Sharp HealthCare's 2018 Compliance Education

Privacy
Module 3

SHARP

Learning Objectives

In this module you will learn and understand the following:

- The privacy requirements for California and federal laws.
- Sharp's policies and procedures relating to these laws
- Sharp's workforce responsibilities addressing Protected Health Information (PHI).
- How to safeguard PHI and prevent a privacy violation.
- How to report allegations of inappropriate/unauthorized access, use or disclosure of PHI.

State Privacy Laws

California Department of Public Health (CDPH) enforces California Privacy laws and requires licensed facilities, like Sharp hospitals to:

- Protect the privacy of patients' medical information.
- Prevent unlawful or unauthorized access, use or disclosure.
- Report unlawful or unauthorized access, use or disclosure of medical information within 15 business days after breach detection unless there is a delay by law enforcement.

Unauthorized Access of Medical Information

The term “**Unauthorized**” means:

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

State Privacy Law Basics:

According to State Privacy Laws:

- A patient's "medical information" is any individually identifiable information derived from a healthcare provider regarding a patient's medical history, mental or physical condition or treatment.

Examples of unlawful access, use or disclosure of medical information:

- **Accessing friends, co-workers, and all family members (including spouses, children and parents etc.) patient's medical information.**
- Faxing or providing medical information to the wrong patient, hospital or company.

State Penalties

CDPH assesses penalties of up to $25,000 per patient whose medical information was breached (maximum of $250,000 per event).

California Medical Information Act (CMIA)

- CMIA prohibits disclosure of medical information by a provider of health care, or health care service plan without written authorization.

CaLOHII Enforcement

- The California Office of Health Information Integrity (CalOHII) was created to enforce CMIA and to impose administrative penalties for unauthorized use of medical information.

CalOHII

The CalOHII, is authorized to investigate and assess penalties against individuals or providers for “Unauthorized Access”.

Current individual fines for violations of the CMIA range from:

- $2,500 - $25,000 for knowingly and willfully violating privacy of medical information.
- $250,000 for violating privacy of medical information for financial gain.

CaLOHII is a Reality for Sharp HealthCare

- Sanctions have been imposed on 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 law.

Federal Privacy Laws

Now that you have a broader understanding of state Privacy Laws, let's review the Federal Privacy Laws.

Federal Privacy Laws: What is HIPAA Privacy?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires all Sharp facilities to:

- Secure patients' PHI (physically and electronically).
- Adhere to the minimum necessary standard for use and disclosure of PHI.
- Specify patients' rights for access, use and disclosure of their PHI.

PHI

PHI is:

- Health information related to a patient's past, present or future physical and/or mental health or condition.
- Includes **at least one of the 18 personal identifiers** (Please refer to the next slide).
- Transmitted in any format: written, spoken, or electronic (including videos, photographs, and x - rays).

PHI Identifiers

- Name
- Postal address
- All elements of dates except year
- Telephone number
- Fax number
- Email address
- URL address
- IP address
- Social security number
- Account numbers
- Medical record number
- Health plan beneficiary number
- Device identifiers and their serial numbers
- Vehicle identifiers and serial number
- Biometric identifiers (finger prints)
- Full face photos and other comparable images
- Any other unique identifying number, code or characteristic
- License numbers

It is your responsibility to be aware of PHI Identifiers and safeguard them.

PHI Breach

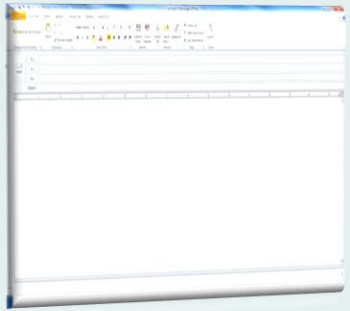
The term “**Breach**” means:

The unauthorized acquisition, access, use or disclosure that compromises the security or privacy of PHI.

Examples of Paper Breaches

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

Examples of Electronic Breaches



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

Where We Have Been Vulnerable

- Employees accessing and/or viewing family, significant other, friends and/or co-workers' PHI. Providing patient with the wrong discharge paper work.
- Misdirected faxes containing PHI.
- Not ensuring electronic devices are encrypted.

Federal Penalties

Penalties to HealthCare Providers:

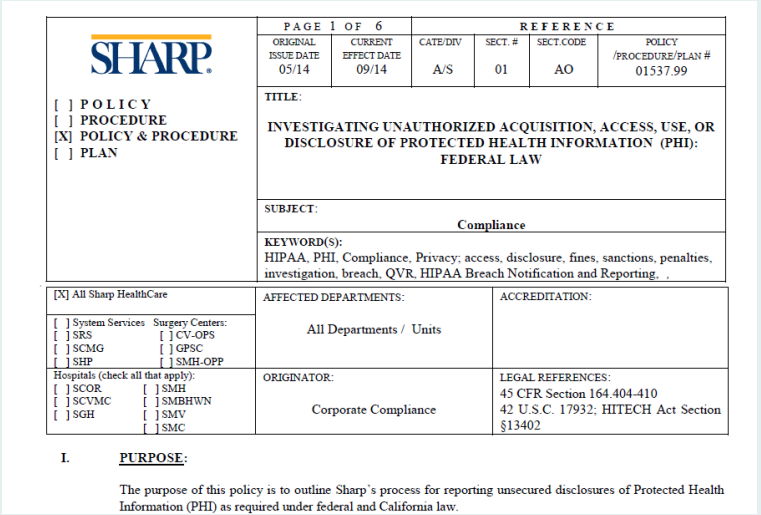
- The Office of Civil Rights increased its penalties up to $1.5 million for non-compliance based on negligence.

Penalties to Individuals:

- 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 the individual committed to sell PHI for financial gain, a minimum fine of $250,000 and/or imprisonment not more than 10 years.

Employee Penalties:

Workforce members who have violated Sharp policy #01537.99 for California and/or federal law will be subject to disciplinary action up to and including termination.



SHARP

[ ] POLICY
[ ] PROCEDURE
[X] POLICY & PROCEDURE
[ ] PLAN

PAGE 1 OF 6

REFERENCE					
ORIGINAL ISSUE DATE	CURRENT EFFECT DATE	CATE/DIV	SECT. #	SECT. CODE	POLICY /PROCEDURE/PLAN #
05/14	09/14	A/S	01	AO	01537.99

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, ,

[X] All Sharp HealthCare [ ] System Services [ ] Surgery Centers: [ ] SRS [ ] CV-OPS [ ] SCMG [ ] GPSC [ ] SHP [ ] SMH-OPP Hospitals (check all that apply): [ ] SCOR [ ] SMH [ ] SCVMC [ ] SMBHWN [ ] SGH [ ] SMV [ ] SMC	AFFECTED DEPARTMENTS: All Departments / Units ORIGINATOR: Corporate Compliance	ACCREDITATION: 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.

SHARP

Policies that support State and Federal Privacy Laws

Health Information:
Minimum Necessary Access, Use & Disclosure:
Policy and Procedure #01956

Health Information: Minimum Necessary Access, Use & Disclosure:

- When using, disclosing, or requesting PHI, members of the Sharp workforce shall take reasonable measures to limit the amount of PHI to the minimum necessary. In other words, the amount of information you "need to know" to perform a given function.

Minimum Necessary Activities:

- For patient payment, care and treatment, HIPAA does not impose restrictions on use and disclosure of PHI.
- **Exceptions for use:** psychotherapy information, HIV test results, and substance abuse information. (This PHI requires a patient /legal representative's written authorization for release of information.)

Notice of Privacy Practices (NPP) Sharp Policy and Procedure: #01955.99

In compliance with federal regulations, Sharp provides a NPP document for the purpose of adequately informing individuals, or their legal representative, of the following:

- The NPP describes how Sharp may use and disclose their PHI.
- Individuals rights regarding their health information.
- Sharp's legal responsibilities with respect to PHI.

The NPP Informs Patients of their Specific Rights:

- Right to access and receive a copy of one's own PHI (paper or electronic formats).
- Right to request amendments to information.
- Right to request restriction of PHI uses and disclosures.
- Right to restrict disclosure to health plans for services self - paid in full ("self - pay restriction").
- Right to request alternative forms of communications (mail to P.O. Box not street address; no message on answering machine, etc.)
- Right to an accounting of the disclosures of PHI.

Requests to View the Medical Record

If a patient wishes to "review" their medical record while in the hospital:

- The Open Medical Record Policy #12043.99 allows the patient to view their medical record with a licensed healthcare provider with discussion of information according to scope of practice.

If a patient wishes to "review" their medical record after they are discharged:

- A Medical Record request must be referred to the Health Information Management Department.
- Encourage the patient to utilize the Follow My Health Portal.

Health Information – Access, Use, and Disclosure Policy #01951.99

Workforce access to health information will be limited to:

1. Personnel providing care and treatment.
2. Individuals requiring information for payment/billing activities.
3. Individuals participating in functions or healthcare operations.
4. Sharp HealthCare workforce members' access to their own electronic health records.

How to Safeguard and Prevent a Privacy Violation

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.). For more information, please refer to Social Security policy number 01538.99.

Safeguards for Data

- When in doubt, call the **T**echnical **A**ssistance **C**enter (TAC) to ask how you can safeguard information that needs to be sent securely via Sharp's electronic network.

  - **T**echnical **A**ssistance **C**enter
    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 Printed PHI

- Be aware of documents that contain patient information.
- Print patient information (demographic, medical or billing) only if required.
- 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 Disposal

- Dispose of documents containing PHI <u>daily</u> in the large receptacles marked “Shredding”.
- Never discard PHI or proprietary information in regular trash containers or receptacles used for recycling.

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.

Reporting Concerns/Complaints

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.

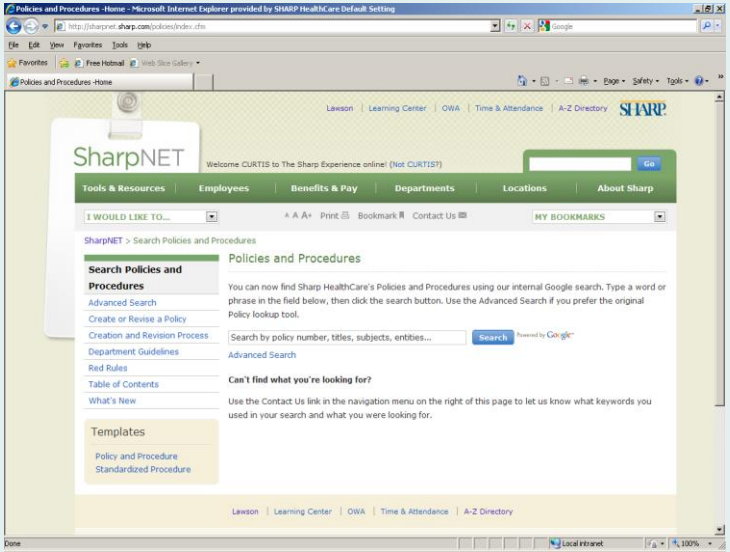
Refer to Sharp Policy #01533.99 for State reporting and #01537.99 for Federal reporting guidelines.

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

- Contact your entity Regulatory Department
- Contact your manager
- Contact Sharp HealthCare's Corporate Compliance/Privacy Office at (858) 499-3138
- To report anonymously, call the Sharp HealthCare Confidential Hotline at (800) 350-5022 or file a report online at www.mycompliancereport.com
- Complete a Quality Variance Report (RL Solutions)

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:

Next Steps:

We hope this course has been informative and helpful.

Click on the “X” (close button) in the upper right hand corner of the screen when you are ready to complete the requirements for this course.