



UPMC Privacy and Information Security Policies

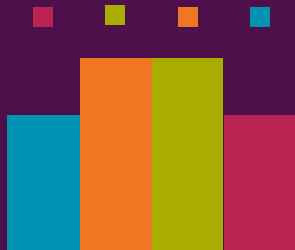
Author(s):

Written by:
**ISG/Office of Patient and
Consumer Privacy**

In conjunction with:
Learning & Development

Objectives

- Identify key concepts from UPMC policies on Privacy and Information Security
- Describe appropriate use and safeguarding of Confidential Information, including Protected Health Information, governed by standards established under UPMC policies in accordance with applicable laws and regulations
- Recognize that the content of this course is not intended to replace the full content of the UPMC policies referenced; it is designed to serve as an aid in promoting awareness and implementation of the policies



Privacy and Information Security

System-wide and local policies intended to protect and promote the Privacy and Security of information are actively maintained by UPMC

Training related to Privacy and Information Security policies must be completed by all UPMC staff, so that UPMC's Code of Conduct, policies, and procedures are known and complied with

- Privacy and Information Security procedures should be reinforced by each department via orientation training to all new staff
- Complete annual mandatory refresher trainings must be completed by all staff

HS-EC1606 Privacy and Security Training Related to Protected Health Information (PHI) HS-HR0736 Confidential Information

Privacy and Information Security

- UPMC is committed to ensuring that our patients', health plan members', and employees' information remains secure and confidential
- The protection of Confidential Information, including Protected Health Information, against inappropriate disclosure, loss, tampering, or use by unauthorized persons is the responsibility of all UPMC staff
- All obligations referenced in this training are rooted in UPMC policy
- Individuals who violate UPMC policy are subject to corrective action pursuant to UPMC policy, and may be individually liable pursuant to underlying applicable law and regulation

HS-EC1606 Privacy and Security Training Related to Protected Health Information (PHI) HS-HR0736 Confidential Information

HIPAA

HIPAA: Health Insurance Portability and Accountability Act

The handling of Protected Health Information, including how it can and cannot be used, how it must be protected, and how patients may access it is regulated by federal law

HIPAA is enforced by the United States Department of Health and Human Services, Office for Civil Rights

Violations of HIPAA are punishable by:

- Civil penalties of up to \$50,000 per violation, with an annual maximum of \$1.5 million
- Criminal penalties of up to \$250,000 in fines and 10 years in jail

Protected Health Information (PHI), defined

- Individually identifiable health information that is created, received, transmitted, or maintained by a HIPAA Covered Entity (such as UPMC) or its Business Associate(s), through which a patient may be identified in any way
- Information relevant to past, present, or future physical or behavioral health condition, provision of health care, and payment information are considered to be PHI
- Clinical and demographic information are both considered to be PHI
- Information in electronic, printed, and oral forms are covered under this definition

Protected Health Information (PHI), defined

- Name
- Social Security Number
- Address or any geographic subdivision smaller than a State
- Email address
- Telephone/fax numbers
- Dates: birth, service, admittance, discharge, death
- Full face or other identifying photographs
- Device identifiers and serial numbers
- Biometric identifiers
- IP/URL address
- Driver's License Number
- Account, insurance, certificate, license plate/vehicle, or medical record numbers

Confidential Information

- Protected Health Information (PHI), business and employee information, and any other information required to be protected under any applicable federal, state or local law are all considered to be Confidential Information
- Confidential Information (inclusive of PHI) may be accessed, used, or disclosed on a need to know basis for a legitimate business purpose only, which includes treatment, payment, or healthcare operations (TPO)
- Only the minimum amount of information necessary should be involved in an appropriate access or disclosure of Confidential Information

HS-HR0736 Confidential Information

Confidential Information – TPO Definition

Treatment: Provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another

Payment: Activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care

- Includes (but is not limited to) billing/collection, risk adjustments, utilization review, determining eligibility or coverage

*HS-HR0736 Confidential Information
HS-MR1000 Release of Protected Health Information*

Confidential Information – TPO Definition

Health Care Operations: Administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment

- Includes (but is not limited to) quality assessment/improvement, case management/coordination, training, accreditation, certification, licensing, performance evaluation, resolution of grievances, cost-management, etc.

*HS-HR0736 Confidential Information
HS-MR1000 Release of Protected Health Information*

Confidential Information

“Need to Know”

- Staff access to patient information is limited to the minimum amount necessary for them to do their jobs
- Inappropriate access, use, or disclosure of Confidential Information by any staff person shall be cause for corrective action

Confidential Information

Confidential Information can be safeguarded by adhering to privacy policies:

- Discussions in high-traffic areas like hallways, elevators, and cafeterias should be avoided; these should be moved to other areas where Confidential Information will not be overheard
- Anyone without a job-related need to know should be asked to leave the area for to ensure the privacy of Confidential Information being discussed
- Physical access to areas containing Protected Health Information (PHI) or other Confidential Information must be secured at all times
- Appropriate authorizations should be obtained, and all recipient identity and contact information should be confirmed prior to the transmission of any Confidential Information
- PHI, other Confidential Information, or references to the same should never be posted on any social media or social networking sites

HS-HR0736 Confidential Information

Confidential Information

Confidential Information can be safeguarded by adhering to privacy policies: (continued)

- Printed documents should always be shredded or disposed of appropriately
- Confidential Information received in error should always be destroyed
- A clean desk and a clear screen should be kept to avoid accidental exposure of information
- Computers must always be locked and physical documents secured before being left unattended
- Printed information should not be left unattended at printers or fax machines
- Fax cover sheets should always be used; when a secure printing function is unavailable, the destination printer should be identified so that printed material can be collected immediately
- PHI or other Confidential Information should not be taken off-site unless absolutely necessary; it should be transported in a secure and appropriately marked container

HS-HR0736 Confidential Information

Confidential Information and Physical Access

- Access to areas containing Confidential Information must be limited
- The movement of people, equipment, and supplies into or out of areas containing Confidential Information should be monitored
- A mechanism for controlling the access of people and the movement of equipment and supplies must be used within secure areas
- UPMC Identification badges should be displayed at all times

*HS-HR0736 Confidential Information
HS-IS0205 Physical Access*

Physical Access

- UPMC computers should be accessed by authorized personnel only
- Staff access to information and locations must be limited to the minimum amount necessary for them to do their jobs
- Access to data centers and support areas containing electronic Confidential Information must be controlled, including limiting entry and monitoring movement of people, equipment, and supplies into or out of any area containing such information
- Staff physical access requirements must be periodically reviewed by UPMC managers and sponsors via the Identity Management System (IMS); staff access must be updated any time any responsibilities change

Notice of Privacy Practices

- UPMC's Notice of Privacy Practices ("Notice") informing patients of how UPMC may use and disclose their Protected Health Information (PHI) must be received by all patients
- The Notice must be provided no later than the date of the first delivery of service in non-emergency situations; it must be posted in patient registration areas, and is also made available online and by verified email transmission when individuals so authorize
- Individual rights and UPMC's duties with respect to PHI are defined within the Notice

*HS-EC1603 Notice of Privacy Practices for Protected Health Information
Pursuant to HIPAA*

Release of Protected Health Information (PHI)

- A valid patient authorization is required to disclose PHI to a third party for non-TPO purposes unless the disclosure falls under a specific exception as outlined in policy
- A valid patient authorization must contain various criteria, including, but not limited to:
 - Patient Full Name
 - Identification information (DOB, MRN)
 - Specific purpose of the disclosure
 - The exact information to be disclosed
 - Dates of treatment
 - Entity of the encounter
 - Name and address of recipient
 - Dated Signature of the recipient
- Oral authorizations may be accepted in emergency situations, and are not appropriate for additionally protected/sensitive information as defined in policy
- Patient approval or authorization of any discussion of PHI with or in front of others (visitors, family) is required before discussions take place

HS-MR1000 Release of Protected Health Information

Release of Protected Health Information (PHI)

- Disclosures of PHI must be limited to the minimum amount of detail necessary to satisfy the request
- Certain types of information may be additionally protected and require specific authorizations before disclosure, including information pertaining to
 - Drugs and Alcohol
 - Behavioral/Mental Health
 - HIV Status/Treatment
- The Risk Management Department, Legal Department, and Health Information Management leadership should be consulted for any questionable requests for release of PHI, including, but not limited to all requests involving court orders, subpoenas, and warrants
- News media inquiries should be directed to UPMC Media Relations

HS-MR1000 Release of Protected Health Information

Release of Protected Health Information (PHI)

It must be determined by UPMC if a patient has requested a restriction of information under the American Recovery and Reinvestment Act (ARRA) before responding to a request for PHI from an insurance company, for payment or healthcare operations purposes

When a patient is designated as “self-pay” for a service/encounter and has requested that related information be restricted and not disclosed to the insurance company for payment or healthcare operations purposes, UPMC must comply with the request

Release of Protected Health Information (PHI)

- A patient's PHI may be reviewed and a copy requested by the patient and/or their legal representative; a copy may also be directed to a third party in any form or medium maintained by UPMC
- A formal authorization form may be used but is not required as long as it is confirmed that the request is from the patient or their legal representative, is in writing, and otherwise contains all required information
- A reasonable cost-based fee may be charged for provision of a copy of patient PHI in accordance with the fee structure approved in UPMC policy
- A Personal Representative may be designated by a patient to act on the patient's behalf to make appointments, to have discussions with health care providers regarding routine tests and treatment, and to be granted limited medical information as necessary to facilitate such discussions, via use of Personal Representative Designation Form

HS-MR1000 Release of Protected Health Information

Release of Protected Health Information (PHI)

Restrictions on the use and disclosure of PHI may by right be requested by patients; requests are considered but not guaranteed by UPMC

Requests for restrictions:

- Request must be submitted in writing
- Request must be made to the UPMC entity at which the patient received services
- PHI the patient wishes to have limited must be defined
- Patient's choice to limit the use of information, the disclosure of information, or both, must be delineated
- Person or entity to which the restriction applies (for example, a spouse) must be named

*HS-EC1602 Use and Disclosure of Protected Health Information, Including:
Fundraising, Marketing and Research
HS-MR1000 Release of Protected Health Information*

Release of Protected Health Information (PHI)

UPMC Personnel with access to the electronic medical record systems for work purposes are permitted to access their own medical records on a limited basis, with exceptions:

- Billing and registration information may not be accessed
- Information may not be altered in any way
- Highly sensitive information such as information related to substance use, behavioral or mental health and HIV test result information may not be accessed
- Access cannot impede or affected work performance the delivery of services

UPMC Personnel access to any other person's medical records, without having a legitimate TPO purpose, is strictly prohibited

- Employees are prohibited from directly accessing the records of family or friends using UPMC Medical Records system, even if asked to do so via a Personal Representative Designation or any other authorization form. This does not preclude using the MyUPMC web portal as a proxy.

HS-MR1000 Release of Protected Health Information

Accounting of Disclosures

- With limited exceptions, disclosures of Protected Health Information (PHI) that are not for Treatment, Payment, or Health Care Operations (TPO) purposes must be documented in UPMC's Accounting of Disclosures database, which is accessible via IMS
- Disclosures must be tracked, including those related to a subpoena, court order, search warrant, for disease reporting to the Department of Health, providing information to health care registries, and any breach of PHI
- An Accounting of Disclosures showing to whom and for what reason PHI was disclosed may, by right, be requested by a patient for a period of up to 6 years prior to the date of the request
- A report of logs showing who has accessed their electronic health record may, by right, be requested by a patient for a period of up to 3 years prior to the date of request

Fundraising, Marketing and Research

Use and Disclosure of Protected Health Information, Including: Fundraising, Marketing and Research

- A minimum of detail should be used when accessing, using, or disclosing Protected Health Information for a legitimate need-to-know purpose
- The traditional provision of clinical care, billing, and registration activities should be considered legitimate purposes
- Other activities governed by specific policies including marketing, fundraising, and research. All have specific requirements regarding when such uses and disclosures are acceptable

*HS-EC1602 Use and Disclosure of Protected Health Information, Including:
Fundraising, Marketing and Research*

Fundraising, Marketing and Research

Use and Disclosure of Protected Health Information, Including: Fundraising, Marketing and Research

A valid patient authorization and provision of UPMC's Notice of Privacy Practices are required to use Protected Health Information (PHI) for Marketing purposes, with limited exceptions

PHI communication IS NOT considered to be Marketing:

- If it is made to describe a health-related product or service that is provided by or included in a plan of benefits
- If it used for treatment purposes
- If it is used for case management or care coordination

*HS-EC1602 Use and Disclosure of Protected Health Information, Including:
Fundraising, Marketing and Research*

Fundraising, Marketing and Research

PHI communication IS considered to be Marketing:

- If it encourages recipients of the communication to purchase or use the product or service,
OR
- If PHI is disclosed to a third party in exchange for direct or indirect remuneration in order for the third party (or its affiliate) to promote the purchase or use their own product or service

*HS-EC1602 Use and Disclosure of Protected Health Information, Including:
Fundraising, Marketing and Research*

Use of Protected Health Information

Use and Disclosure of Protected Health Information, Including: Fundraising, Marketing and Research

Protected Health Information may be used for Fundraising purposes without first obtaining an authorization, provided that UPMC's Notice of Privacy Practices (containing a statement that the individual may be contacted by UPMC Fundraising staff) has been received by the patient

- “Fundraising” is defined as the organized activity of requesting charitable gifts in support of research, education, training, or other aspects of the advancement of health care delivery
- Clear instructions on how to opt out of Fundraising communications must be provided to current/prior patients within all fundraising solicitations, whether verbal or in print; authorization is required for the use of certain types of information for used Fundraising purposes, such as diagnosis, nature of service, or treatment

*HS-EC1602 Use and Disclosure of Protected Health Information, Including:
Fundraising, Marketing and Research*

Use of Protected Health Information

Use and Disclosure of Protected Health Information, Including: Fundraising, Marketing and Research

- PHI may also be used for Research purposes if the patient-subject has received UPMC's Notice of Privacy Practices, has signed a TPO Consent, and has completed a valid Research Authorization form (or if a waiver has been approved)
- Institutional Review Board (IRB) approval is required to conduct any Research activity; a separate privacy board is not operated by UPMC
- All Research-related policies, procedures and supporting offices should be reviewed and understood by individuals involved in research in any capacity

*HS-EC1602 Use and Disclosure of Protected Health Information, Including:
Fundraising, Marketing and Research*

HS-PS0497 IRB Approval of Human Subjects Research at UPMC

HS-RS0004 Research and Clinical Training Involving Decedents

HS-RS0005 Research Using UPMC Electronic Protected Health Information (e-PHI)

Sale of Protected Health Information Prohibition

Direct or indirect payment in exchange for disclosure of Protected Health Information (PHI) is not received by UPMC unless a valid patient authorization specifically stating that such information can be exchanged for payment is in place, or if an exception applies

- Exceptions are noted in policy, including but not limited to the following
- Exchange of PHI is made in return for treatment
- Exchange of PHI is to made to pay a vendor for services provided to/on behalf of UPMC pursuant to a Business Associate Agreement
- Exchange of PHI is made for health care operations
- Exchange of PHI is to made to provide an individual with a copy of their record

Guidelines for Business Associates

- A vendor is considered a Business Associate (BA) of UPMC when it accesses, creates, or receives Protected Health Information (PHI) in the course of providing services to UPMC
- A Business Associate Agreement (BAA) is established to obligate the UPMC Vendor to appropriately manage and safeguard PHI that is accessed, used, or disclosed by Vendor in the course of providing services to UPMC
- The BAA is established through UPMC Supply Chain Management
- A BAA must be established with all BAs to ensure that PHI is appropriately used and protected

Restriction on Patient/Resident Information

- A Directory may be maintained at UPMC facilities to allow for the locating of patients/residents
- Visitors or members of the clergy may be directed to patients/residents via the Directory when the patient is asked for by name
- A patient's/resident's name may be removed from the Directory at the patient's request; this Information Block can be extended by the patient to specify that information released is limited to specific individuals
- Patients being treated for a sensitive matter may be automatically placed on an Information Block (violent trauma, child abuse or neglect, behavioral health, substance abuse/drug/alcohol treatment)

*HS-EC1605 Facility Directories and Information Restriction on
Patient/Resident Information
(Information Block)*

Handling Protected Information Outside UPMC

Proper Handling of Protected Health Information Outside of UPMC

- Protected Health Information (PHI) should be taken off-site only when absolutely necessary for job related reasons
- Personnel removing PHI from UPMC property are required to take all necessary precautions to protect and safeguard the information, including completing all required forms and notices, transporting the information in a secured container, and never leaving the information unattended (even in a locked vehicle)
- While off site, safeguarding the information is the sole responsibility of the individual who removed it from the premises
- The information should be returned to the UPMC facility as soon as possible, and if no longer needed should be disposed of properly on site at UPMC

HS-EC1615 Proper Handling of Protected Health Information Outside of UPMC

Disposition of Electronic Media

All storage media and portable devices capable of storing data that contain UPMC information, whether encrypted or unencrypted, functional or not, must be removed from service using standards established by the Information Services Division (ISD) of the UPMC Information Security Group (ISG)

- Examples of media and devices include but are not limited to hard drives, removable drives, optical disks, floppy disks, USB memory devices, magnetic tapes, cellular phones, PDAs, smart phones

Failed storage media and portable devices containing UPMC information will be destroyed by a certified third party data destruction company in an environmentally responsible manner and in compliance with appropriate security standards established by the ISD ISG

Authentication and Access Controls

- Information access is limited by “Need to Know” and “Minimum Necessary” principles, based on staff role and job responsibility
- In addition to the use of multiple factor authentication, one or more approvals (supervisor, application owner, others) may be required in order to secure access to higher level data applications
- Employee, non-employee, and third-party access to data is controlled by the supervisor or sponsor via Identity Management System (IMS); access must be reviewed on an annual basis or when there is a change in responsibility

Photographing, Filming and Recording

Photographing, filming or recording within UPMC facilities is governed by policy

- Photographing, filming or recording within a UPMC facility by any UPMC Personnel or UPMC Vendor should only occur within a facility if it is appropriate and necessary for a business, education or patient care purpose, or if it is otherwise approved by a member of Executive Management of the UPMC facility in question
- Such activity by a patient, a patient's family member, or patient's visitor may be prohibited for any reason
- In no case can such activity by a patient, a patient's family member, or a patient's visitor be permitted where it includes other patients or UPMC Personnel, or when it otherwise affects the privacy rights of a patient or a staff member; an exception is found, in accordance with UPMC policy, in the limited case of the recording of the birth of a baby

HS-FM0214 Photographing, Filming and Recording within UPMC Facilities

Social Networking

Social Networking use must be approved by UPMC Corporate Communications; it shall **not** be used by UPMC Personnel in any way that would risk, cause, or suggest:

- The compromise or disclosure of Protected Health Information or other protected personal or financial information of any patient or patient family, including photographs of employees engaged in patient care
- The disclosure of any business-related, technological or academic information related to the activities and operations of UPMC
- The posting of erroneous information misstating facts about UPMC, its employees and representatives; slanderous, libelous or otherwise offensive material according to policy
- The making of any promise on behalf of UPMC, including unapproved use of Brand Identity (logos, copyrighted materials, taglines) which may communicate endorsement or participation

HS-HR0748 Social Networking

HS-IS02 Acceptable Use of Information Technology Resources

Reporting and Non-Retaliation

- Instances of wrong-doing must be reported by employees to the appropriate UPMC Personnel or designated officials, or via UPMC Compliance Hotline
- An employee, patient, or other third party who reports an issue or files a complaint in good faith will not be subject to retaliation by UPMC
- Policies are maintained that further provide for whistleblower protections, a harassment-free workplace, and corrective action in response to the filing of false claims

Complaint Management

Complaint Management Pursuant to the HIPAA Privacy Rule Theft and/or Breach of Personal Information that is Maintained by UPMC

Knowledge or suspicion of any actual or potential unauthorized acquisition, access, use or disclosure (i.e. breach) of Protected Health Information (PHI), as well as any complaint regarding the same, must be immediately reported to the appropriate UPMC Privacy Officer, as may be found on Infonet. Such matters may also be reported to:

- Office of Patient and Consumer Privacy, privacyaskus@upmc.edu, 412-647-6286 or 412-647-5757
- Office of Ethics and Compliance, complianceaskus@upmc.edu, 412-647-5774
- Your Human Resources representative or your Manager

*HS-EC1601 Complaint Management Pursuant to the HIPAA Privacy Rule
HS-EC1803 Theft and/or Breach of Personal Information that is Maintained by UPMC*

Complaint Management

Reports must be made immediately to ensure full and timely mitigation, investigation and notification

- Confirmation of the immediate return or destruction of any inappropriately disclosed PHI is essential
- If the breach is deemed to be reportable by the appropriate Privacy Officer, it must be reported to affected individuals, the US Department of Health and Human Services, and other applicable state agencies
- Affected individuals must be notified no later than sixty days after the breach was discovered
- US Department of Health and Human Services notification must be completed annually; it may be required immediately if a breach affects more than 500 individuals
- If serving as a Business Associate, UPMC may be required contractually to provide more immediate notice to affected parties

*HS-EC1601 Complaint Management Pursuant to the HIPAA Privacy Rule
HS-EC1803 Theft and/or Breach of Personal Information that is Maintained by UPMC*

Information Systems Security Policy Administration

Information systems shall be secured to appropriately protect the confidentiality and integrity of all patient, personnel, business, academic, and research information, and to ensure that such information is made available exclusively to appropriate staff on a need-to-know basis

Acceptable Use of Information Technology

Standards for acceptable use of technology resources must be followed by all staff

Best practices to safeguard confidential and protected information, appropriate web use, and methods to control unauthorized visual, physical, or electronic access to data are defined

Examples

- UPMC passwords and data should never be accessed using public computers or networks
- Computer screens should be turned away from public view
- UPMC Confidential Information may not be stored on a remote computer or mobile device not owned by UPMC
- UPMC approved encrypted devices and removable media should be used exclusively
- ISD Help Desk should be contacted at 412-647-4357 for guidance on disposal of electronic media

Acceptable Use of Information Technology

Personnel may be permitted “De Minimis” personal use of UPMC Information Technology, provided that such use does not violate policy, law, or negatively affect performance or operations in any way

All UPMC business information, data and documents should be stored to a network shared drive assigned to the user, to a departmental shared drive, or to an approved secure cloud storage location so that the data is adequately secured, backed up, and not lost upon device replacement or failure

Personally Owned Devices used for business purposes must be configured to meet applicable ISD standards including but not limited to the ability to manage the configuration of the device (including the use of encryption, anti-virus software, and password protection) and the ability to delete UPMC data on the device

HS-IS0202 Acceptable Use of Information Technology Resources

Application Ownership

- All information systems are assigned an Application Owner to ensure that systems comply with and are maintained according to regulations and policy
- All high risk vulnerabilities are remediated by the Application Owner to the extent feasible; written rationale for any vulnerabilities left unaddressed are provided to ISD
- Security incidents or breaches are monitored and reported by the Application Owner
- Life-cycle management of system components, data and software is conducted by the Application Owner when strategies or products are modified or updated
- Application Owners are responsible for service continuity plans and disaster recovery management

*HS-IS0208 Application Ownership
HS-IS0215 IT Service Continuity, Backup and Recovery*

Auditing, Logging, and Monitoring

- Access to UPMC electronic medical records is monitored routinely to verify compliance to privacy policies
- Managers (clinical reviewers) are responsible for review and investigation of log alerts relating to staff activity in electronic medical record systems; manager alert reviews are to be conducted within 10 day of an issued alert
- Access of records for reasons other than legitimate TPO purposes must be escalated to the entity Privacy Officer or Human Resources

Information Systems Response and Reporting

- Any suspected information security incident or breach (real or suspected event that compromises system operation or information security) must be reported immediately to the ISD Help Desk at 412-647-4357 (HELP)
- Any suspicious email received should be reported immediately using the “Report Phishing” button at the top right corner of the Outlook toolbar
- Accidental clicking of a link or opening of an attachment in a suspicious email must be reported immediately by calling the ISD Help Desk

Electronic Mail, Messaging and Texting

UPMC email and messaging systems should be used for official business purposes only

- Secure formatting using the subject line prefix “Secure:” should be used when sending Confidential Information to a recipient outside of the UPMC network
- A confidentiality disclaimer should be included on all electronic communications
- Messages from unsolicited sources should be handled with extreme care; download of files and attachments from unknown origins should be avoided
- Recipients’ email addresses should be verified prior to sending any email message
- UPMC email addresses should not be provided to non-work related entities
- Texting should not be used to transmit PHI

Telecommuting/Working Remotely

Staff working remotely are expected to maintain appropriate data security protocols and to adhere to UPMC policies and standards just as if they were working on site

- Approved remote access tools (MyApps, Direct Access, Office365) should be used when accessing UPMC information systems from off site
- UPMC Confidential Information must not be stored on any remote computer or mobile device not owned by UPMC
- Remote devices must utilize antivirus and spyware detection software, be up to date, and be regularly updated with the latest security patches
- Public computers and unsecured Wi-Fi access points are not secure and should not be used to connect remotely to UPMC

HS-IS0219 Secure Remote Access

HS-IS0202 Acceptable Use of Information Technology Resources

HS-IS0212 Anti-Virus Software Use

Data Encryption and Data Transfer

Data encryption should be employed with digital media storage devices to protect the confidentiality and integrity of stored data, and to protect all confidential data transmitted over non-dedicated or public communication networks, such as the internet

- Confidential information including Protected Health Information (PHI) sent outside of the UPMC system must be encrypted
- Confidential Information includes:
 - Consumer financial and credit information – all account numbers, consumer credit reports
 - Personally Identifiable Information
 - PHI
 - Social Security Number
- Transfers containing PHI must be tracked so that information disclosure may be properly accounted for

*HS-IS0216 Data Encryption
HS-IS0210 Data Transfer*

Use Of Electronic Messaging, Internet, Computer

Summary of proper use of email, internet and computers (pursuant to HS-IS and HS-DG system policy set)

Email and Internet Use:

- Email and internet should be used for official UPMC business only, and must never be used in ways that are disruptive, offensive or harmful
- UPMC email addresses should not be provided to non-work related websites or subscriptions
- Secure email formatting using the subject line prefix “Secure:” should be used when sending Confidential Information to a recipient outside of the UPMC network; inclusion of Confidential Information as part of an email subject line should be avoided at all times
- All email correspondence must include a confidentiality disclaimer
- Destination email addresses should be confirmed prior to clicking “send”
- Emails from unsolicited sources are untrusted; any included links or file attachments should not be used or downloaded

*HS-IS0147 Electronic Mail, Messaging and Texting
HS-IS0202 Acceptable Use of Information Technology Resources
HS-DG3000 Information Ownership and Classification*

Use Of Electronic Messaging, Internet, Computer

Summary of proper use of email, internet and computers (pursuant to HS-IS and HS-DG system policy set)

Password and PC Security Management:

- Strong and unique passwords that are not easily guessed should be used for each system log in; a common password should not be used for multiple systems
- Passwords should not be shared with anyone, including supervisors
- Passwords should not be written down
- Computers/screens should be locked when users step away or leave
- Administrator passwords with elevated privileges must be changed every 30 days
- Passwords that have been compromised should be changed immediately; ISD Help Desk should be notified at 412-647-4357 (HELP)

*HS-IS0147 Electronic Mail, Messaging and Texting
HS-IS0202 Acceptable Use of Information Technology Resources
HS-DG3000 Information Ownership and Classification*

Use Of Electronic Messaging, Internet, Computer

Summary of proper use of email, internet and computers (pursuant to hs-is and hs-dg system policy set)

System Security Best Practices:

- Anti-virus software should be in use at all times, including when working remotely
- Software or content not previously approved by ISD should not be downloaded
- Risk may be minimized by avoiding access of unknown or suspect URLS and websites
- Only ISD-approved file sharing solutions should be used
- UPMC computers, systems, and data should be accessed by authorized individuals only

HS-IS0147 Electronic Mail, Messaging and Texting
HS-IS0202 Acceptable Use of Information Technology Resources
HS-DG3000 Information Ownership and Classification

Resources

UPMC Office of Patient and Consumer Privacy (OPCP)

- privacyaskus@upmc.edu / 412-647-6286 / 412-647-5757

UPMC Ethics and Compliance Office

- complianceaskus@upmc.edu / 412-647-5774

UPMC Fraud Team

- Fraudteam@upmc.edu / 412-647-5774

Information Security Group (ISG) and Technical Support

- SecurityServices@upmc.edu
- imsreq@upmc.edu / 412-647-HELP

UPMC Compliance Hotline

- 1-877-983-8442
- Offers an anonymous reporting option

Additional information can be found on UPMC's Infonet

UPMC System Policy Glossary

- HS-DG3000 Information Ownership and Classification
- HS-DG3001 Use of Test Persons in Production Environments
- HS-EC1600 Accounting of Disclosures of Protected Health Information
- HS-EC1601 Complaint Management Pursuant to the HIPAA Privacy Rule
- HS-EC1602 Use and Disclosure of Protected Health Information, Including: Fundraising, Marketing and Research
- HS-EC1603 Notice of Privacy Practices for Protected Health Information Pursuant to HIPAA
- HS-EC1605 Facility Directories and Information Restriction on Patient/Resident Information (Information Block)
- HS-EC1606 Privacy and Security Training Related to Protected Health Information
- HS-EC1609 Patient Amendments to Protected Health Information
- HS-EC1614 Prohibition on Sale of Protected Health Information
- HS-EC1615 Proper Handling of Protected Health Information Outside of UPMC

UPMC System Policy Glossary, continued

- HS-EC1802 Reporting and Non-Retaliation
- HS-EC1803 Theft and/or Breach of Personal Information that is Maintained by UPMC
- HS-EC1804 Identity Fraud and Theft Program
- HS-EC Other Privacy Related Policies
- HS-FM 0208 / PRO Waste Management
- HS-FM 0214 Photographing, Filming and Recording within UPMC Facilities
- HS-HD-PR-01 Patients' Notice and Bill of Rights and Responsibilities
- HS-HR 0704 Corrective Action
- HS-HR0733 Orientation Period
- HS-HR0736 Confidential Information
- HS-HR0748 Social Networking
- HS-IS0147 Electronic Mail, Messaging and Texting

UPMC System Policy Glossary, continued

- HS-IS0201 Information Systems Security Policy Administration
- HS-IS0202 Acceptable Use of Information Technology Resources
- HS-IS0204 Authentication and Access Controls
- HS-IS0205 Physical Access
- HS-IS0206 Information Systems Incident Response and Reporting
- HS-IS0208 Application Ownership
- HS-IS0210 Data Transfer
- HS-IS0212 Anti-Virus Software Use
- HS-IS0214 Disposition of Electronic Media
- HS-IS0215 IT Service Continuity, Backup, and Recovery
- HS-IS0216 Data Encryption
- HS-IS0217 System Management and Change Control/Management

UPMC System Policy Glossary, continued

- HS-IS0218 Auditing, Logging, and Monitoring
- HS-MM0300 Guidelines for Purchasing Materials, Goods, and Services
- HS-MR1000 Release of Protected Health Information
- HS-PS0497 IRB Approval of Human Subjects Research at UPMC
- HS-RS0004 Research and Clinical Training Involving Decedents
- HS-RS0005 Research Using UPMC Electronic Protected Health Information (e-PHI)
- The UPMC Health Plan (Insurance Services Division) additionally maintains policies and procedures regarding its Privacy and Security program and associated standards as related to its operations

Reminder

UPMC staff encountering a privacy or security issue of any kind (any concern, known or suspected breach, as well as any complaint) shall be responsible for taking immediate action to report the issue

Test Instructions



Passing Score:

Passing score for this training is 80%.



Question Attempts:

You will have ONE attempt to answer each question correctly.



Test Attempts:

If a passing score is not met, you may take the test again.

Test

Quiz - 14 questions

Last modified: Wednesday, July 19, 2017 at 3:27:38 PM

Properties

On passing, 'Finish' button:

[Close window](#)

On failing, 'Finish' button:

[Close window](#)

Allow user to leave quiz:

[At any time](#)

User may view slides after quiz:

[Any time](#)

Show quiz in menu as:

[Single Item](#)



Edit in Quizmaker



Edit Properties