

Sharp HealthCare's 2014 Compliance Education

Privacy (Federal and State) Module 3

Learning Objectives

In this module you will learn the following:

- Understand updated privacy laws on state and federal levels.
- Recognize various risks in breaches of patient medical information.
- Identify Sharp HealthCare's expectations regarding ethical conduct relating to the access, use, and disclosure of Protected Health Information (PHI).
- Recognize when you may access PHI as well as circumstances when it is prohibited.
- Understand how to report allegations of inappropriate access, use and/or disclosure of PHI.

Origins

Privacy and confidentiality has always been fundamental in the health care industry, both ethically and morally.





Did you know...

With the growing rate of identity theft, laws continue to emerge and sanctions have increased in an effort to protect patient's health information.

Overview of State Privacy Laws



State Privacy Laws



- CDPH enforces California Privacy laws.
- Requires all health care providers and facilities to prevent unlawful or unauthorized access, use or disclosure of patient medical information.
- Requires health care facilities to establish safeguards to protect the privacy of patient's medical information.

Unauthorized Access



The term “Unauthorized” means:

The inappropriate access, review, or viewing of patient health information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by California’s Confidentiality of Medical Information Act (CMIA).

California Department of Public Health (CDPH) News in 2014

- Colusa Regional Medical Center, failed to prevent unauthorized access and use of three patient's medical information by one employee, when another employee forgot to logoff their computer.

California Department of Public Health (CDPH) News in 2014

- Redwood Memorial Hospital failed to ensure a patients' PHI was not accessed, when a clinic employee accessed a hospital patient's electronic medical record using the physicians office password.

California Department of Public Health (CDPH) News in 2014

- Sierra Nevada Memorial Hospital failed to ensure unauthorized access when three employees and one physician accessed a high profile patients medical record when they did not have a treatment relationship.

State Penalties



CDPH is authorized to investigate privacy breaches in health facilities and assess penalties of up to \$25,000 per patient whose medical information was breached (maximum of \$250,000 per event).

Furthermore, CDPH, may assess a penalty of \$100 per day that unauthorized use or disclosure is not reported.

Severe Penalties for Patient Breaches

As you can see, we could face severe penalties for patient breaches, including fines, criminal sentencing and disciplinary action including termination of employment in accordance with Sharp policy.



CaLOHII Enforcement



- The California Office of Health Information Integrity (CaLOHII), is authorized to investigate and assess penalties against individuals for “Unauthorized Access”.

Individual Penalties

Current individual fines for violations of the CMIA range from:

\$2,500 - \$25,000 for knowingly and willfully violating privacy of patient health information.

\$250,000 for violating privacy of patient health information for financial gain.

**Maximum Fine:
Willfully Knowing**

\$25,000

**PHI Fine:
Violation of Privacy**

\$250,000



We are all Vulnerable

CaLOHII may investigate individuals including:

- Physicians
- Nurses
- Physical Therapists
- Medical Record Clerks
- Technicians, etc.

.....upon receipt of a referral
from CDPH.



CaLOHII is a reality for Sharp HealthCare



- Imposed sanctions have been applied to Sharp employees who have accessed a patient's electronic medical record without a direct need for medical diagnosis, treatment or other lawful propose under state and federal law.

Federal Privacy Laws



Now that you have a broader understanding of state Privacy Laws, **lets review the federal Privacy Laws.**

Federal Privacy Laws



- The Office of Civil Rights (OCR) enforces the Federal (a.k.a., HIPAA and HITECH) Privacy Laws.
- The laws require all Covered Entities (CE) including their Business Associates (BA's) to protect the security and confidentiality of patient health information.
- The HITECH laws require CE and their BA's to report Privacy Breaches within 60 days of detection to the patient and OCR.

New Federal Laws effective September 23, 2013

New HIPAA Rules

- An impermissible acquisition, access, use or disclosures of PHI is presumed a breach UNLESS the entity demonstrates that there is a low probability that the PHI has been compromised.
- To demonstrate a low probability, a risk assessment must be completed on all privacy violations.

Sharp Initiatives

Risk Assessment of the following four factors will be completed on every reportable PHI breach:

- Nature and extent of PHI involved.
- The unauthorized person who used the PHI or to whom the disclosure was made.
- Whether the PHI actually was acquired or viewed.
- The action taken to mitigate risk.

New Federal Laws effective September 23, 2013

New HIPAA Rules

Increased Patient Rights:

- A patient may request their medical information in an electronic format.
- Covered entities must withhold information from a health plan IF the patient pays in full for the service.
- Genetic information is prohibited from use for underwriting purposes.
- Covered entities must provide an opt-out option for fundraising.
- Covered entities may not receive payment in exchange for PHI.

Sharp Initiatives

All rights have been included in related policies and procedures and Notice of Privacy Practices.

New Federal Laws effective September 23, 2013

Increased Enforcement:

- OCR will investigate all cases of possible willful neglect.
- OCR has expanded requirements to business associates that receive PHI.
- OCR has increased its penalties up to **\$1.5 million** for noncompliance based on level of negligence.

U.S Department of Health and Human Services (DHHS) News

- In May 14, 2014 a New York-Presbyterian Hospital and Columbia University Medical Center failed to secure 6,800 patients' electronic protected health information.
- Assessed Penalty by OCR : **\$4.8 million** and a three year corrective action plan which included: risk analysis and management plan, revising policies and procedures to ensure compliance with security rules. **The largest settlement to date.**

U.S Department of Health and Human Services (DHHS) News



- In June 2013, Shasta Medical Regional Center executives in Los Angeles disclosed identifiable PHI to multiple media outlets on at least three occasions.
- Assessed Penalty by OCR : **\$275,000** settlement and a corrective action plan to implement policies and procedures regarding PHI disclosures to Media.

Remember PHI is....

- Any information, in any form, that relates to the past, present, or future physical or mental health or condition of an individual;
- The provision of health care to an individual;
- The past, present, or future payment for the provision of health care to an individual;
- That can be used to identify an individual.

Federal Privacy Laws



Unlike state privacy laws, federal law does not use the term “Unauthorized” for privacy violations; instead it uses the term **“Breach”**.

Breach



The term “Breach” means:

The unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the protected health information.

Federal Penalties



- Individuals, not just entities, are subject to penalties.
- Criminal penalties apply to an individual who obtains or discloses individually identifiable health information without a business need to know.
- Penalties can be applied up to \$50,000 and/or imprisoned more than one year.
- If offense is committed to sell for financial gain, a minimum fine of \$250,000 and/or imprisonment not more than 10 years.

EXAMPLES OF BREACHES

Example of a Privacy Breach

An employee or medical staff member **peeking** at a patient's medical record merely to satisfy his or her own curiosity; even if the employee or medical staff member does not disclose any medical information about the patient to any other person.



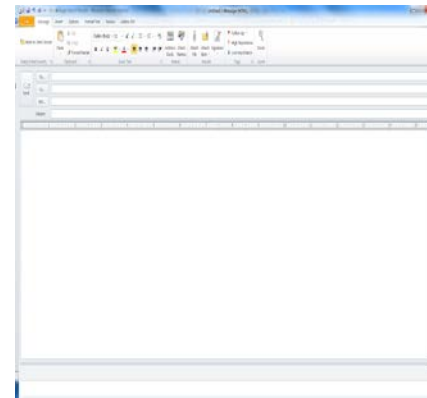
Examples of Paper Breaches

- Misdirected paper faxes with PHI outside of Sharp.
- Loss or theft of paper documents containing PHI.
- Mailing documents with PHI to the incorrect provider or patient.

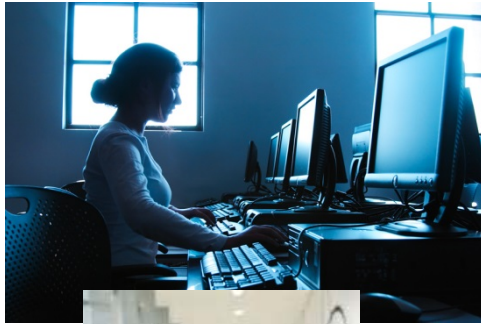


Examples of Electronic Breaches

- Misdirected emails with PHI sent to individuals outside of Sharp.
- Stolen unencrypted laptops, hard drives, or personal mobile devices containing PHI.
- Lost or stolen unencrypted thumb drives.



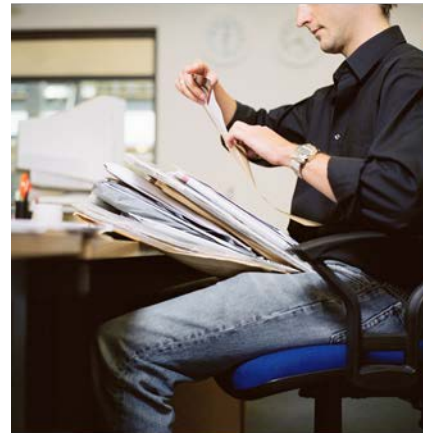
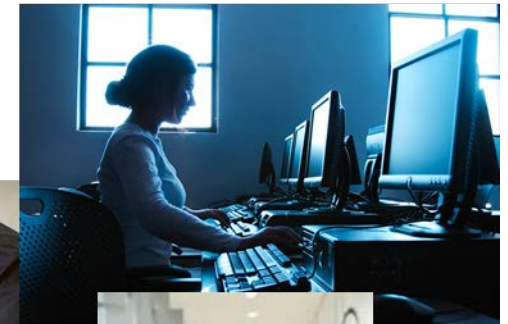
Where We Have Been Vulnerable



- Misdirected faxes containing PHI.
- Providing the wrong prescription to another patient.
- Providing patient with the wrong discharge paper work.
- Mailing patient information to the wrong patient.
- Employees accessing and/or viewing family, significant other, friends and/or co-workers information.

Consequently, Immediate Action is Required

These events must be reported to CDPH and/or the OCR and the affected patient.



How These Laws Affect Us

- Sharp HealthCare's privacy policies reflect these laws and emphasize that unauthorized access, use, disclosure or viewing of medical information is unlawful and subject to sanctions and disciplinary actions up to and including termination.
- In connection with our continued emphasis on privacy, Sharp has expanded existing initiatives to monitor access to and use of patient records. This monitoring activity occurs monthly in an effort to prevent unauthorized access.

SAFEGUARDS

Safeguards for Faxing



- ✓ Notify the recipient prior to sending a fax.
- ✓ Verify the fax number.
- ✓ Use a cover page with a confidentiality statement.
- ✓ Do not leave a fax containing PHI in the fax machine.

Safeguards for Printed PHI



- Be aware of documents that contain patient information.
- Print patient information (demographic, medical or billing) only if you need to.
- Printing PHI or proprietary information creates an additional responsibility for you to ensure it remains secure.
- Make sure documents under your control are always safeguarded from unintended disclosure.

Safeguards for Document Disposition

- Dispose of documents containing PHI daily in the large receptacles marked “Shredding”.



- Never discard PHI or proprietary information in regular trash containers or receptacles used for recycling.

Safeguards for Data

If your job requires the creation, sending or reporting of PHI make sure you:

Utilize non-sensitive data elements to identify the person (medical record number, account number) and,

Eliminate the use of social security numbers as an identifier in conjunction with other demographic or medical information (name, address, diagnosis, etc.)

It is Your Responsibility:



- To know when it's appropriate to use PHI identifiers.
- If there isn't a need for a PHI identifier, use a different identifier or a combination of less sensitive identifiers.

Safeguards for Data

- When in doubt, call the Technical Assistance Center to ask how you can safeguard information that needs to be sent securely via Sharp's electronic network.
 - **Technical Assistance Center**
Sharp TAC: (858) 627-5000
- Remember to ensure you are authorized to send the information prior to doing so, and that the recipient is authorized to receive it.



Safeguards for Verbal Communication

When talking about your work and/or about patients:


Use generalities when discussing patient's health status such as, "My patient had major surgery" or, "My patient was just told they have cancer."

Use generalities when discussing patient's reactions/feelings about their health or diagnosis such as, "My patient is really concerned about how his/her family will manage while he/she is in the hospital."

Notice of Privacy Practices (NPP)

Notice of Privacy Practices

Sharp must provide every patient with a copy of our Notice of Privacy Practices (similar to the notice you receive from your financial institutions.)

 <input type="checkbox"/> POLICY <input type="checkbox"/> PROCEDURE <input checked="" type="checkbox"/> POLICY & PROCEDURE <input type="checkbox"/> PLAN	PAGE 1 OF 4		REFERENCE			
	ORIGINAL ISSUE DATE 04/03	CURRENT EFFECT DATE 07/11	CATE/DIV D/S	SECT. # 01	SEC.CODE AO	POLICY/ PROCEDURE 01955.99
	TITLE: NOTICE OF PRIVACY PRACTICES					
	SUBJECT: Compliance					
KEYWORD(s): HIPAA, PRIVACY, CONFIDENTIALITY, COMPLIANCE, PHI, NOTICE						
<input checked="" type="checkbox"/> All Sharp HealthCare <input type="checkbox"/> System Services Surgery Centers: <input type="checkbox"/> SRS <input type="checkbox"/> CV-OPS <input type="checkbox"/> SCMG <input type="checkbox"/> GPSC <input type="checkbox"/> SHP <input type="checkbox"/> SMH-OPP		AFFECTED DEPARTMENTS: All Departments / Units		ACCREDITATION: The Joint Commission; Information Management		
Hospitals (check all that apply): <input type="checkbox"/> SCOR <input type="checkbox"/> SMH <input type="checkbox"/> SCVMC <input type="checkbox"/> SMBHWN <input type="checkbox"/> SGH <input type="checkbox"/> SMV <input type="checkbox"/> SMC		ORIGINATOR: Corporate Compliance		LEGAL REFERENCES: 45 CFR Parts 160 and 164		

I. **PURPOSE:**

To establish policy for the creation and distribution of a Notice of Privacy Practices document to individuals receiving services at Sharp. This document is available in both English and Spanish languages. The provision of the notice and the process of obtaining patient acknowledgement are intended to promote the individuals understanding of Sharp's privacy practices as well as provide the patient with an opportunity to request additional restrictions or confidential communications.

The Notice of Privacy Practices



- Serves as a communication tool from Sharp HealthCare to our patients.
- It educates our patients on:
 - Their rights
 - Our responsibilities
 - How we may use and disclose their PHI.
- It directs patients where to go with questions and concerns regarding their health information.

Remember What the Notice tells the Patient

The Notice describes the ways Sharp may use and disclose patients' protected health information.

For example, in certain circumstances:

- Sharp may disclose to a relative, a close personal friend of the patient, or any other person identified by the patient, the protected health information directly relevant to their involvement with the patient's care.
- Sharp may also disclose limited information to notify a requester of the patient's general location or condition if the requester asks for the patient by name.

Individuals Who Are Involved in the Patient's Care

- If the patient is **present and has the capacity** to make health care decisions, a verbal authorization is required in order to disclose their information. Sharp staff must document this information in the patients' medical record.
- If the patient is **not present or is incapacitated**, use your professional judgment to determine whether the disclosure is in the best interest of the individual. If so, disclose only the PHI directly relevant to that persons' involvement in the patient's care.
- It is acceptable, however, to use professional judgment and experience with common practice in allowing a person to pick up prescriptions, medical supplies, x-rays or other similar forms of PHI.

Patients Have a Right to...



Request restrictions on certain uses and disclosures

- Requests will be evaluated on a case by case basis.
- Refer requests to a supervisor.
- Granting requests will be based on our systems' capabilities to restrict health information.
- **Important!** If Sharp agrees to the restriction, we must establish a procedure to ensure that we continue to accommodate the request indefinitely.

Refer to Sharp's Health Information – Access, Use and Disclosure Policy #01951.99 for more information.

Patients Have a Right to...



- Inspect and request a copy of their Protected Health Information.
 - Health Information not only includes clinical information, it also includes billing information.

Patient Access to Their Health Information

- Requests for access to and copies of medical records will be handled by the Health Information/Medical Records Department. There are strict laws that must be followed when releasing information, so make sure you refer the patients to the experts!

Requests for copies of a patient's medical record must be in writing and processed through the Health Information/ Medical Records Department and provided within 15 days of the request. The Patient Access policy identifies what information Sharp HealthCare needs to make available to the patient upon request.



Patient Request For Copy of Medical Record



- All requests for inspection and copying must be in writing and directed to the Health Information/Medical Records Department.
- Provide the patient with an “Authorization for Use and Disclosure of Health Information” form for completion.
- Forward the original form to the Health Information/ Medical Records Department, and provide a copy to the patient upon request.
- Inform the patient that there may be a charge for this service.

Patient Authorization

- **An Authorization For Use and Disclosure of Health Information form must be completed and must include:**
 - A description of information to be disclosed
 - The identity of the Sharp HealthCare entity authorized to disclose information
 - The identity of the person or entity allowed to receive the information
 - The signature of the patient or legal representative
 - The date the authorization was signed
 - The purpose for which the disclosure was authorized
 - A statement that the individual understands they can revoke an authorization except to the extent that action has been taken in reliance on the authorization
 - An expiration of the authorization, either a date or event (e.g., end of research study)

Patient Authorization

Important:

If any of the previous elements are not included in the authorization, the authorization is considered INVALID and we may not act on it!

If we do act on an invalid authorization, we are in violation of the HIPAA Privacy regulation.

Reminder:

Completion of this form does not permit you to access and/or view patient information.

Refer to Sharp's Notice of Privacy Practices policy #01955.99 for more information.

Patient Requests to View Their Medical Record

Open Medical Record Policy #12043.99

If a patient wishes to “review” their medical record:

- The Open Medical Record review process is coordinated by a licensed healthcare provider with discussion of information according to scope of practice.
- Patients may designate others to receive their open (inpatient) or closed (discharged) health information through signed authorization and request inspection per Sharp Policy and Procedure #01951.99 Health Information: Access, Use and Disclosure.

What about Requests from Physicians who may or may not work at my Entity?



You are permitted to disclose pertinent patient medical information to a physician (or their staff) once you have verified they are or have been involved in the patient's care.

We Are All Responsible for Privacy!



- Respect everyone's right to privacy.
- Access patient demographic or medical information only if your job duties require it.
- Treat everyone's information the way you would want yours to be treated.

What Should I Do if I See a Co-Worker Accessing PHI for Non-Business Related Reasons?

To report confirmed or suspected violations, you may do any of the following:

- Contact Paul Belton, Sharp HealthCare's Corporate Compliance Officer at (858) 499-3138 or paul.belton@sharp.com.
- Contact your entity Privacy Liaison.
- Contact your manager.
- Report the incident to the Sharp Confidential Hotline at (800) 350-5022.
- Complete a Compliance Report at <http://www.mycompliancereport.com>.
- Complete a Quality Variance Report (QVR).


Reporting Concerns/Complaint



Sharp's policy requires you to report all privacy complaints. HIPAA privacy laws require that Sharp document all privacy complaints and retain them for six years.

Sharp's Privacy Complaint Policy

Sharp's Privacy Complaint Policy outlines the process for capturing all complaints and concerns into one database.

PAGE 1 OF 6		REFERENCE			
ORIGINAL ISSUE DATE	CURRENT EFFECT DATE	CATE/DIV	SECT. #	SECT.CODE	POLICY /PROCEDURE/PLAN #
05/14	05/14	A/S	01	AO	01537.99
 <input type="checkbox"/> POLICY <input type="checkbox"/> PROCEDURE <input checked="" type="checkbox"/> POLICY & PROCEDURE <input type="checkbox"/> PLAN		TITLE: INVESTIGATING UNAUTHORIZED ACQUISITION, ACCESS, USE, OR DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI): FEDERAL LAW			
		SUBJECT: Compliance			
		KEYWORD(S): HIPAA, PHI, Compliance, Privacy; access, disclosure, fines, sanctions, penalties, investigation, breach, QVR, HIPAA Breach Notification and Reporting.			
<input checked="" type="checkbox"/> All Sharp HealthCare <input type="checkbox"/> System Services Surgery Centers: <input type="checkbox"/> SRS <input type="checkbox"/> CV-OPS <input type="checkbox"/> SCMG <input type="checkbox"/> GPSC <input type="checkbox"/> SHP <input type="checkbox"/> SMH-OPP		AFFECTED DEPARTMENTS: All Departments / Units		ACCREDITATION:	
Hospitals (check all that apply): <input type="checkbox"/> SCOR <input type="checkbox"/> SMH <input type="checkbox"/> SCVMC <input type="checkbox"/> SMBHWN <input type="checkbox"/> SGH <input type="checkbox"/> SMV <input type="checkbox"/> SMC		ORIGINATOR: Corporate Compliance		LEGAL REFERENCES: 45 CFR Section 164.404-410 42 U.S.C. 17932; HITECH Act Section §13402	

I. PURPOSE:

The purpose of this policy is to outline Sharp's process for reporting unsecured disclosures of Protected Health Information (PHI) as required under federal and California law.

Refer to Sharp Policy #01537.99, Investigating Unauthorized Acquisition, Access, use or Disclosure of Protected Health Information (PHI): Federal Law.

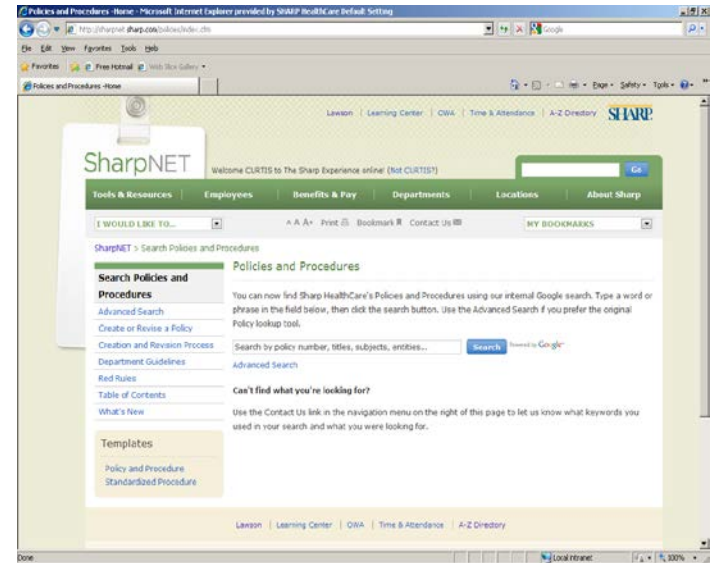
Where Do I Find Additional Resources?

The Sharp Intranet is the best place to access information regarding our privacy policies.

Go to SharpNET and look up “HIPAA” and select “HIPAA Privacy.”

or

Search Sharp HealthCare’s Policies and Procedures using the Keyword “Privacy.”



Final Reminder



Our patients have entrusted their care to us and need the assurance that all information, both personal and medical, will remain confidential and not used for personal curiosity or gain.

Exit Instructions

We hope this course has been informative and helpful.

**Please take the
Module 3 Quiz**