UPMC LIFE CHANGING MEDICINE

PRIVACY AND SECURITY OBLIGATIONS

CONFIDENTIAL INFORMATION

Confidential information includes, but is not limited to:

- Activities or operations of UPMC including physicians, hospitals, laboratories or others.
- Non-public results of research or clinical trials.
- Past, present and future financial information; operating data; organizational and cost structures.
- Protected Health Information (PHI), patient lists, patient identity, patient personal and medical history, patient treatment, all billing and reimbursement information.
- All employment, medical or sensitive personal information of fellow staff members that you receive or obtain at any time during employment.
- Details are included in the following UPMC policies:
  - HS-HR0736, Confidential Information
  - HS-EC1602, Use and Disclosure of Protected Health Information (PHI).

PROTECTED HEALTH INFORMATION

Protected Health Information (PHI) is a specific type of confidential information which includes any known information about a patient, including demographic information such as:

- Name, date of birth (DOB), age
- Specific health information - diagnosis, history, medications
- Social security number (SSN) or medical insurance number
- Photos or pictures of a patient

HIGHLY CONFIDENTIAL PHI

- All information relating to drug and alcohol abuse treatment will be treated as highly confidential, and shall not be disclosed without a valid authorization as previously described.
- HIV related information is also treated as sensitive information, and may likewise not be released without a specific authorization.
- All information related to Mental Health will be treated as highly confidential, and may only be released under specific situations as highlighted in UPMC policy.
- For further information on sensitive information issues, please read HS-MR1000 Release of Protected Health Information.

ACCESSING PHI

Patient PHI may only be accessed, used or disclosed for a legitimate healthcare or business need, or with a proper patient authorization.

Only the minimum amount of information necessary to satisfy the request.

- For further information, please read HS-EC1602, Use and Disclosure of Protected Health Information (PHI) and HS-MR1000 Release of Protected Health Information.

Any access, use or disclosure of PHI not falling under these guidelines must be reported to a manager, Privacy Officer or the UPMC Office of Patient and Consumer Privacy immediately, so that a proper investigation can take place.

- For further information, please read HS-EC1601 Complaint Management Process Pursuant to the HIPAA Privacy Rule.

DISCLOSING PHI?

- If a staff member is unsure if information is confidential or whether it can be disclosed under applicable policy, he or she must ask their supervisor and/or check UPMC policies prior to releasing the information.

REMEMBER: IT IS BETTER TO BE SAFE, THAN SORRY!

- Remember that you MUST notify your supervisor of any legal, government or agency request that you receive, and obtain supervisory consent before disclosing confidential information.
- Any violation of a confidentiality policy may result in corrective action up to, and including, termination of employment.

HANDLING PHI

Do’s and Don’ts

DO: Refrain from disclosing or revealing confidential information to any person, except as specifically necessary to perform your job; consider who may be overhearing your conversations.

DO: Log off or lock your electronic workstation when walking away, or at the end of your shift. Refer to UPMC policy: HS-IS0225, Clear Desk, Clear Screen

DO: Confirm the fax and telephone number of the person you are faxing PHI to.

DON’T: Access PHI of friends, neighbors, family members, VIPs, co-workers and others electronic or paper files, *even if they have asked you to*, except as specifically necessary to perform your job.

DON’T: Leave sensitive information unsecured on your workstation, desk, and/or computer screen, even if you work in a secured unit or administrative area.

PHYSICAL ACCESS - DO'S AND DON'TS

DO: Always wear your ID badge!

DO: Question unfamiliar faces that are not displaying an ID badge, or a visitor badge

DO: Immediately report the loss of ID badge or access key card in accordance with policy

DO: Report any unauthorized or unregistered individuals to the appropriate physical security department

DO: Refer to UPMC Physical Access Policy HS-IS0205 for further details

DON'T: Share your ID badge or allow any other person to borrow your access key card for entry into any secured area.

HANDLING PHI OUTSIDE OF UPMC

UPMC policy HS-EC1615, Proper Handling of Protected Health Information Outside of UPMC gives guidance on how to ensure PHI remains confidential and secure when it is transported physically or transmitted electronically from a UPMC facility. This can include:

- Emailing
- Faxing
- Using mobile devices
- Removable devices such as USB drives
- Transporting paper records
- Mailing or shipping

Reminder:

- PHI should only be taken off site if necessary for your job
- PHI is the sole responsibility of the individual who takes it off site
- PHI must either be encrypted or otherwise secured in the event it is lost or stolen
- PHI should never be left unattended (even if in a locked car)

ACCESSING YOUR OWN PHI

UPMC staff who have otherwise been granted access to UPMC **clinical** systems in order to perform their job duties may access their own PHI **using such systems**, subject restrictions as listed in HS-MR1000 Release of Protected Health Information.

- This permission does not allow an employee to access someone else's records via clinical systems.
  - Employees and non-UPMC employees shall not directly access the medical records of their spouse, children, relatives or others.
  - UPMC will not provide access to UPMC clinical systems to employees solely for the purpose of the employee reviewing his/her PHI.
  - Permission to access one's own medical record does NOT include permission to alter or amend the documentation in any way.
  - Permission to access one's own medical record does not extend to the use of non-clinical systems.
  - You may not access your own records related to HIV, Drug & Alcohol, Mental/Behavioral Health, and/or registration information (including billing information in EPIC and MediPac)

RELEASE OF PHI

- A valid authorization for the release of PHI includes specific information as identified in HS-MR1000 Release of Protected Health Information.
- A patient or their designee has the right to access, inspect and obtain a copy of the information contained in their medical record.
  - The UPMC Authorization for Release of PHI should be utilized for patient access requests.
  - For further information, please read HS-MR1000 Release of Protected Health Information.
  - Permission to access the medical record does NOT include altering or amending the documentation in any way.
    - Please refer to Policy HS-EC1609 Patient Amendment to Protect Health Information for guidance on how to request a change to the documentation.
- HS-MR1000 also cites various scenarios associated with the permitted and conditioned releases of PHI.
    - Please review the HS-MR1000 for further detail as to these guidelines.

PERSONAL REPRESENTATIVE

- Patients may also appoint a personal representative to act on their behalf in the specific situations:
  - Making appointments for health care services
  - Discussions with health care providers about routine tests and treatments that do not require informed consent
  - Access to the information or results contained in the medical record, as necessary, to have discussion with health care providers in relation to the care or treatment provided to the patient
- In order to appoint a personal representative, a Personal Representative Designation Form must be utilized.
  - The form is NOT applicable and cannot be used for UPMC behavioral health patients or for any patient when major health care decisions are involved.
- For further information, please read HS-MR1000 Release of Protected Health Information.

INFORMATION BLOCKS

- An information block refers to the removal of patient identifiers from a facility directory.
- For patients NOT on an information block, minimal information (such as room number) can be disclosed to someone who calls a hospital or facility and identifies the patient by name.
- However, if a patient requests or is placed on an information block, no information is permitted to be released about them.
- Therefore, prior to releasing any information to someone who calls and identifies a patient by name, it should first be checked to make sure the patient is not on an information block.
- Details are included in UPMC policy, HS-EC1605, Information Restriction on Patient/Resident Information (Information Block)

KEEP IT CONFIDENTIAL

Paper/Electronic Media:

- Use “secure print” function when printing to a shared printer.
- All removable media must be encrypted.
- Dispose of confidential information by shredding or using designated containers.
- Ensure confidential information is not accessible to others who do not need to access it.
- Properly dispose of electronic media (CDs, USB drives, etc.) according to the UPMC policy HS-IS0214, Disposition of Electronic Media

Social Media:

- Know your responsibilities as a UPMC staff member regarding the use of social networking media.
- The Social Networking page on the Infonet has been designed as a resource for employees.
  - See policy, HS-HR0748, Social Networking.
  - For more information, see UPMC policy HS-MR1000, Release of Protected Health Information

Computers/Electronic Devices:

- Don’t share your password.
- Report viruses immediately.
- Use email for official UPMC business only.
- Secure laptops, PDAs, and other mobile devices; do not leave unattended.
- All UPMC PCs (including laptops) must be encrypted.
- Lock the computer when you are not at your workstation.
- Restrict the view of confidential information.
- If you must save confidential information electronically, you must save it to a supported storage solution

REPORTING A VIOLATION

Do I have to report a possible HIPAA violation?

- **Yes!** Regardless of the reporting method, any potential or possible violation of UPMC policy must be addressed.
- It is your responsibility to be alert to possible violations of law or policy, and communicate your concerns and observations in a manner consistent with the chain of command guidelines.
- If you need assistance, you should first contact your manager or supervisor.
  - Managers and Supervisors have a duty to thoroughly review privacy access alerts for their employees, and to report all appropriate matters to Human Resources, the UPMC Office of Patient and Consumer Privacy or entity Privacy Officer for ultimate disposition.
- If you are not comfortable with, or are unable to follow the chain of command, Human Resources, the UPMC Office of Patient and Consumer Privacy or entity Privacy Officer should be contacted.

REPORTING A VIOLATION

UPMC fosters a culture of compliance and ethics.

- UPMC employees have a responsibility to report, in good faith, instances of wrongdoing and, suspicious activity to the appropriate UPMC personnel or to a designated official or public body without fear of retaliation.

UPMC Prohibits Retaliation against:

- Anyone raising a concern or question in good faith about inappropriate or illegal behavior.
- Anyone participating in an investigation or providing information related to an alleged violation.

Whistleblower Protections

- Retaliation is not tolerated at UPMC! All suspected or alleged instances of retaliation shall result in a complete investigation of the circumstances.
- The Federal False Claims Act and the Pennsylvania Whistleblower Law address protections.
- For further information on these laws and UPMC policy, please read:
  - HS-EC1802, Reporting and Non-Retaliation
  - HS-EC1805, False Claims Act
  - HS-HR0705, Harassment-free Workplace

REPORTING OPTIONS

- Office of Patient and Consumer Privacy:
  - Phone: 412-647-6286 -OR- 412-647-5757 -OR- Email: privacyaskus@upmc.edu
  - List of entity specific Privacy Officer Contact Information
- UPMC Helpline: 1-877-98ETHIC (1-877-983-8442)
  - Calls are answered and routed by non-UPMC staff
  - Confidential - You may choose to remain anonymous
  - Available 24 hours a day, seven days a week
  - You can report any concerns or issues, whether they have occurred recently or in the past

Always remember that Life Solutions, UPMC employee assistance program, is always available to help you address personal or job-related concerns in a private and confidential environment. For more information, go to LifeSolutions.

POLICY AWARENESS REMINDER…

- It is your responsibility to comply with all UPMC policies.
- All UPMC policies can be found on Infonet.
- Check with your supervisor and/or department manager to determine if there are additional Compliance/Privacy policies and/or procedures (not discussed in this training) that relate specifically to your job responsibilities. Some examples:
  - Use of PHI for marketing and/or fundraising
  - Use and/or disclosure of PHI for research purposes
  - Patient access to PHI
  - Patient amendments to PHI
  - Release and minimum necessary standards for disclosure of PHI
  - Notice of privacy practices
  - Accounting of disclosures
  - Guidelines for Purchasing

RESOURCES AVAILABLE TO YOU

- Should you have privacy and security questions, contact the Office of Patient and Consumer Privacy.
- The OPCP and ISG groups have Infonet webpages available at:
  - http://infonet2.upmc.com/OurOrganization/Enterprise/Privacy/Pages/default.aspx
  - http://infonet2.upmc.com/OurOrganization/Enterprise/ISD/ISG/Pages/default.aspx