures. To increase patient confidence that information is protected at UPMC, all employees are required to:

- abide by UPMC policies and all applicable laws
- protect patient privacy
- safeguard confidential information
- read and understand policies related to their job function

Every UPMC employee must respect our patients' expectations that their information will be kept confidential.

IT'S TRUE!

On July 20, 2009, the Department of Justice announced that three employees of St. Vincent Infirmary Medical Center (SVIMC) in Arkansas, including the medical director, admitted to accessing patient files out of curiosity. All three employees had received HIPAA training and understood that they were violating HIPAA when accessing the files. The medical director was suspended and the two other employees were fired from their positions. All three were charged criminally and received one year of probation and fines totaling $9,000.

1.3 Consequences for Violating Privacy and Security Policies

Employees who violate any UPMC policy that supports compliance with HIPAA regulations may receive disciplinary action, up to and including termination.

The United States Department of Health and Human Services has appointed government agencies to enforce HIPAA compliance. Those who violate HIPAA can face the following penalties:

- individual fines of up to $250,000
- imprisonment up to 10 years

1.4 What is PHI?

Protected health information (PHI) includes any health information about our patients and is considered confidential. PHI can include, but is not limited to:

- general information:
  - patient's name
  - medical record number
  - social security number
  - address
  - date of birth
- health information:
  - diagnosis
  - medical history
  - medications
- medical coverage information
- dental coverage information

2.0 Safeguarding Information

You are only permitted to access and use patient information as it relates to your job. If you see or hear patient information in the course of doing your job that you do not need to know, remember that this information is confidential. You are not permitted to repeat it or share it with others — even friends, family, or other employees who do not have a need to know it.

- Additionally, you are not permitted to share this information with others when you no longer work for UPMC.
- All UPMC staff members play an important role in safeguarding sensitive information.
- You are obligated to maintain a patient's privacy and safeguard PHI for anyone who receives services at UPMC facilities.

2.1 Information Without Safeguards

An unauthorized individual may be able to gain access to information if sufficient safeguards are not in place. This information may reveal confidential patient, staff, financial, research, or other business information.

Places where this type of information may be accessed:

- computers that were left logged into
- cafeterias or hallways
- fax machines and/or printers
- wastebaskets
- desks or counters

And it could be used in an inappropriate manner to:

- reveal confidential information
- sell information to a tabloid
- cause negative publicity

If this occurs:

- A patient's privacy rights may have been violated.
- State and federal laws may have been violated.
- UPMC and associated staff may be responsible for damages.

2.2 Potential Threats or Activities that May Compromise Information

There are many ways that confidential information can be inappropriately accessed or disclosed. All must be reported to your manager or privacy officer. These may include:

- unauthorized access to information, either by an unauthorized individual or by an individual who has the right to access to information, but accesses the information for unauthorized reasons
- computer viruses
- inappropriately deleting information
- during a burglary, paper information may be accessed or duplicated
- theft of computer equipment, records, and/or information
- unauthorized disclosure of information

WHAT SHOULD YOU DO?

You are called into a patient's room to perform a job assignment. You knock on the door and are invited inside. Another staff person is in the room discussing the patient's treatment plan. What should you do?

If you must do the job immediately to properly care for the patient, announce your presence and what you are there to do. If the job is routine in nature, ask if you may interrupt or if you should come back later. This protects the patient's privacy by allowing the patient to openly discuss his or her condition without being overheard.

3.0 Protecting Privacy

By following certain guidelines, you can protect information and the privacy of our patients. Use the following safeguards in your daily activity.

3.1 Oral Communication

Confidential or sensitive information should only be communicated or accessed on a need-to-know basis. You should access only the minimum amount of this type of information needed to perform your job.

You can maintain privacy by:

- disclosing confidential information only to those who have a need to know it
- speaking in an appropriate tone of voice (lowering your voice when others are nearby and may be able to overhear your conversation)
- moving discussions to areas where others cannot overhear
- asking those around you who do not need to know this information to leave the area so you may have privacy
- avoiding discussions about confidential information in high-traffic areas such as hallways, reception areas, waiting rooms, elevators, and cafeterias.

What Should You Do?

A health care employee was using a cellular telephone when discussing PHI in a restaurant down the street from the hospital. Another hospital employee sitting nearby overheard the conversation and approached the individual. The employee informed the individual that the conversation could be overheard and this was a violation of patient privacy.

The right thing to do:

- Employees should never conduct hospital business and discuss confidential information in public areas.
- All hospital employees have the responsibility to abide by hospital policies and to protect patient privacy.
- Protecting patient privacy is an expectation of all employees, whether on duty or off duty.
- If you overhear others discussing confidential information, let them know that they can be overheard.
- In any event any information that you overhear should not be repeated or communicated to others.
- You should report inappropriate incidents or situations to your hospital's privacy officer.

3.2 Physical Security

Simple measures can be taken to prevent an unauthorized individual from gaining physical access to confidential information.

These measures include:

- Question individuals you do not recognize if they are in or near areas that contain confidential information.
- Offer assistance to those who may be lost.
- Keep file cabinets, doors, and desks locked in nurses' stations, offices, etc.
- Insist that all repair/maintenance personnel show proper identification if they arrive in your work area to service equipment.
- If necessary, call the service company to have the identity of repair or maintenance personnel confirmed.
- Accompany visitors and repair/maintenance personnel to and from their destinations.
- Notify Security when there is an unauthorized individual in a secured work area.
- Restrict access to computers and data centers to prevent unauthorized individuals from accessing electronic information.
- Ensure that all vendor representatives, especially from the pharmaceutical, biotechnology, medical device, and hospital equipment industries, have registered with UPMC Supply Chain Management before they appear onsite. (Visit the Industry Relations Policy section of Infonet for more information.)

3.3 Photocopiers

When making copies of confidential information, you should not leave the copier until your job is complete. Additionally, employees should:

- Remove all papers containing confidential information.
- Check all areas of the photocopier, including the output tray, the input feeder, and the top of the glass surface.
- Not allow others to see the information that you are copying. If someone is standing close enough to see this information, advise him or her that you are copying confidential information. Offer to let the person know when you are finished so that he or she may come back to use the machine.
- Destroy or return to the owner any confidential information that has been left on a photocopier.

IT'S TRUE!

Confidential reports were found in a routine wastebasket on a unit. After an investigation, disciplinary action was taken against the employee responsible for violating UPMC policy.

WHAT SHOULD YOU DO?

You pass by a trash can and notice a stack of photocopied patient records has been placed on top.

You should:

- Gather the records and take them to your supervisor.
- Report this improper disposal violation to your facility's privacy officer so that an investigation can be conducted.

3.4 Fax Machines

The faxing of PHI should be performed only when absolutely necessary. Other, more secure ways of sending information should be considered, such as secure e-mail, registered/insured mail, etc. When you are asked to fax information to a UPMC location, determine if the requester can access the information electronically, which would eliminate the need to fax the information.

If you must fax, use a cover sheet that shows your contact information and contains a confidentiality disclaimer. Use the standardized fax cover sheet (see link below). Additionally, employees should:

- Confirm the fax and telephone numbers of the person you are faxing to.
- Prior to faxing confidential information, let the person you are faxing to know so he or she may retrieve it from the fax machine immediately.
- Follow up with the person to verify that he or she received the fax.
- Immediately remove confidential information from the fax machine.
- Destroy or return to the owner any confidential information that has been left on a fax machine.
- Destroy confidential information that has been received in error and advise the sender of the error.
- Periodically verify that preprogrammed fax numbers are still correct.
- Contact the privacy officer to report inadvertent faxing to the wrong person.
- Consider using other means as opposed to faxing.

Policy HS-EC1607, Retention and Destruction of Health Care Documentation Containing Protected Health Information

UPMC Standard Fax Cover Sheet — http://forms.infonet.upmc.com

3.5 Disposal of Confidential Information

- Never discard paper, computer disks, or other portable media that contains patient information in a "routine" wastebasket. This makes the information accessible to unauthorized personnel. Such confidential information should be discarded in accordance with your business unit's policies regarding the destruction of protected health information.
- Always shred or dispose of confidential information in an appropriate designated container.
- Check with your manager or supervisor to find out how your department disposes of confidential information.

3.6 News Media Inquiries

The news media may contact your facility for information if a well-known person or someone involved in a newsworthy situation, such as an accident, is being treated at your facility.

Direct all news media inquiries to UPMC Media Relations.

3.7 Report Inappropriate Use of Patient Information

If you feel that a patient's privacy or confidentiality has been violated, report the incident to your facility or business unit's privacy officer, your security liaison for electronic security-related issues, or contact the:

- UPMC HIPAA Program Office at 412-647-5757 or hipaaskus@upmc.edu
- Compliance Helpline (anonymous option) toll-free at 1-877-983-8442
- Compliance e-mail address, complianceaskus@upmc.edu

IT'S TRUE!

You are responsible for any activity that takes place under your username and password.

4.0 Protecting Electronic Information

Every UPMC staff member plays an important role in protecting UPMC's electronic patient, business, personnel, academic, and research information. Staff shall take reasonable precautions to ensure that electronic information is available, has integrity, and is secured against unauthorized access.

4.1 Creating and Protecting Passwords

- Passwords are used to verify your identity to a computer system.
- Passwords should be a unique combination of letters, numbers, and symbols.
- Passwords are the electronic equivalent of your signature.
- Do not share your password with anyone (this includes your boss and the information technology staff).
- You are responsible for all actions performed under your username and password.
- Treat your password as you would treat any piece of personal and confidential information by taking measures to keep it confidential.

4.2 Creating Complex Passwords

Creating a complex password — one that cannot be guessed easily by someone else — is one way to protect your password.

- Don't base your password on information that is commonly known about you, such as your birth date, the names of your children or pets, or a hobby.
- It's also best to avoid common words, such as mother or father.

Passwords should meet the following requirements:

- must not contain all or part of the user's account name
- must be at least seven characters long
- must contain characters from three of the following four categories:
  - uppercase characters
  - lowercase characters
  - numbers, 0-9
  - nonalphanumeric characters (!, #, %, *,)

Examples:

- I love to golf! = Iluv2GLF!
- Opera singer = 0praS!ngr
- I owe you $44.95 = iOu$4495

4.3 Protecting Your Password

Once you've selected a complex password, follow these tips to keep it confidential:

- Don't share your password with anyone.
- Memorize your password.
- Never store your password in a computer file or PDA.
- Do not keep a written password in plain view or easily accessible to others. All written passwords are to be kept secured.
- If someone learns your password, you should immediately:
  - Change your password.
  - Tell your supervisor and privacy officer.
- Remember, you are accountable for any actions made under your username and password.

Policy HS-IS0204, Authentication and Access Controls

4.4 Protecting Your Computer from Viruses

A virus is a computer program that performs unexpected or unauthorized actions.

A virus can occur without your permission or knowledge.

Viruses threaten all types of information, can render a system unavailable, and corrupt information contained in a system.

A virus might:

- expose or change confidential information
- delete or remove important files
- display unusual messages
- e-mail everyone in your address book
- disable computers
- spread to other computers

4.5 Signs of a Computer Virus

Contact the ISD Help Desk at 412-647-HELP (4357) or the help desk for your UPMC facility if you notice any of the following, which might indicate your computer is infected with a virus:

- antivirus software pop-up alerts
- missing files
- unusual activity (for example, programs opening that you did not open)
- responses to e-mails that you did not send
- drastic, unexplained reductions in your computer's memory or disk space

TELL ME MORE:
More on Appropriate Use of E-mail

Delete unnecessary e-mail.

If you have not done so already, add the following disclaimer to all your e-mail messages. This disclaimer can be found in policy HS-IS0147, Electronic Mail and Messaging, in the system-wide policy manual on Infonet.

This e-mail may contain confidential information of the sending organization. Any unauthorized or improper disclosure, copying, distribution, or use of the contents of this e-mail and attached document(s) is prohibited. The information contained in this e-mail and attached document(s) is intended only for the personal and confidential use of the recipient(s) named above. If you have received this communication in error, please notify the sender immediately by e-mail and delete the original e-mail and attached document(s).

4.6 Preventing Viruses

Precautions that you can take to help protect your computer from becoming infected with a virus are:

- Never open or run unexpected e-mail attachments or other programs.
- Always use antivirus software and never disable it.
- Scan all e-mails and downloads.

Policy HS-IS0211, Open Desktop Computer Configuration

Policy HS-IS0212, Anti-Virus Software Use

4.7 Appropriate Use of E-mail

Electronic mail (e-mail) is provided for the purpose of conducting UPMC business and providing service to our customers. Appropriate use of e-mail can prevent the accidental disclosure of confidential information and the disruption of computer services. As an employee:

- Use e-mail only for official UPMC business and in accordance with UPMC policies.
- Do not use e-mail in a way that is disruptive, offensive, or harmful.
- Do not use e-mail to sponsor or promote a political party or candidate or to campaign against a political party or candidate.
- Do not use e-mail to solicit employees to support any group or organization.
- Confirm destination of e-mail addresses you are sending to.
- Do not use "reply all" unless necessary.

Prior to communicating with patients via e-mail, review the UPMC policy HS-1SO147 (Electronic Mail and Messaging). This will describe the guidelines to follow, such as:

- Getting the patient to sign a consent form.
- Using an appropriately worded footer in e-mails.

4.8 Appropriate Use of E-mail (cont.)

Although it is delivered electronically, e-mail is still a written form of communication. Approach it as you would other forms of written communication, such as a memo or fax. You should:

- Delete unnecessary e-mail.
- Use additional security methods when sending confidential information.
- Include a confidentiality disclaimer on e-mails.
- Don't write something in an e-mail that you would not say in an official memo.

Policy HS-IS0147, Electronic Mail and Messaging

4.9 Printers

Because many employees often share one printer, it is necessary to take measures to protect confidential information when printing.

Follow these steps:

- If your business unit has a Xerox multi-function machine you should use the "Secure" printing option. This means the document will not print until you release it by entering a code number that you select.
- If your business unit does not have a Xerox multi-function machine then you should retrieve your documents immediately.

No matter what type of machine you are printing to, you must:

- Confirm to which printer you are printing, especially if you share a network printer.
- Immediately remove confidential items.
- Cancel or retrieve any confidential information printed on the wrong printer.
- Deliver or dispose of confidential information found on a printer.
- Only print what is necessary if you need to maintain a hard copy.

4.10 Internet Use

The Internet is a great source of information and a way to improve business efficiency.

- UPMC provides Internet access to facilitate business and for educational purposes.
- Do not use the Internet in a way that violates UPMC policies.
- Do not download software that is not approved for UPMC computers, including screen savers and games.
- Do not view information that is offensive, disruptive, or harmful to morale.
- Use antivirus software.

Policy HS-IS0202, Acceptable Use of Information Technology Resources

4.11 Proper Computer Workstation Use

Be sure to restrict the view or access of others by positioning your computer screen so that others cannot view it. Place your computer workstation in a secure area that is not easily accessible by unauthorized personnel. Make sure your screen saver is set to automatically activate and lock your computer and hide confidential information when your computer is not in use. If you cannot restrict others from viewing your screen, ask your manager to order a privacy screen for you that will be placed over your monitor. The privacy screen prohibits people who are not directly lined up to the monitor from viewing the information on the screen. Employees should:

- restrict views of others
- place computers in secure areas
- use automatic screen savers that lock your computer

4.12 Log-on and Log-off Procedures

Follow appropriate log-on and log-off procedures.

- Never use someone else's username and password or allow someone else to use yours.
- Don't offer to log on to a computer so someone else may use it.
- Prevent another person from using your log-on by locking or logging off your computer workstation when leaving it unattended.
- To lock your workstation, press control-alt-delete, and select lock computer.
- Look away when other individuals are entering their passwords.
- Log off a computer when no longer using it.
- Follow these guidelines even when you are remotely logging onto the UPMC system and accessing confidential information.

4.13 Confidential Information Storage

Do not store sensitive and confidential patient information on a local computer workstation (C Drive), laptops (C Drive), and mobile devices such as, flash drives or memory sticks unless you are authorized to do so. Instead, store information on your network shared drive or departmental shared folders.

- If you are authorized to store sensitive and confidential information on removable media such as, CD-ROMs, DVDs, floppy disks, flash drives, or memory sticks, then you must secure this removable media by keeping them in a locked drawer or cabinet.
- Delete files that are no longer needed.
- Secure removable media such as floppy disks, CD-ROMs, DVDs, memory sticks, etc., by keeping them in a locked drawer or cabinet.

4.14 Software Installation/Removal Procedures

Follow software installation and removal procedures:

- UPMC must own a valid software license for all software installed on its computers.
- Unlicensed software shall be removed or a valid license shall be acquired immediately.
- Don't download software that is not approved for UPMC computers.

Policy HS-IS0202, Acceptable Use of Information Technology Resources

4.15 Technical Support

Seek technical support when necessary, especially when installing or removing hardware or software.

- Seek technical support for hardware installation or removal.
- Do not attempt to fix computer problems. You may cause more difficulties by attempting to resolve the problem on your own.
- Do not install or remove hardware, for example, modems, sound cards, video cards, or CD-ROMs yourself. Submit a request to complete the project.
- Contact the Help Desk for your facility for technical support at 412-647-HELP (4357).

Policy HS-IS0217, System Management and Change Control

4.16 Remote Access Procedures

Follow established remote access procedures:

- UPMC offers ways to access its network resources from off-site (remote) locations.
- Contact your Help Desk to discuss these solutions.
- You should not install any hardware, such as a modem or software used for remote connections, on a UPMC computer.
- Always contact your Help Desk for this service.
- Regardless of where you access information, remote or on-site, this information must remain confidential and secure.
- Use approved solutions for accessing UPMC's network.
- Do not install any hardware that would allow remote connections.

Policy HS-IS0219, Secured Remote Access

IT'S TRUE!

An employee's laptop was sent to IT for repair and a rebuild. A diagnostic was performed and it was discovered that the laptop contained PHI. The files were moved to the employee's network drive and deleted from the laptop hard drive. It was also noted that the existing laptop did not have the proper security measures in place, such as encryption software, to protect the data from inappropriate disclosure and/or access. Encryption software was installed before the new laptop was returned to the employee. The employee received corrective action for not following UMPC policy, and a HIPAA refresher was presented at the monthly department meeting.

TELL ME MORE:
Laptops and PDAs

Take the additional following security measures:

- Physically secure laptops and PDAs with locking mechanisms.
- Use the same measures outlined for protecting a computer workstation.
- The use of any unsecured wireless network is not allowed, unless the appropriate approval has been obtained.
- Confidential information should not be accessed using an unsecured wireless network.
- Contact the ISD Help Desk with any questions.

4.17 Laptops and PDAs

Laptops and personal digital assistants (PDAs) often contain confidential information. Therefore, all staff should take the following security measures:

- Physically secure laptops and PDAs.
- Use a password.
- Encrypt information.
- Do not leave a laptop or PDA unattended in a public place.
- The use of any unsecured wireless network is not allowed, unless the appropriate approval has been obtained.
- Confidential information should not be accessed without approval.
- Contact the ISD Help Desk with any questions.

4.18 Disposal of Electronic Media

Electronic media must be disposed of properly.

- Floppy disks, CD-ROMs, DVDs, and backup tapes containing confidential information should be physically destroyed.
- This can be done by using a CD-ROM shredder or placing the items in designated shredding bins, which is the preferred method. Caution: The process of manually breaking a CD-ROM can cause sharp pieces of plastic to fly through the air.
- Special measures must be taken to remove confidential information from fax machines, copiers, printers, and other devices capable of data storage.
- Contact the ISD Help Desk at your facility to have the appropriate technical support staff remove all traces of confidential information from a computer hard drive and other devices.

Policy HS-IS0214, Disposition of Electronic Media.

5.0 UPMC Privacy and Security Policy Overview

You are required to understand all UPMC privacy and security policies.

This section provides an overview of these policies. In addition to these, your business unit or facility may have additional privacy- and security-related policies or procedures.

If you do not understand a policy or procedure, ask your manager for clarification.

Some forms, such as the Authorization for Release of PHI, have been updated in accordance with applicable regulations.

5.1 UPMC Privacy and Security Policies

UPMC developed privacy and security policies that address a variety of topics. Summaries of these policies are on the next several pages. The complete text of these policies can be found in the systemwide policy manual located on Infonet.
http://policymanuals.infonet.upmc.com/System

5.2 Release of PHI

Strict rules apply to the release of PHI when necessary for reasons other than treatment, payment, or health care operations (TPO).

These rules vary based on the sensitivity of the information.

If you are involved with disclosing PHI, you are responsible for being aware of these rules.

Generally patients must sign an authorization to release their PHI if for reasons other than TPO.

If a patient pays for services out of pocket in full, and supplies in writing their request that we do not share this information with his or her insurer, we are not to release the information.

A valid authorization must contain certain information.

Please direct questions related to releasing patient information to your Health Information Management department or your Privacy Officer.

Policy HS-MR1000, Release of Protected Health Information (PHI)

5.3 Notice of Privacy Practices for PHI

The Notice of Privacy Practices is to be posted and made available in public areas of health care facilities, such as a registration area. The notice also must be given to patients during their first visit to UPMC and offered each additional time a patient registers for services. Patients should acknowledge that they have received a copy of the notice. At UPMC, patients acknowledge they have received the notice by signing the Consent for Treatment Form. If you are unable to obtain a patient's acknowledgement, you must document the effort and the reason why the acknowledgement was not obtained. During emergency situations, the acknowledgement should be obtained within a reasonable amount of time.

- All staff should read the Notice of Privacy Practices. The notice may be downloaded from the HIPAA section of UPMC Infonet.
- Notice of Privacy Practices (NOPP) describes:
  - how PHI may be used or disclosed
  - patient rights under HIPAA
  - whom to contact if patients believe their rights have been violated

Policy HS-EC1603, Notice of Privacy Practices for Protected Health Information (PHI) Pursuant to the HIPAA Privacy Rule

5.4 Business Associates (Guidelines for Purchasing)

- A business associate is an external individual, business, or vendor that uses PHI to perform a service or provide a product on behalf of UPMC. These services may include, but are not limited to, legal, actuarial, accounting, consulting, management, administrative, accreditation, data aggregation, or financial services.
- UPMC is required to enter into a contract with a business associate that clearly defines the business associates responsibilities for using, sharing, and safeguarding PHI, including the reporting of any breach of protected health information. For more details about these terms and conditions, business associates should refer to the Purchasing section of UPMC's public website at http://purchasing.upmc.com.
- All business associates must enter into an agreement with UPMC to safeguard PHI.

Policy HS-MM0300, Guidelines for Purchasing (Business Associate Contracts)

5.5 Use of PHI for Marketing

Marketing is defined as any type of communication that seeks to convince an individual to use or purchase a product or service.

UPMC must request and obtain written authorization from an individual to use or disclose his or her PHI for marketing purposes.

Examples not considered marketing:

- face-to-face communications, such as when pharmaceutical samples are given to a patient during a doctor's office visit
- communicating additional treatment options, care management activities, or alternative care settings

Policy HS-EC1610, Use of Protected Health Information for Marketing

5.6 Use of PHI for Fundraising

Fundraising refers to any activity to raise charitable donations that support research, education, or the advancement of health care activities within UPMC.

- Types of PHI that may be used for fundraising purposes without obtaining the patient's authorization must be de-identified and include:
  - demographic information that does not identify the patient (age, race, gender, etc.)
  - dates that health care was provided to a patient
- The Notice of Privacy Practices describes how a patient's PHI may be used for fundraising activities.
- Use of other types of PHI that identifies the patient requires a separate authorization from the patient.

Policy HS-EC1608, Use of Protected Health Information for Fundraising

5.7 Use and Disclosure of PHI for Research Purposes Pursuant to the HIPAA Privacy Rule

All research activities must be conducted in accordance with the rules of the Institutional Review Board (IRB).

- Patients must sign a research authorization for their PHI to be used or disclosed.
- De-identified information (as described in the HIPAA Privacy Rule) may be used for research without the patient's authorization.

UPMC also uses external institutional review boards for clinical trials, such as the Independent Investigational Review Board. For a complete list, contact the UPMC Clinical Trials Office at clinicaltrialsoffice@upmc.edu.

Institutional Review Board of the University of Pittsburgh: www.irb.pitt.edu

Independent Investigational Review Board: www.iirb.com

Policy HS-EC1611, Use and Disclosure of Protected Health Information for Research Purposes Pursuant to the HIPAA Privacy Rules

5.8 Accounting of Disclosures of PHI

- Accounting of Disclosures (AOD) is a summary of where a patient's PHI was disclosed, and includes a list of those people who have received or accessed protected health information.
- Patients have a right to receive an accounting of disclosures, and AODs must be maintained for six years.
  - Subject to a schedule established by federal law, UPMC must provide an accounting of disclosures of all individuals who have received or accessed a patient's electronic record for a period of three years prior to the date on which the accounting is requested.
  - In addition, business associates also will be required to supply an accounting of disclosures when requested.

Policy HS-EC1600, Accounting of Disclosures of Protected Health Information

5.9 Filing a Complaint — Complaint Management Process

- Patients and staff have a right to file a complaint if they feel their privacy rights have been violated. There are many options for filing a complaint.
- Staff can file a complaint by first contacting their manager or supervisor. If they are unable to or uncomfortable with doing so, then complaints can be filed by using the same methods available to patients, as described below.
- Patients (or parent/guardian/other authorized person) can file a complaint by:
  - informing a UPMC employee
    - > Employee receiving a complaint must report it to the entity privacy officer.
  - contacting the entity's privacy officer
  - calling the:
    - > HIPAA Helpline – 412-647-5757
    - > Compliance Helpline – 1-877-983-8442 (anonymous option)
  - Writing (paper or electronic) to the Secretary of the United States Department of Health and Human Services (DHHS), 200 Independence Avenue, SW, Washington, DC 20201

Policy HS-EC1601, Complaint Management Process Pursuant to the HIPAA Privacy Rule

5.10 Patient Access to PHI

Patients have a right to access and review their PHI. A patient must submit a written request and schedule an appointment at the facility where the treatment was provided in order to access his or her PHI.

UPMC may deny a patient access under certain situations:

- contains psychotherapy notes
- compiled for court proceedings
- physician determines not appropriate
- could result in danger to another person
- prohibited by law

Policy HS-MR1000, Release of Protected Health Information

5.11 Employees Accessing PHI

- If an employee has an account for a UPMC clinical system, the employee is generally permitted to access his or her own medical information on that system. The exceptions are that (a) an employee is not entitled to access his or her behavioral health or drug/alcohol treatment information; (b) UPMC reserves that right to limit an employee's access to his or her medical information on UPMC Clinical Systems; and (c) an employee's use of UPMC clinical system must not interfere with the employee's or other staff's work.
- Employees are prohibited from accessing medical records of their spouses, children, relatives, and others.
- Employees are permitted only to access information needed to perform their job.
- Employees will be subject to disciplinary action if PHI has been accessed inappropriately and may be subject to fine, imprisonment, and termination.

5.12 Patient Amendment of PHI

Patients may request to amend or correct their PHI, if they feel that UPMC has recorded incorrect or incomplete information about them. A patient who wants to amend his or her PHI must make a written request to the facility where the medical information was created. The request must include the reason the information should be amended.

UPMC may deny a request when:

- request to amend is not in writing
- patient does not include a reason to support the request
- information was not created by the facility
- health care provider verifies the existing information is true and accurate

The facility must notify the patient of the outcome of the request to amend, approved or denied, in writing. The patient may submit a statement of disagreement, which will become part of the patient record when an amendment request is denied.

Policy HS-EC1609, Patient Amendment to Protected Health Information

5.13 Minimum Necessary Standards for Using PHI

- PHI is available to UPMC staff on a need-to-know basis.
- Need-to-know means that you rely on or need PHI in order to do your job.
- However, you should access only the minimum amount of information that you need to perform your job.
- For example, all of the patient's health information is available for a physician, nurse, or other staff member to use to provide direct patient care. However, this same information is not available to the hospital's telephone operator. The need-to-know information the telephone operator requires is the patient's name and room number. Accessing patient information that is not relevant to your job may result in disciplinary action, up to, and including termination.
- A log of all users accessing PHI via electronic means is available to monitor this.

5.14 Minimum Necessary Standards for Disclosing PHI

If you are required to disclose PHI to someone for purposes other than treatment, payment, or operations, such as a court order, you must verify:

- who the requesting party is
- that they have a need-to-know this information
- that only the minimum necessary information is provided.

If a patient pays for services out of pocket in full, and supplies in writing his or her request that we do not share this information we are not to release the information.

Questions regarding the minimum necessary standards for using or disclosing PHI should be directed to your privacy officer or Health Information Management (medical records) department.

Policy HS-EC1602, Minimum Necessary Standards for the Use and Disclosure of Protected Health Information

6.0 Reporting Suspected Problems

It is every staff member's responsibility to be alert to unethical behavior or possible violations of UPMC policies.

There are many examples of inappropriate use or disclosure of protected health information. These include, but are not limited to:

- Faxing — If the patient's information is sent to the wrong fax number or wrong location, the doctor's office or requesting agent must be reported to either HIM or your privacy officer.
- Patient Identification — If a patient presents with identification that does not appear to be consistent with existing information, alert your privacy officer to notify him or her of the possibility of identity theft.
- Access/Disclosure — All inappropriate PHI access, or a suspected breach in security, shall be reported in accordance with appropriate UPMC policies.
- Communicate your concerns and observations in a manner consistent with the chain of command. You should first contact your manager if you need assistance. If you are not comfortable with following, or unable to follow, the chain of command, the following additional resources are available:
  - privacy officer
  - compliance officer
  - Corporate Compliance Office
  - Human Resources
  - Legal
  - UPMC Compliance Helpline toll-free at 1-877-983-8442 (anonymous)

UPMC prohibits retaliation against anyone for raising, in good faith, a concern or question about inappropriate or illegal behavior. Retaliation is not allowed against anyone participating in an investigation or providing information related to an alleged violation.

Policy: HS-EC1802, Reporting and Non-Retaliation Policy

7.0 "Red Flag Rules": Reporting Suspected Identity Theft

Congress enacted the Fair and Accurate Credit Transaction Act (FACTA) of 2003, which amended the Fair Credit Reporting Act (FCRA), in response to the increase in identity theft. Subsequently, the Federal Trade Commission (FTC) issued the "Red Flag Rules."

The Red Flag Rules aim to protect the consumer from identity theft. The rules require that any business entity ("creditors") that maintains an account ("covered account") that allows deferred payment and/or credit to a client must implement a program to identify, detect, and respond to identity theft.

Identity theft occurs when someone uses another person's personal information (e.g., name, address, Social Security number, credit card number insurance information, or other identifying personal information) to fraudulently obtain medical services.

Red flags are defined as any pattern, practice, or specific activity that could indicate identity theft.

If you suspect that identity theft has occurred, communicate your concerns and observations in a manner consistent with the chain of command. You should first contact your manager or supervisor, who will perform an initial investigation. If you are not comfortable with following, or unable to follow, the chain of command, additional resources are available:

- privacy officer
- compliance officer
- UPMC Compliance Helpline toll-free at 1-877- 983-8442 (anonymous)

Policy HS-EC1804, Identity Theft Policy

5.17 Theft and/or Breach of Personal Information

In General:
A "breach" occurs when there is an unauthorized acquisition, access, use, or disclosure of PHI. If you suspect that a breach has occurred, you should notify your supervisor or privacy officer immediately. If it is determined that there was a breach, UPMC will need to report the breach, including providing written notification to the affected patient(s).

Example:
Without a work-related need, a nurse intentionally opens her co-worker's record.

Exceptions:
There are a variety of exceptions where a breach does not need to be reported, including situations where it is unlikely that the information could be misused. However, the decision whether or not to report it may only be made following an investigation by UPMC.

Policy, HS-EC1803, Theft and/or Breach of Personal Information

8.0 Privacy and Security Glossary

Accounting of Disclosures:
The accounting of disclosures is a summary containing certain information that tells a patient to whom their PHI was released.

Authorization:
A patient's written permission to disclose PHI for reasons other than providing treatment, obtaining payment, or performing related health care operations.

Breach:
The term breach means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the information, except where the unauthorized person to whom the information is disclosed would not reasonably have been able to retain the information.

Examples:

- Without a work-related need, a nurse intentionally opens her co-worker's record without his consent.
- Mailings were crossed.

Exceptions:
The term "breach" does not include:

- Any unintentional acquisition, access, or use of PHI by an employee or individual acting under authority of a covered entity or business associate if:
  - the acquisition, access, or use was made in good faith
  - the information is not further acquired, accessed, used, or disclosed
- any inadvertent disclosure from an individual who is otherwise authorized to access PHI.
- any information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

  Examples:
  - Patient complains he or she overheard his or her information being openly discussed; this is unintentional human error.
  - A financial clerk enters the patient information number to enter charges, but realizes after opening that he or she entered the wrong number and immediately exits the account.

Business Associate:
Any individual, business, or vendor that is not part of UPMC and has access to PHI to perform a service or provide a product. Examples are answering services, computer companies (EPIC), consultants hired to assist with billing, shredding companies, courier services, cleaning companies, medical records copy services, transcription companies, and records storage companies. A business associate also may be a covered entity (see definition of covered entity).

Covered Entity:
A covered entity is a provider of medical and/or health services or any other person or organization that performs services for the provider, bills, or is paid for health care in the normal course of business. Examples are health care providers, insurance companies, billing companies. A covered entity also may be a business associate (see definition of business associate).

De-identified Information:
Information that does not allow an individual to be identified because specified personal identifiers have been removed, such as name, social security number, date of birth, etc.

Disclosure:
Sharing or divulging PHI with anyone outside UPMC. UPMC Health Plan is considered a separate covered entity. Note: The appropriate use or disclosure of PHI depends on its intended purpose and the existence of an authorization.

Electronic Health Record:
The term electronic health record means an electronic record of health-related information about an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Health Care Operations:
- Activities related to the operation of UPMC. These may include, but are not limited to conducting quality assessment and improvement activities.
- reviewing the competence or qualifications of health care professionals
- conducting or arranging for medical review, legal services, and auditing functions
- business planning and development
- management activities related to compliance

Minimum Necessary:
Limits the access and disclosure of PHI to that which is reasonably necessary to achieve the business purpose.

Need-to-Know Principle:
Private and confidential information should be accessed by employees only when performing their job responsibilities.

Payment:
Billing and receiving payment for treatment provided to a patient. This also includes obtaining preapproval for future treatment.

Personal Health Record:
An electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources or that is managed, shared, and controlled by or primarily for the individual.

Protected Health Information (PHI):
Information that could identify a patient, such as his or her name, medical record number, Social Security number, address, date of birth, and health details (diagnosis, medical history, etc.), in any medium (oral, written, computer systems, etc.), collected and directly used for documenting health care or health status.

Examples are the patient's name, date of birth, Social Security number, phone number, diagnosis, and test results; even the fact that the person is a patient of a specific office or that the person has an appointment with a particular doctor, is confidential.

Release of Information:
Strict rules govern the release of PHI when PHI is not used for transactions related to treatment, payment, or health care operations. These rules vary based on the sensitivity of the information. If you are involved with releasing PHI, you must understand what type and under what circumstances information may be released.

Research:
A systematic investigation, including development, testing, and evaluation designed to develop or contribute to general knowledge. This includes the development of research repositories and databases for research.

Treatment:
Providing health care services to patients.

Use:
Refers to sharing PHI within UPMC, excluding UPMC Health Plan.
Note: The appropriate use or disclosure of PHI depends on its intended purpose and the existence of an authorization.

Workforce:
Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of the covered entity, whether or not they are paid by the covered entity.

Contact/Help Information

UPMC Ethics and Compliance Office:
412-647-5774 or complianceaskus@upmc.edu

HIPAA Program Office:
412-647-5757 or hipaaskus@upmc.edu

Compliance Helpline:
1-877-983-8442 (toll-free)

Infonet:
HIPAA FAQs — http://hipaa.infonet.upmc.com/FAQ.htm