Privacy and Confidentiality Handbook

A Handbook for All Staff

TABLE OF CONTENTS

AHS HIPAA HANDBOOK

HANDBOOK OBJECTIVES

This Handbook is a general introduction for all AHS faculty, staff, students, trainees, vendors, and volunteers to the privacy and security regulations dictated by the federal Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), other Federal and California privacy laws, and AHS Policies and Procedures. You are expected to follow the policies outlined in the Confidentiality Statement (Appendix 2). In addition, your department or organizational unit may have policies and procedures that supplement this document.

PRIVACY AND CONFIDENTIALITY OVERVIEW

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law which, in part, protects the privacy of individually identifiable patient information, provides for the electronic and physical security of health and patient medical information, and simplifies billing and other electronic transactions through the use of standard transactions and code sets (billing codes). HIPAA applies to all "covered entities" such as hospitals, physicians and other providers, health plans, their employees and other members of the covered entities' workforce. HIPAA privacy and security standards were updated in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Privacy and security are addressed separately in HIPAA under two distinct rules, the Privacy Rule and the Security Rule. The Privacy Rule sets the standards for how all protected health information should be controlled. Privacy standards define what information must be protected, who is authorized to access, use or disclose information, what processes must be in place to control the access, use, and disclosure of information, and patient rights. The Security Rule defines the standards that require covered entities to implement basic security safeguards to protect electronic protected health information (ePHI). Security is the ability to control access to electronic information, and to protect it from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. The standards include administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of ePHI.

Highlights of Privacy Rule
The Privacy Rule requires that access to protected health information (PHI), including electronic PHI (ePHI), by AHS faculty, staff, students, trainees, vendors, or volunteers is based on the general principles of "need to know" and "minimum necessary," wherein access is limited only to the patient information needed to perform a job function.

The HIPAA Privacy Rule also accords certain rights to patients, such as:

- Right to request access to their own health records
- Right to request an amendment of information in their records
- Right to receive an accounting of disclosure of their information
- Right to request copies of their health records in paper format, or in electronic format if available
- Right to request restrictions on how we will communicate with the patient or release their information. This includes the right to request a restriction of disclosure of health information to their health plan for the purpose of payment or healthcare operations, if the service or procedure has been paid for by the patient out of pocket and in full.

Potential Consequences of Breaking the Law
The Privacy Rule imposes penalties for non-compliance and for breaches of privacy which range from $100 to $1,500,000 per violation, in addition to costs and attorneys' fees, depending on the type of violation. Penalties include fines up to a maximum of $1,500,000 per event, and the potential for civil lawsuits, misdemeanor charges, the reporting of individual violators to licensing boards for violations, and imprisonment.

HIPAA and California Confidentiality of Medical Information Act (COMIA) also impose penalties and fines for non-compliance and for breaches of privacy. Breach of AHS policies can result in discipline up to and including termination of employment or professional relationship with AHS.

Specifically, SB 541 and AB211 are two California laws that were implemented on January 1, 2009. These laws provide stricter requirements and increased penalties for unlawful or unauthorized access to, and use or disclosure of, patients' medical information. SB 541 and AB211 make providers, health plans, health facilities, and individuals accountable for unauthorized access to, and use or disclosure of, patients' medical information. External investigations of violations can result in serious penalties such as:

1. SB 541 authorizes the California Department of Public Health (CDPH) to investigate health information privacy breaches in health facilities and assess fines of up to $25,000 per patient whose medical information was unlawfully or without authorization accessed, used or disclosed, and up to $17,500 per subsequent occurrence of breach (to a maximum of $250,000 per reportable event). Facilities must report every breach to both CDPH and the patient within 15 days of the detection or may be fined $100 per day for failure to report.
2. AB 211 establishes the Office of Health Information Integrity (OHII), and authorizes it to assess penalties against individuals who unlawfully view patient information. Current fines range from $2,500 for negligent unlawful disclosures up to $250,000 for unlawful disclosures for the purpose of financial gain. OHII may not assess penalties against health facilities that are governed by the provisions enacted in SB541.

Equally serious, a privacy violation will injure the reputation of AHS and could lead to costly lawsuits.

What do HIPAA's Administrative Simplification Rules Cover?
The HIPAA Administrative Simplification Rules include four main provisions:
1. **Transaction Code Sets** - Uniform Electronic Transaction Standards for health care data
2. **Privacy and confidentiality** provisions for individually-identifiable health care data
3. **Security procedures** to protect electronically maintained health information
4. **Unique health identifiers** for providers, employers, plans and individuals to be used in connection with the Uniform Electronic Transaction Standards

CONFIDENTIAL INFORMATION: DEFINITION AND RIGHTS TO ACCESS

What is considered confidential protected health information (PHI)?
Protected Health Information is the personal, individually-identifiable medical data that relates to a patient's health, the provision of health services, and the payment for health services. PHI includes a broad range of medical information relating to any individual. The information includes: patient name and address, birth date, age, medical record number, patient number, phone and fax numbers, e-mail addresses, medical records, diagnoses, x-rays, photos and images, prescriptions, lab work and test results, billing records, claim data, referral authorizations, and explanation of benefits. Research records of patient care must also be protected. If health related information is de-identified, it is not PHI and may be shared without restriction. De-identification means the removal of all personal identifiers. PHI can be transmitted or maintained electronically, written, or orally. The Notice of Privacy Practices explains how AHS may use PHI.

Who is authorized to see confidential PHI?
Doctors, nurses and other licensed providers in the health care team may access the entire medical record, based on their "need to know." All other members of the workforce have access only to the information needed to do their jobs. The AHS "Notice of Privacy Practices" describes the ways in which we may use PHI without obtaining the patient's specific authorization. Certain uses such as for **T**reatment, **P**ayment and Health Care **O**perations (TPO) are permitted:

1. **Treatment** of the patient, including appointment reminders
2. **Payment** of health care bills (claim submission, authorizations and payment posting)
3. Health Care **Operations** and business operations, including, teaching and medical staff quality activities, research (when approved by the IRB and with a patient's written permission); health care communications between a patient and their physician; hospital directory; and AHS fundraising, planning and development.

When can students and trainees access PHI?
Students and trainees in AHS may have access to PHI. Students and trainees are required to complete a privacy orientation or training and to sign a confidentiality agreement. Students and trainees are not permitted to remove any PHI from premises under any circumstances. Students and trainees may request copies of de-identified data for use in case presentations, however the request for use or disclosure must be coordinated with AHS' Health Information Management (HIM) Department where they are providing care.

Minimum Necessary Standard
The minimum necessary standard in the Privacy Rule requires that when a covered entity uses or discloses PHI or requests PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to that which is reasonably necessary to accomplish the intended purpose of the use, disclosure, or request. You are expected to apply the minimum necessary standard when you access PHI. For example, although physicians, nurses, and care providers may need to view the entire medical record, a billing clerk would likely only need to see a specific report to determine the billing codes. An admissions staff member may not need to see the medical record at all, only an order form with the admitting diagnosis and identification of the admitting physician. You are permitted to access and use only the minimum patient information necessary to do your own job.

Written Authorizations
To use or disclose PHI for almost any other reason, you will need to obtain a written authorization from the patient prior to access or disclosure. Refer to the "Notice of Privacy Practices" for a list of covered exceptions to the authorization requirement related to public policy, certain health disease reporting requirements and law enforcement activities. If you still have questions, please read the "Notice of Privacy Practices" and ask your supervisor or department chair.

Violations
A violation is an act that is contrary to the meaning of HIPAA and AHS guidelines to guarantee the confidentiality of protected health information. The unauthorized access, use or disclosure of PHI is a privacy violation. State and Federal laws impose civil and/or criminal liability, including fines, on the organization and the workforce member who inappropriately accesses PHI. In addition, the workforce member may be subject to disciplinary action, up to and including termination.

There are two levels of privacy violations. The following list provides an outline of some, but not all, types of violations under each level.
Level 1 –unintentional violations include, but are not limited to:

a. Misdirecting faxes or emails that contain PHI
b. Discussing PHI in public areas where the public could overhear conversation
c. Leaving computer and/or documents with PHI unattended or in a non-secure area
d. Accidentally accessing the wrong patient medical record
e. Accidentally providing a patient's PHI to another patient

Level 2 –intentional violations include, but are not limited to:

a. Committing multiple (2 or more using a one year look back) Level 1 violations
b. Obtaining PHI under false pretenses
c. Access, use or disclosure of PHI without a job-related reason
d. Discussing PHI with any unauthorized individual
e. Requesting or assisting an individual in gaining unauthorized access to PHI
f. Sharing computer information, such as passwords, that allows others to access PHI
g. Using PHI for commercial or personal purposes
h. Falsifying information or failing to cooperate during a privacy investigation

Sanctions
Failure to comply with AHS' policies and procedures will result in disciplinary action. A Level 1 violation will result in a Final Reminder and a Level 2 violation will result in **immediate** termination. Compliance Department will collaborate with the Human Resources Department regarding appropriate disciplinary action. Results of the investigation and decision will be documented in writing and records will be retained in the employee's HR file.

Contractors/Vendors:
Failure of a contractor/vendor to follow any provisions of this policy or mitigate any unauthorized access, use or disclosure of PHI upon mutually agreeable terms may result in termination of the contract and/or vendor agreement.

Reporting Violations
All staff are responsible for reporting suspected violations of privacy laws or privacy policies. Report concerns to your supervisor or the AHS Confidential Compliance Hotline (1-844-310-0005). All reports will be handled confidentially. Upon receiving a report, the Privacy Officer will immediately conduct a thorough investigation and coordinate corrective measures, as necessary. There will be no retribution or retaliation against anyone reporting a violation in good faith. Failure to report privacy violations will result in disciplinary action.

MEDICAL RECORD ACCESS AND CONTROL

Medical records are maintained for the benefit of the patient, medical staff, and the hospital and shall be available upon request of:

- Treating Physicians;
- Non-physicians involved with the patient's direct care (i.e. Nursing, Pharmacy);
- Any authorized officer, agent or employee of the Medical Center or its Medical Staff (i.e. Risk Management, Patient Relations, Privacy Officer);
- AHS researchers as part of an approved Institutional Review Board (IRB) Committee protocol that involves medical record review;
- Any other person authorized by law to make such a request (i.e. medical examiners, law enforcement, regulatory agencies); or
- Patient and/or patient's authorized representative.

AHS will maintain ownership of the Medical Record and it may be removed from the Medical Center jurisdiction only by:

- Subpoena,
- Court order, or
- Statute

Medical records are not to be removed from patient care areas except by authorized HIM staff.

HIM is responsible for maintaining control of access to medical records. Please go to the Medical Records Department to obtain an authorization form to obtain access to medical records.

PATIENTS' RIGHTS

Patients' rights under HIPAA are described in the "Notice of Privacy Practices." The Notice will be made available to patients in many settings. These rights include:

1**. Right to receive the "Notice of Privacy Practices,"** which informs patients of their rights and how to exercise them. AHS is required to make this notice available to patients. We are required to make a good faith effort to obtain the patient's acknowledgement of receipt.

2. **Right of Access**. Patients may request to inspect their medical record and may request copies. There is a fee to produce the copies. The process on how to request copies is explained in the "Notice of Privacy Practices."

3. **Right to Request an Amendment or Addendum**. The Notice describes how to file a request for an amendment or addendum.

4. **Right to an Accounting of Disclosures**. We can be asked to account for all unauthorized disclosures of the patient's PHI. Patients have the right to receive an accounting of disclosures of their PHI. The Notice describes how to request an accounting.

5. **Right to Request Restrictions**. Patients have the right to request restrictions on how we will communicate with the patient or release information. Generally, we will make every effort to try to accommodate reasonable requests for restrictions, e.g., where release of information could be harmful to the patient.

6. **Right to Complain**. Patients have the right to complain if they think that privacy rights have been violated. The “Notice of Privacy Practices” describes where to file a complaint, either within or outside of AHS.

Exceptions to the Rules
Under HIPAA, there are certain exceptions to these general rules. These exceptions are described in the “Notice of Privacy Practices.” Disclosures can be made without patient authorization: subject to professional judgment, for public health and safety purposes, for government functions, law enforcement and based on a judicial request or subpoena.

Psychotherapy notes require special handling and authorizations. All requests for psychotherapy notes should be routed to HIM.

Information may be used for research, fundraising, public information or marketing, but special rules apply. For many of these purposes, patients have a right to ask that their information not be accessed.

If you are unsure whether a request for information is authorized, please check with your supervisor or HIM. Since these disclosures may be subject to a request for an accounting, the requests need to be coordinated, tracked and archived by HIM.

Facility Patient Directories (Admitted Patients)
AHS can use and disclose selected PHI, which includes name, location in the hospital, condition (e.g., good, fair, critical) and religious affiliation (for clergy) in order to create facility patient directories. Keep in mind that AHS can use and disclose a patient’s location in the facility (e.g., patient’s room number), but may not release information that indicates a patient is being treated in an area of the hospital that is limited to treatment of certain diseases or conditions, such as alcohol or drug rehabilitation, detoxification, psychiatric treatment, or communicable disease treatment.

These directories are for use by the clergy and for responding to those who ask for a patient by name. Patients may opt out of the facility patient directory, in which case AHS will not provide this information to requesting individuals.

Release of Information to Individuals Involved in Patient Care
AHS may tell a patient’s family about their general condition and that they are in the hospital unless the patient requests AHS not to provide this information. Upon the request of a family member and with the patient’s consent, AHS may give the family member notification of their diagnosis, prognosis, medications prescribed, and their side effects, and progress. If a request for information is made by the patient’s spouse, parent, child, or sibling and the patient is unable to authorize the release of such information, AHS is required to give notification of the patient’s presence in the hospital, except to the extent prohibited by federal law. Upon a patient’s admission, AHS is required to make reasonable attempts to notify the patient’s next of kin or any other person designated by the patient, of their admission, and, upon request of the family member only, of the patient’s release, transfer, serious illness, injury, or death, unless the patient requests that this information not be provided.

Authorizations
HIPAA specifies the content of an authorization to disclose PHI. Accordingly, the authorization process should be managed by HIM. A written authorization from the patient (or the patient’s personal representative) is required to disclose or access PHI for uses, other than for treatment, payment and/or healthcare operations. Authorization is required to access any psychotherapy

record. AHS researchers must also complete request forms to review medical records as part of an approved IRB protocol.

De-Identification of PHI

Individuals must make all reasonable efforts to limit the use or disclosure of PHI. PHI that has been de-identified may be used without restrictions and without an authorization.
The de-identification rule states that you can disclose health information after it is no longer PHI because the 19 identifying data elements listed in the regulations have been removed. (See Appendix 1 for a list of the 19 data elements).

Another class of information referred to as a "limited data set" is PHI that excludes 16 of the 19 identifiers. (See Appendix 1 for data elements allowed for use.) The limited data set can be used for research, public health or health care operations, as long as the recipient of the data signs a data use agreement with AHS.

BUSINESS ASSOCIATES (B.A.)

Under HIPAA, a vendor or third-party entity that handles AHS' PHI is its "business associate" and it is required to subject them to the federal HIPAA privacy and security requirements through contract language. Business associates are required to implement policies that establish administrative, physical, and technical safeguards. Business associates will additionally be subject to direct penalties for violations of the security provisions. This requirement applies to companies or persons who conduct, for example, the following activities or functions, such as:

1. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing; or

2. Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to, or for AHS, when provision of the service involves the disclosure of individually identifiable health information.

This is not an all-inclusive list. AHS will not disclose protected health information to a business associate or permit a business associate to create or receive protected health information on AHS' behalf unless the business associate has given AHS the requisite "satisfactory assurance" by written contract.

If AHS learns that a business associate has materially breached or violated the "satisfactory assurance" of its business associate contract with AHS, AHS must take prompt reasonable steps to see that the breach or violation is cured. If the business associate does not promptly and efficiently cure the breach or violation, AHS must terminate its contract with the business associate, or if contract termination is not feasible, report the business associate's breach or violation to HHS.

In these circumstances, refer the Contracts Department to implement a business associate agreement with the vendor or third-party entity. The agreement can be handled as an addendum for existing contracts.

CLINICAL RESEARCH AND OTHER RESEARCH INVOLVING HUMAN SUBJECTS (INCLUDING THE USE OF HUMAN SPECIMENS OR INFORMATION FROM MEDICAL RECORDS AND DATABASES)

At AHS, the Institutional Review Board (IRB) reviews all uses and disclosures of PHI for research purposes. The expanded protection of health information does, however, impose additional requirements to protect confidentiality of patient information, research studies whether they are routine clinical studies or tissue/data repositories. The area most strongly impacted by HIPAA is

the identification and recruitment of potential research subjects through medical record searches or searches of other databases containing PHI.

Other changes include HIPAA limitations on the sharing of PHI, electronic transmission and physical security of the PHI, and specific privacy issues that must be addressed in the research protocol and informed consent documents. With IRB approval, clinical databases, data repositories, tissue and specimen banks can continue to be developed for research purposes and be maintained in perpetuity as long as they are HIPAA compliant. However, if IRB approval is not already in place, then IRB approval will need to be obtained prior to formation of these repositories and databases. HIM controls the access to medical records for research protocols involving chart review or decedent research.

Any new subjects enrolled after April 14, 2003 in studies in which HIPAA regulations apply will have to sign either an authorization to use PHI or a modified informed consent document approved by the IRB.

SECURITY RULE

Purpose of Security Rule
The Security Rule encompasses computer systems and electronic transmissions of information, for the purposes of:

- Ensuring **confidentiality**, **integrity** and **availability** of all electronic protected health information (ePHI) that is created, received, maintained or transmitted by the covered entity.
- Protecting against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
- Protecting against any reasonably anticipated uses or disclosures of ePHI.
- Ensuring compliance by its workforce

Definition of Security
Security is generally defined as having controls, counter-measures, and procedures in place to ensure the appropriate protection of information assets, and to control access to valued resources. The purpose of security is to minimize the vulnerability of assets and resources.

Requirements for Security
Under HIPAA, AHS is required to secure all access to electronically stored and transmitted protected health information (ePHI).

- The Information Security department is responsible for establishing security policies, procedures and systems that protect the medical center's computers from threats or vulnerabilities.
- Workforce members are responsible for employing appropriate and applicable security controls to protect all AHS electronic information resources under their control, such as:
    - Safeguarding PHI from accidental or intentional disclosure to unauthorized persons
    - Safeguarding PHI from accidental or intentional alteration, destruction, or loss
    - Safeguarding computers from viruses and malware

- Taking precautions that will minimize the potential for theft, destruction, or any type of loss
- Protecting workstations from unauthorized access and theft (e.g., via password authenticated access and physical lockdown) to ensure that ePHI is accessed, used, and/or disclosed only by authorized persons
- Protecting other electronic assets and portable media (e.g., USB thumb drives, external hard drives, CD-ROM/DVD disks, floppy disks, magnetic tapes, VHS tapes, SD memory cards, and all other forms of removable media or electronic storage devices) from unauthorized access and theft, to ensure that ePHI contained within is accessed, used, and/or disclosed only by authorized persons

Basic Privacy and Security Practices

Many of the privacy and security practices used to protect patients' health information are things we do as professional and as common sense business practices. Examples of what can be done to protect PHI and ePHI:

Privacy

1. Don't discuss patients' health information in a public place (i.e. hallway or elevator) in such a way that someone overhearing you could identify the person.

2. Don't leave medical or research records—whether printed or on a computer screen—unattended.

3. Don't use speakerphones to listen to patient messages or to speak with colleagues about confidential information.

4. Never leave sensitive or confidential information in a trash bin. Destroy all papers that contain PHI. Always follow the proper paper disposal procedure (i.e. gray bins for shredding). Locked, shredder disposal bins are located throughout AHS.

Physical Security

1. Store PHI in locked areas, desks, and cabinets.

2. Control access to research areas.

3. Obtain lock-down mechanisms for devices and equipment in easily accessed areas.

4. Challenge persons without badges in restricted areas.

5. Verify requests of maintenance, IS, or delivery personnel.

6. Keep confidential or sensitive information locked away when not in use. File documents in locked cabinets or drawers when you are finished with them.

Internet, Email and Fax Use Security

1. Be careful what you send via email. Do not send confidential information unless absolutely necessary. De-identify the information if possible. Warn patients who communicate with you via email that their confidentiality cannot be ensured.

2. Use the same care in sending e-mails that you would with a letter. Do not write anything in an e-mail that you might regret later. Assume e-mails are never erased.

3. Do not send attachments containing ePHI without encryption.

4. Add a confidential message footer to your messages, such as:
   CONFIDENTIALITY NOTICE This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.

5. If ePHI must be transmitted via email outside AHS, then the transmission must be encrypted by using AHS' "Secure" email. To trigger email security, the subject line must begin with the word SECURE directly followed by a colon and space. Capitalization of the trigger word and the use of a space after the colon are required.

6. Do not store ePHI on any website.

7. Never fax information to an unsecured fax machine. Have a designated employee pick up the fax and distribute.

8. Always check the destination fax number before faxing.

9. Use cover sheets containing a confidentiality statement, such as:
   CONFIDENTIALITY NOTICE This communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.

10. Immediately alert the sender of any faxes you receive in error, do not use or disclose the information, and either return or destroy the fax.

11. If you are advised that you sent a fax of PHI to the wrong recipient, confirm that the recipient either destroyed all copies or returned them to you and did not use or disclose the information. Immediately contact the Privacy Office for next steps.

Desktop/Workstation Security

1. Arrange computer screen so that it is not visible by unauthorized persons.

2. Log off before leaving the workstation.

3. Configure the workstation to automatically log off and require user to login if no activity for more than 15 minutes.

4. Set a screensaver with password protection to engage after 5-10 minutes of inactivity.

5. Manage your patient and research data. Store documents and databases with ePHI securely on a network file server. Do not store ePHI on the workstation (C: drive).

6. Do not allow coworkers to use your computer without first logging off.

7. If you have permission to work from home or a remote location, contact your IS department to securely configure the workstation.

Account Management

1. Do not share your user account, password, or other system access. You are responsible for all actions associated with your user ID and password.

2. Use strong passwords that are at least 6 to 8 characters long. Include upper- and lowercase letters, numbers, and special characters (#, %, ?, $).

3. Do not use pet names, birthdates, or words found in the dictionary.

4. If you must write down your password, keep it locked up or in your wallet protected like a credit card.

5. Do not enable your browser to remember your password.

6. Only access PHI/ePHI for business-related purposes.

7. Do not use your system access to look up medical information on yourself, family, friends, or coworkers.

8. Notify IS support immediately if you believe your system access has been compromised.

Portable Device Security

1. Portable devices include hand-held, notebook, tablet, and laptop computers; PDAs; cell phones; and pocket or portable memory devices such as thumb and jump drives.

2. Do not use a portable device for storing ePHI.

3. Use encryption when transporting ePHI on any mobile computing device. Be sure to backup encryption keys.

4. Use password protection.

5. Delete ePHI when it is no longer needed.

6. Keep your application software up-to-date.

7. Back-up critical software and data on a secured network.

8. Follow all of the recommendations for workstation security.

9. Use only VPN for remote wired and wireless connectivity.

10. Check with IS representatives for other security safeguards.

11. Use caution when uploading or downloading files to or from mobile devices. Adhere to the “minimum necessary” standard and never transfer ePHI over a network without using encryption.

12. Off-site work requires greater vigilance to maintain the required level of privacy and security.

13. Be alert to recognize and report all privacy and security incidents to your department supervisor or manager, the Privacy Office, and to IS for security issues.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) FOR MARKETING, FUNDRAISING AND TO THE MEDIA

Marketing
AHS must obtain a patient's authorization before using or disclosing a patient's PHI for marketing purposes unless an exception exists. If the marketing involves direct or indirect remuneration to AHS from a third party, the authorization must state that such remuneration is involved.

In limited circumstances, AHS may use PHI for marketing purposes to describe health products or services of nominal value that promote health-related services and/or for health insurance products if certain conditions are met. Communications relating to treatment options and health plan coverage are permitted. Example: If a hospital offered classes for patients on various health topics, sending a calendar of upcoming classes is allowed.

Fundraising
Although HIPAA does not prohibit fundraising efforts that target patients, the regulations strictly limit both how and how much PHI can be used and disclosed for fundraising. Specifically, only a patient's demographic information and dates of health care services can be used for fundraising without prior written authorization. Otherwise, AHS may use or disclose PHI about a patient for fundraising purposes only if it has first obtained the patient's authorization.

Media
The AHS Public Relations Office is responsible for managing media relations, and internal and external communications for AHS. If any reporters, photographers or other media representatives call you with questions, please refer them to the Public Relations Office.

CASE SCENARIOS

Case 1: Breach of HIPAA Privacy
A nurse you are friendly with asks you what type of surgery is being performed on one of your patients. She is concerned about the patient because it is her neighbor and a co-worker. What is the correct response to this situation under the HIPAA privacy regulations?

Explanation: Since the nurse asked for the patient by name, you may refer the nurse to the hospital operator to obtain whatever facility directory information is available, e.g., name, status condition, etc. The operator will check first to determine whether the patient is a "no disclosure" status. If you reveal the patient's diagnosis to this nurse without the prior oral and/or written consent from your patient, it is a breach of privacy. You could lose your job and be assessed fines!

Ask yourself the following questions before giving out any patient information to friends, patient's family members, or co-workers – even if the patient is a fellow employee:

1. Is the patient listed in the facility's records?

2. Has the patient consented to the release of directory information?

3. Does the requestor have a “need to know”, e.g., treatment, payment, healthcare operations? If you are unsure, refer the requestor to the patient’s treating physician or to the nurse manager in charge.

4. Do you have permission to disclose information to this visitor? If not, have you checked with the patient before giving out any information?

5. What is the minimum information necessary that you may provide?

6. Have you verified the visitor's identity before sending that person to the patient's room or disclosing information?

Case 2: Breach of HIPAA Privacy
You run into a former patient at the supermarket. She tells you that she had some cash flow problems and her bill was sent to collections. She mentions that her neighbor recently asked her if she was fully recovered from her surgery. Your patient is upset because she never mentioned her surgery to anyone. It turns out her neighbor’s son works for AHS’ billing department.

Explanation: Report the incident to the AHS Privacy Office. The AHS employee has violated HIPAA and the matter must be investigated. Disciplinary action up to and including termination could result from this unlawful disclosure.

FREQUENTLY ASKED QUESTIONS (FAQS)

HIPAA Privacy

Other than the patient’s medical record, are there other types of PHI that we need to protect?

AHS is required to make reasonable efforts to limit the amount of PHI used or disclosed to the minimum necessary to accomplish the intended use or disclosure. Examples of common healthcare activities involving PHI that must be protected (in addition to the medical record) are:

- Filled out prescription forms
- Faxed results from a reference laboratory and medical progress reports
- Copies of a consultant’s report from another physician
- Face sheets with registration or other demographic information
- Medical billing records which identify the patient
- Explanation of medical benefit statements received from a payer
- Components of the medical chart, such as the initial intake form, progress notes, drug history or records kept in the outpatient/clinic chart
- Financial disclosures and waivers signed by the patient
- Eligibility lists received from an HMO
- A letter requesting progress notes from a Medical Director of a Health Plan
- Correspondence from a malpractice carrier regarding a patient
- Referral authorizations received from health plans
- Collection agency reports
- E-mailed files from the transcriptionist
- X-rays and images

Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the

appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

Does the HIPAA Privacy Rule permit doctors, nurses, and other health care providers to share patient health information for treatment purposes without the patient's authorization?

Yes. The Privacy Rule allows those doctors, nurses, hospitals, laboratory technicians, and other health care providers that are covered entities to use or disclose protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient's authorization. This includes sharing the information to consult with other providers, including providers who are not covered entities, to treat a different patient, or to refer the patient.

Who are business associates or B.A.s under HIPAA?

Examples of obvious business associates that will most likely need a business associate agreements implemented are: medical billing firms; healthcare consultants; healthcare lawyers; record storage and document destruction companies; medical malpractice carrier; external audit

firms; billing collection agencies; medical staffing and temporary agencies; durable medical equipment vendors and medical transcription vendors, etc.

Refer all purchase orders or agreements involving protected health information to the Contracts Department to review. AHS has specific language that must be used in these agreements. Do not agree to sign or authorize another vendor's business associate agreement without consulting with the Contracts Department.

Under HIPAA can a hospital release PHI without authorization to another hospital when the patient is being directly transferred?

Yes, assuming that the question is referring to the release of PHI without authorization.
Explanation: HIPAA defines treatment as the provision of health care by, or the coordination of health care among health care providers. Treatment includes the referral of a patient from one provider to another and the coordination of health care among providers. There is no problem under HIPAA with transferring a patient from one hospital to another for care, the PHI can be transferred with the patient or disclosed to the receiving hospital by the transferring hospital. Additionally, HIPAA contains a provision that compels health care entities, including hospitals, to comply with laws requiring the use or disclosure of PHI, provided the use or disclosure meets and is limited to the relevant requirements of these other laws. In many instances, state laws may require the disclosure of relevant PHI when a patient is transferred from one hospital to another. These laws would be an additional, but more limited, basis under HIPAA to support disclosure of PHI from a transferring hospital to a receiving hospital.

For white boards or marker boards, what information can be listed?

The use of last names and first initials on the board within the department is appropriate. Due to special considerations in the operating room, first and last names are used.
Explanation: The important considerations are: if the board is visible to passers-by, does it contain PHI? If yes, are there other ways that the protected data (including demographic data) could be "reasonably" limited to the minimum necessary to allow the unit to safely manage patient care?

A patient's relative sent our department an e-mail to request insurance authorization. The e-mail contains protected health information. Can we respond to the e-mail?

No. Explanation: This question raises several issues: personal representative; authorization to disclose health information; use of e-mail. First, we need the patient's or the patient's designated representative's written authorization to share/disclose protected health information with a third-party. We cannot transmit protected health information data over e-mail without the patient's written consent. The department should call the relative to explain that we are not permitted to discuss the information without a written authorization from the patient. Advise the individual that the patient (or authorized representative) may call for the authorization and provide them with the telephone number to do so.

The newspaper reported that a famous person has come to the hospital for treatment. You are curious if this is true. Should you ask around or look for records about this person?

No, you are not allowed to satisfy your curiosity.
Explanation: Breach of patient confidentiality can result in disciplinary action up to and including termination of employment or professional relationship with AHS. The entire workforce shares a responsibility in protecting confidential information. The workforce includes faculty, staff, students, trainees and volunteers, regardless of whether they are caring for patients. This rule applies to everyone!

HIPAA Security

Why do I need to be HIPAA Security compliant?
The HIPAA law requires all covered health care entities or organizations and business associates to safeguard the privacy of patient health information. HIPAA also requires that we implement required security measures to protect patient health information.

What is the difference between the HIPAA Privacy and the HIPAA Security Rules?
The Privacy Rule sets the standards for how protected patient health information should be controlled. The Security Rule defines the standards that require covered entities to implement basic safeguards to protect ePHI. Privacy depends upon security measures – without security there is no privacy.

How are HIPAA Privacy and Security rules linked?
The Security and Privacy Rules are distinct but inextricably linked. Privacy of information depends in large part upon the existence of security measures. The HIPAA Security Rule defines the standards, which require covered entities to implement basic safeguards to protect ePHI. The Privacy Rule sets the standards for how protected ePHI should be controlled.

What does HIPAA mean by electronic media?
Electronic storage media including memory in computer hard drives and any removable/transportable digital memory medium such as magnetic tapes or disk, optical disk, memory card, or transmission media used to exchange information (internet, leased lines, dial-up, intranets, private networks).

What does electronic protected health information (ePHI) mean?
If the patient health information is computer based, meaning it is stored or maintained or processed electronically, it is ePHI and protected individually identifiable health information. This includes enrollment, individual eligibility health information that is transmitted by electronic media or maintained in electronic media.

APPENDIX 1

PHI Data Elements

1. Names

2. Postal address information, other than town or city, State and zip code

3. Telephone numbers

4. Fax numbers

5. E-mail addresses

6. Social Security Numbers

7. Medical record numbers

8. Health plan beneficiary numbers

9. Account numbers

10. Certificate/license numbers

11. Vehicle identifiers and serial numbers, including license plate numbers

12. Device identifiers and serial numbers

13. Web Universal Resource Locators (URLs)

14. Internet Protocol (IP) addresses

15. Biometric identifiers including voice and fingerprints

16. Full-face photographs and comparable images

*17. All elements of dates (except year) for dates related to an individual

*18. All elements of dates (including year) indicative of age, except an aggregated single category of “90 or older” is permissible

- birth date, admission date, discharge date, date of death, all ages over 90

*19. Any other unique identifying number, characteristic or code

* Data elements that are allowed in a Limited Data Set.

APPENDIX 2

This Attestation between Alameda Health System, hereinafter termed AHS, and myself, in conjunction with the **EMPLOYEE CONFIDENTIALITY STATEMENT AND AGREEMENT** and the **COMPUTER USE POLICY**, which I have signed previously, is related to the issuance, proper use of, and disposition of the Secured User ID and Password.

As an employee of AHS, I recognize that AHS must protect information related to its patients and the public in general and agree to and understand that I hold myself responsible for the observance of all policies and procedures pertaining to the release of confidential information. I further understand and agree that the aforesaid information is vital to the success of Alameda Health System business, and that through my activities and the duties of my employment, I may become acquainted with information of a confidential nature.

In view of the above and in consideration of my employment, for such length of time as employment may continue, I agree as follows:

1. In order to perform my duties, I have been provided with a secured and unique User ID and Password to use in conjunctions with the patient information systems.

   A. I agree to and understand that I will access, use or disclose patient confidential information only in the performance of my AHS duties, when required or permitted by law, and to disclose information only to persons who have the right to receive that information.

   B. When accessing, using or disclosing confidential information, I will access, use or disclose only the minimum information necessary.

   C. I agree to and understand that I may not allow any other person(s) to use my User ID and Password to access the patient electronic information system, nor will I use someone else's ID.

   D. If I believe someone else has used my User ID and Password, I will immediately report the use to the IT Department and request a new password.

   E. My User ID constitutes my signature and I will be responsible for all entries made under my User ID. My User ID is equivalent to my legal signature for Clinical Documentation.

   F. I agree to log off the computer system upon completion of review and/or data entry.

2. I understand that my access to all AHS electronic information systems is subject to audit in accordance with AHS policy.

3. Upon termination of my employment, I will notify my Hiring Manager and IT Department and surrender my User ID and Password to all AHS systems.

4. By signing the Employee User and Confidentiality Access Attestation, I agree to comply with the attestation form and EHR policy. I further understand that I am responsible for any breach of confidentiality resulting from access made to AHS electronic information systems using my User ID and Password, and may result in disciplinary action up to and including termination, civil fines for which I may be personally responsible and criminal sanctions.

IN TESTIMONY WHEREOF, I affix my signature,

_____

USER SIGNATURE DATE

_____

PRINT NAME DEPARTMENT NAME/AUTHORIZING MANAGER