• This educational training session will provide you with an overview of some of the key UPMC Privacy and Security policies, PSD policies, guidance for dealing with situations that you encounter during both routine and non-routine situations, HIPAA do’s and don’ts, and information on when to notify the Privacy Officer.

• All UPMC employees are required to adhere to all approved policies and procedures and are responsible to know the specific policies and procedures that relate to their job responsibilities
  – Failure to adhere to corporate and PSD HIPAA policies and procedures could result in corrective action.
  – A PSD share point site has been created that contains all of the Privacy and Security policies and procedures which is available to all staff. The address is https://spis.upmc.com/psd/home/HIPAA/default.aspx
HIPAA and Patient Privacy

Directions for Ordering HIPAA Forms and Supplies
- HIPAA Forms and Supplies
- Privacy Screens
- Rifkin Security Bags

HIPAA Policy Manual
- Accounting of Disclosure
- ARRA Self-pay
- Authentication and Access (Role Based Access) Control
- Business Associates Agreement
- Complaint Management
- Confidential Information
- Confidentiality Agreements
- Contact Info
- Designated Record Set
- Email Policy
- Free Screen Consent Form
- HIPAA Audit
- Information Protection (Patient, Resident)
- Manager's Guide
- Minimum Necessary
- Notice of Privacy

Announcements
There are currently no active announcements. To add a new announcement, click “Add new announcement” below.

Links
- Corporate HIPAA Site
- Policy Manuals
- PSD SharePoint
- Add new link
HIPAA Key Concepts

In order to successfully complete this training, it is important to understand some of the basic concepts and acronyms common to HIPAA and this session:

- **Protected Health Information (PHI)** – individually identified data, in any medium (oral, written, computer systems, etc), collected and directly used in and/or documenting healthcare or health status
  
  **Examples**: patient name, date of birth, social security number, phone number, diagnosis, test results, even the fact that the person is a patient of your office or that they have an appointment with a particular doctor is confidential

- **TPO** – Treatment, Payment, Healthcare Operations

- **Covered Entity** - Provider of medical and/or health services and any other person or organization who performs services for the provider, bills, or is paid for health care in the normal course of business
  
  **Examples**: Medical record copy service, transcription companies, Record storage company

- **Business Associate** – any individual, business, or vendor that is not part of UPMC and has access to protected health information (PHI) to perform a service
  
  **Examples**: Answering service, computer companies (EPIC), consultants hired to assist with billing, shredding company, courier service, cleaning companies, etc.

- **“Need to know” principle** – access to private and confidential information should be granted only in order for the employee to perform their job responsibilities. Specifies that only the information necessary for completion of a job assigned task is to be accessed.

- **Minimum Necessary** – limits the PHI disclosed, also limits the PHI accessed, to the amount reasonably necessary for an employee to perform his or her job responsibilities.
Consequences for Violating Privacy and Security Policies

- Disciplinary action, up to and including termination.

- The federal government has prosecuted individuals who have violated the HIPAA regulation. Violators can face the following:
  - Individual fines up to $250,000
  - 10 years imprisonment
“Acceptable Use”

All files containing UPMC business and/or PHI are to be stored on a network drive (commonly referred to as an “M” drive), or a share drive.

PHI is NOT to be stored on the “C” or hard drive of any desktop or laptop computer, or external storage devices such as memory sticks or third party applications (such as “Drop Box”).

PLEASE NOTE: If you do not know how to do this, or are unsure if your documents are being stored–on your “C” drive–immediately notify your supervisor / manager / IT representative who can assist you.
“Acceptable Use”  

• Security controls have been established to prevent unauthorized access to electronically maintained information including:

  – Unique usernames and passwords – Do not share (or post) your usernames and password with anyone!
  – Monitors are to be placed so that it prohibits unauthorized viewing of the information on the screen. When this is not possible, a privacy screen should be placed on the monitor.
    • In offices with EpicCare, the computers in the treatment may be viewable to the patient. Care must be taken when initially accessing the daily schedule to ensure that the patient is not exposed to the schedule.
  – Always log off or lock applications/computers and handheld devices when you leave the computer unattended.
  – The computers are set to time out appropriately - Do not change or alter the timeout settings!

• “Information technology resources (computers, servers, internet, e-mail, etc) are made available solely for the purpose of supporting the business, clinical, research, and educational activities of the UPMC workforce members.”
When information is released to a third party (verbally or by providing copies of charts) without the patient’s authorization, for purposes other than for Treatment, Payment, Health Care Operations (TPO), we must track the details. The specifics of the disclosure is to be entered into the electronic “accounting of disclosures” database. Each PSD office has assigned individuals who are responsible for this task.

Examples of occurrences that must be entered into the database:
- PennDot – any time we notify PennDot of a reportable item (seizures, glaucoma, etc.)
- Department of Health (DOH), County Health Department, Center for Disease Control – reportable diseases, including: AIDS/HIV, influenza, cancer, hepatitis, TB, rabies, animal bites, food poisoning etc.
- Required Registries – Cancer/Tumor, Trauma
- Subpoenas or Court Orders
- Errors – when information is inappropriately released / accessed

"Accounting of Disclosures" Policy number HS-EC1600
“Auditing, Logging, and Monitoring”

Policy number HS-IS0218

• Employee access to PHI is monitored via audit trails for appropriateness. If access is not appropriate, disciplinary actions are taken.

“Authentication and Access Controls”

Policy number HS – ISO204

This policy sets the requirements for the authentication controls for computer user accounts.

– Each UPMC employee is assigned a unique username
– All users must protect the confidentiality of all of their passwords -- **Do not share your passwords with anyone!**
“Electronic Mail and Messaging”

- E-mail is in place in order to assist UPMC staff with conducting UPMC business.
- The following footer message is to be included in all email messages:
  - “This email 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).”
- **Each practice/department will determine if they would like to email with patients.** Please check with the operational manager if you are not certain of the decision made by your office. When communicating with patients, it is important to follow all steps in the policy. Additional footer language should be added when emailing with patients.
- When it is necessary to send email outside of the UPMC system (meaning, to an email address that is not “XXX@upmc.edu”) that contains any patient and/or UPMC business information – the email is to be sent secure. To do this – simply type the following into the subject line of the email: “secure:”.

Policy number HS-ISO147

Physician Services Division
• PSD staff should not work directly with outside vendors without including the Purchasing / Supply chain management staff. **This applies to all purchased good and purchased services arrangements – even when someone is offering us “free” services.**
“Use and Disclosure of Protected Health Information for RESEARCH Purposes Pursuant to the HIPAA Privacy Rules”

Policy number HS-EC1611

• In order to access PHI for research purposes, a “HIPAA research authorization” signed by the patient must be obtained prior to accessing the patients information. This authorization is in addition to the informed consent of patients/subjects using the IRB-approved document.

• The policy addresses specifics that any employee working with a research project is expected to be familiar with. This would include items such as: a patient’s right to access information; conditions on participation with regard to PHI; access to Patient information preparatory to research; de-identified information, etc. This policy also addresses when an Honest Broker System needs to be utilized to “de-identify” information.
“HONEST BROKER Certification Process Related to the De-identification of Health Information for Research and Other Duties/Requirements of an Honest Broker”

Policy number HS-EC1807

• An Honest Broker collects and provides health information to research investigators in a de-identified manner whereby it would not be reasonably possible to identify the patients-subjects directly or indirectly.

NOTE: Employees that are involved with and/or in research projects need to review the specific HIPAA research policies and be familiar with the requirements they establish.
“Minimum Necessary Standard for the Use and Disclosure of Protected Health Information”

Policy number HS-EC1602

• Access and use of PHI is only to occur in order to carryout or perform your job responsibilities

  – For example: a person whose sole job responsibility is to schedule appointments for patients would not be granted MARS access. This is because a person scheduling an appointment for a patient does NOT need to read the medical record in order to schedule the appointment.
“Notice of Privacy Practices for Protected Health Information (PHI) Pursuant to the HIPAA Privacy Rules”

Important things to know about the Privacy Notice

- The notice must be posted in a public area of each UPMC site
- Every patient is to be offered the Privacy Notice
- The notice advises the patient that they have the following rights:
  - **Right** to ask to see and copy their medical record
  - **Right** to ask that incorrect or incomplete information in their medical record be corrected
  - **Right** to ask for a list of non-UPMC parties with whom UPMC has shared your health information (Accounting of Disclosure)
  - **Right** to ask UPMC to limit how UPMC uses and shares their health information without their consent.
  - **Right** to ask for confidential communications
  - **Right** to ask for a paper copy of the Notice of Privacy Practices
“Patient Amendment to Protected Health Information”  

Policy number HS-EC1609

- A patient has a right to request an amendment to their PHI.

- Only the author of the documentation can make a change when requested.

- HIPAA regulations require that the patient receives our response within sixty (60) days after we receive their written request. For that reason, it is important to immediately give all amendment requests to the person in the office responsible for processing them.

- Employees charged with processing these requests, need to be intimately familiar with the procedures associated with this type of patient request.
“Physical Access”

Identifies guidelines in order to make sure that access to UPMC physical locations and confidential information is locked and secured.

- There are many areas of a physician office that require restricted access (i.e. medical records, business office, sample medication areas, supply areas, etc.). Non UPMC employees are NOT to be in these areas.

- All UPMC employees are to wear UPMC Identification badges at all times when on duty.

- When employees are terminated:
  - Supervisors must immediately notify ISD and have the employees electronic access rights revoked. It is important to also remember to notify outside vendors (or the appropriate contacts) if the employee has access to other systems such as the Spheris Transcription system.
  - If the employee has access to a share drive, supervisors should be sure to remove access to those drives as well.
  - Supervisors should also collect keys (to desks, the office, etc) and change access codes to the office after employment ends.
“Release of Information”

- State and Federal law govern the release of PHI. Care must be taken to ensure that information is not released inappropriately.
- This policy provides guidelines regarding how and under what circumstances PHI can be released and includes specifics for a variety of requestor types (employer, insurance co., law enforcement, attorneys, coroner, etc.).
- Avoid unintentional disclosures:
  - PHI should not be discussed in public areas such as elevators, hallways, waiting rooms, etc.
  - When discussing patient information be aware of the loudness of your voice and who may overhear the information.
  - PHI should not be used in presentations or web sites (unless patient authorization has been obtained giving permission).

NOTE: State and Federal law specify the components of a valid authorization – see policy for details.
“Release of Information”

• When releasing PHI additional care must be exercised when releasing information classified as “sensitive” which includes:
  – Drug and Alcohol Information
  – Mental Health Information
  – HIV/AIDS Information
  – Adoption Information
  – Child or older adult abuse information
  – Abortion information
• See policy for specifics
“Release of Information”

Requesting access to the medical record:

• The patient has the right to request to review their medical record as well as their billing information.

• In order to request access to the original medical record, the patient must complete an “Authorization for the Release of Protected Health Information” form. The physician of record must review the patients request and chart and will determine whether the request should be approved or denied.
  - Under certain circumstances, the physician can deny the requests. Please see policy for greater details.

• NOTE: in order to protect the integrity of the medical record, the patient is not to be left alone with the record.
UPMC Employee Access to their PHI:

– Does NOT include access to:

• Behavioral Health
• Drug/Alcohol treatment
• HIV
• Registration Systems/Information
• Billing Systems/Information (including but not limited to Medipac and Epic Registration and Scheduling systems)

• Access is granted only for yourself, no one else.
• Staff are not permitted to access the records of persons for whom they have been named as a personal representative. (There is an exception to this rule for physicians)
Internal Release of Information

- Requesting records from UPMC offices and/or facilities:
  - Use the Internal release of PHI form
    - Does not require the signature of the patient when requesting records for treatment, payment, or operational purposes.
    - Can be used for all requests to UPMC offices for general medical information (it is not valid for mental health or Drug/Alcohol treatment.)
Procedure for FAXING Protected Health Information

• Unless the information is needed immediately, send the documents by US Mail.

• Use the approved PSD cover sheet and clearly specify the intended recipient of the fax.

• Preset or program commonly used fax numbers whenever possible and check the numbers regularly to validate their accuracy.

• When sending a fax to a non-routine recipient, notify the recipient in advance and verify the fax number is correct prior to sending.

• When possible, ask the patient to provide the fax number as part of his/her authorization.

• After the fax has gone through, verify with the recipient that the fax has been received.

• If the fax was not received by the intended recipient, notify your supervisor and the Privacy Officer.
Telephone Guidelines

• Principles for phone messages:
  – Limit information to that needed for confirming an appointment (e.g. date, time, general location)
  – Put yourself in the position of the patient (e.g. what would I object to others overhearing on a phone message)
  – Treat the information that you would leave on a telephone message the same as you would treat any release of clinical information
  – Be aware that the name of some services, by their inherent nature, are of a sensitive nature. Some examples may include: OB/GYN; pediatrics; plastics; surgery; transplants; cancer
  – “This is (insert name) from UPMC/Practice/Doctor name calling for (insert patient name). Please have him/her return my call at 412-xxx-xxxx.”
Retention and Destruction of Health Care Documentation Containing Protected Health Information

- Paper that contains PHI should never be placed in the normal trash container. The information must be shredded.

- If your office has a shredder on site – you should shred it in accordance with your office policy.

- If your office uses a “bin” that is picked up by an outside company - all information is to be placed in the bin on a routine basis, but at least daily. The bin is to be locked at all times.

Disposition of Electronic Media

- All electronic media must be disposed of in a manner that assures the information is rendered unreadable. If you have electronic media (i.e. CD’s, floppy discs, external drives, etc), that you need to dispose of contact the Privacy Officer or your IT representative for proper instructions.
Theft and/or Breach of Personal Information that is maintained by UPMC

- Breach = Unauthorized acquisition, access, use, or disclosure of protected health information.
- A breach MUST be reported immediately to the practice manager and/or administrator AND the Privacy Officer.
- There is limited time to conduct the investigation and notify the patient of the breach, **so report suspected cases immediately.**
If you suspect a Breach:

- If your password is stolen, or you suspect a breach of confidentiality or security - report it immediately to:
  - The ISD Help Desk – 412-647-HELP
  - The Privacy Officer, AnnE Rice – 412-647-8507
  - Your manager

- If you have knowledge of an actual or potential theft, loss of information or identity, report it immediately to:
  - Your direct manager
  - PSD Privacy Officer, AnnE Rice – 412-647-8507
Filing a complaint

- Anyone who suspects that the privacy and security of their information has been compromised, or their rights have been violated may file a complaint.
  - Complaints can be filed with any UPMC employee – who must report the complaint to their supervisor, who will report it to the Privacy officer.
  - Complaints can be made directly to the Privacy Officer
  - Complaints can be phoned into the corporate HIPAA helpline at 412-647-5757.
  - Complaints can be phoned in to the compliance hotline at 1-877-983-8442. Callers can remain anonymous if they choose.
  - Complaints can be made in writing to the Secretary of the US Dept. of Health and Human Services
Transportation of PHI

• **Secured/Tamper-Evident Carrier**
  – The container MUST be tamper-evident.
  – Examples: locked suitcase, lockable box, “transit sac”

• **Transported PHI log sheet**
  – All items placed in the secure carrier must be logged on the log sheet or on a copy of the Epic schedule
  – Fax the log to the destination.

• **Upon arrival/ receiving the PHI:**
  – Inspect the container to ensure seal/lock was not tampered with.
    • If seal/lock is broken, OR there is any doubt to the integrity of the container, notify the Practice Manager and the Privacy Officer immediately.
  – Match contents to the log sheet – note any discrepancies. Notify manager and Privacy officer of all discrepancies!
ARRA Self-Pay Regulation

• Under this act (ARRA), a patient can self pay their bill (not submit it to their health insurance company) and exercise their right to request that UPMC not release or disclose their information to any third party payer for the purposes of payment or health care operations.

• Additional information and procedures can be found on the HIPAA Share Point site, and the Epic training site.
HIPAA in Practice

• When handing patients documentation in the office, please look at all pages of the documentation and call the patient by the name listed on the documentation PRIOR to handing it to them. That way if the document is not being given to the correct patient, it is discovered BEFORE a breach occurs. For example, when handing Mrs. Smith her AVS, say “Mrs. Smith, here is a copy of your after visit summary.”
HIPAA in Practice

• When your office is notified that information has incorrectly been received by someone – it is important to advise the person that we need to have the (incorrect) documentation returned to us. Please offer to send the person a SASE (self addressed stamped envelope) if they voice concerns about the expense of returning the documentation.
HIPAA in Practice

• You are learning to use a new computer program / system or are teaching one of your coworkers to use the system. While sitting in front of the computer, you would like to “practice” using the new system that you have learned. What name should you use to “practice” with or to show your coworker the functionality?

Response: Most systems have “test” patients for such purposes or training systems that should be used. In the Epic system, there are several patients with the last name of “Crayon” and a variety of colors (magenta, blue, etc) for a first name that should be used.
HIPAA in Practice

You and your coworkers are talking about the game last night and one of the players’ injuries. A close friend or family member idolizes that sports figure. You hear that he is being treated in the building you work in or one close by. You can imagine how your family/friends eyes will light up if you can get them an autograph when they are in the building. So you go into EPIC to look up where the injured player will be and when, so that you or someone else that you will tell can “run into them” and obtain their autograph. Is this ok?

Response: No, Never! UPMC employees are only to access the information that they need in order to complete a job assigned task.
HIPAA in Practice

- A coworker is off on an extended leave. You are thinking of them and want to send her a card, but you do not know her address. Is it ok to go into our electronic systems (such as EPIC, MARS, e-Record, etc.) or their medical record and look up his/her mailing address so that you can send them a card?

  
  Response: No, Never! UPMC employees are only to access the information that they need in order to complete a business related task.
-You stop by the supermarket on your way home. You see the daughter of one of your patients who phoned you today inquiring about getting an elective procedure scheduled. As soon as you see the daughter, you realize that you never called her mother to notify her of the final arrangements that you made. Is it acceptable to tell the daughter?

-Response: No! Information about a patient should not be released to anyone other than the patient without their written consent!
HIPAA in Practice

• You and your co-worker are discussing your child who has been ill and was seen by the pediatrician a few days ago. You are anxious to hear something about the test results and mention this to your co-worker. She suggests that you look in one of the electronic systems to obtain the results. You do not have access to anything, but she does. Is it acceptable for either of you to obtain the results?

  – Response: NO! It is never acceptable to access records without a UPMC business need to do so.
HIPAA in Practice

• You receive a phone call from a patient who advises you that they received an invoice for a visit with one of your physicians. The patient tells you that he has never been seen by your physician. What do you do?

Response: You should notify your supervisor immediately. The supervisor is to notify the CBO and the Privacy Officer of the issue. While each case is different, evaluations will be completed to determine if fraud may have occurred; current processes will be evaluated; adjustments may be made to the bill; and the information will be entered into the “Accounting of Disclosure” database.
HIPAA in Practice

• You receive a phone call from a patient who advises you that they received another patient's lab results mixed in with theirs. What do you do?

- Response: While on the phone with the caller, explain that we would like to have them return the documentation to your office. Offer to send the patient a stamped envelope for their convenience. You should notify your supervisor immediately. The supervisor will notify the Privacy Officer of the issue. While each case is different and will be handled appropriately for the case, often times an investigation will include completing an evaluation to determine if policies and procedures were followed; and to determine if process changes are necessary. Additionally the information will be entered in to the “Accounting of Disclosure” database.
Recent Headlines:

- UCLA Health System agreed to pay a $865,500 penalty and enter into a three year corrective action plan with the US government because employees who inappropriately accessed medical records were not properly sanctioned.
- Mass. General fined 1 million dollars because an employee who was transporting medical records failed to keep them secured when they excited public transportation without the records.
- Cignet Health of Maryland was fined $4.3 million dollars because they denied patients access to their medical records when requested.
- A former UPMC Shadyside employee plead guilty June 30, 2011 to violating federal law by knowingly disclosing patient health information.
Relationship between several policies

• It is important to remember many of the policies inter-relate, and come together to tell the whole picture of how we can utilize PHI.
  – An employee who is charged with preparing the medical records prior to a patient's visit, may be granted MARS access in order to obtain all of the key documents as appropriate, as well as to the e-record, EPIC, Stentor, etc. However; the employee is only permitted to access the electronic records of the patients whose charts are currently being prepared. If “George” is a patient of the office, the clerk should only be accessing George’s PHI when she has a specific job-assigned task. To do so at any other time – would be a violation of the following policies
    » Access
    » Minimum necessary
    » Release of information
    » Authentication and Access Controls
When to call the Privacy Officer

- When a patient or their family voices a complaint concerning the privacy and/or security of their protected health information (PHI)
- When you suspect that a privacy or security breach has occurred in the office
- When equipment containing PHI cannot be found, has been misplaced, lost, stolen, or has been accessed inappropriately (including but not limited to PDA’s, smart phones, computers, digital cameras, external storage devices, etc),
- When a patient wants to exercise one of their rights (access or amend their medical record, etc) and you are not sure what do to next
- If you have a question/concern about Patient privacy and/or the security of patient information
- If you want to report a HIPAA violation or suspected violation
If you have questions, please phone

- **AnnE Rice, MS, RHIA**
  Senior Director, Health Information Management and Privacy Officer
  Phone: 412-647-8507
  Fax: 412-647-8929
  E-mail: Riceae@upmc.edu or

- **Kimberly Peterson, MS, RHIA**
  Associate Director, Health Information Management
  Phone: 412-647-5630
  Fax: 412-647-8929
  Pager: 412-958-4827
  E-mail: Petersonk@upmc.edu or

- **HIPAA Program Office**
  Phone: 412-647-5757 or
  To report Anonymously: 877-983-8442
  E-mail: HIPAAaskus@upmc.edu
  http://HIPAA.infonet.upmc.com
Thank you for participating in the UPMC FY12 Physician Services Division Annual HIPAA Training Program. This fulfills your HIPAA training requirement.