

HIPAA Privacy, Security and (PHI) Compliance

Monday March 27th, 2018

Facilitator: Ellie Gillis, Director of Operational & Regulatory Compliance



What We Will Cover:

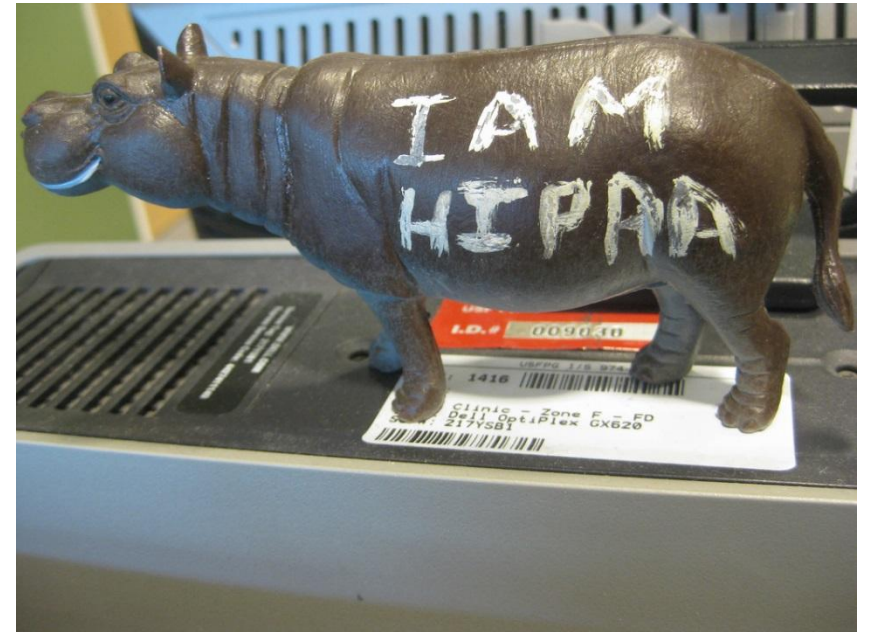
- Overview of the key components of the HIPAA privacy regulations
- How can a covered entity use and disclose PHI?
- What are the patient's rights?
- Overview of the key components of the security rule
- Minimum Necessary Rule
- HIPAA Policy & Procedures for FCL Dental
- HIPAA Civil Monetary Penalties
- Employee Responsibilities
- HIPAA Reporting
- Test your knowledge/ Questions



What is HIPAA ?

- H = Health
- I = Insurance
- P = Portability
- A = Accountability
- A = Act

**Patient
Privacy**



Key Components of HIPAA



The 3 Regulatory Key Components of HIPAA:

1. The Privacy Rule (April 14, 2003/42 CFR 164.500)
2. The Security Rule (April 20, 2005/ 42 CFR 164.300)
3. Electronic Transaction Standards (October 16, 2002/ 42 CFR 162)

Key Components of HIPAA



- The following benefits are NOT subject to the HIPAA Privacy and Security Rules:
- Accident only;
- Life insurance;
- Workers' compensation
- Disability income
- Liability insurance

Note: The benefits excluded under the HIPAA Privacy and Security Rules differ from those excluded under HIPAA's portability and nondiscrimination rules (for example, limited scope dental and vision plans ARE subject to the HIPAA Privacy and Security Rule).

HIPAA – General Rule (164.502)

A covered entity may not use or disclose Protected Health Information (PHI), except as *permitted or required* under HIPAA.

1. What are covered entities?
2. What is PHI?

**KNOW THE
RULES!**



Covered Entities – Types


- Health Plans: A plan that provides or pays the cost of medical care. Includes Medicaid, Medicare and self-funded plans.
- Providers: A provider of medical or health services such as a dental office, home health, hospital or PCP.
- Clearinghouses: Process health information for billing payment or claims payment.

Protected Health Information – PHI


PHI is health information collected from an individual, created or received by a covered entity. Some PHI identifiers are:

- individual names
- street address, city, zip code
- birth date
- telephone numbers
- fax numbers
- email addresses
- social security numbers
- medical record numbers
- health plan beneficiary numbers
- full face photographic images

Uses or Disclosures (160.103)

- Internal: 

Use means, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that has access to PHI.

- External: 

Disclosure means the release, transfer, provision of, access to, or divulging in any manner , of information outside the entity holding the PHI information.

Uses or Disclosures (160.103)- Continued

PHI can be used or disclosed for:

1. Payment, treatment and Healthcare Operation (164.502)
2. Required/ Mandatory by Law (164.502(a))
3. Uses and Disclosures with an authorization (164.508) – PHI Release Form
4. Uses and Disclosures with an opportunity to object (164.510) – Subpoena
5. Public Health Activities or to report abuse or neglect

Privacy Vs. Security



- ✓ It's possible to have security without privacy
- ✓ It's also possible to have privacy without security
- ✓ However with HIPAA, to keep information completely secure and confidential we need to have both
- ✓ The Privacy rule identifies what is to be protected and outlines the individual's rights to control access to their PHI
- ✓ The Security rule defines how to protect PHI in electronic form.

General Security Rule

The intent of the security role is to protect the confidentiality, integrity and availability (CIA) of PHI in electronic form:

- Confidentiality – ensuring that only those individuals who are supposed to access PHI do
- Integrity – ensuring that PHI input today is the PHI that is retrieved tomorrow, next week, next year, etc.
- Availability – ensuring that PHI is available to those who need it when they need it

Security Rule Compliance

FCL Dental supports the Security Rule (CIA) through administrative, technical and physical safeguards. To ensure compliance to the Security Rule the following safeguards are in place:

- ID badges
- System log-in and passwords
- Laptop and other mobile device security
- Email encryption and decryption
- Data back-up and storage

Minimum Necessary Rule

- Those of us who work with PHI are given access to it on a “need-to-know” basis. You are allowed to see PHI only as necessary to do your job.
- You should not attempt to view information that you have not been authorized to access.
- If you think you need information that you cannot access or if there is an emergency and you need more information quickly, ask your supervisor.

HIPAA Privacy/Security Quick Tips!

❖ Uses and Disclosure of PHI (Authorization)

- ✓ A signed authorization form must be received from all members before using or disclosing PHI
- ✓ An authorization is not required to carry out treatment, payment, health care operation or as required by law

❖ Faxing PHI

- ✓ Verify the identity and authority of the individual requesting the PHI
- ✓ Always use a fax cover sheet
- ✓ Verify the fax number
- ✓ Call to confirm the faxed was sent to the correct number

❖ Clean Desk Policy

- ✓ Do not leave PHI unattended at ANY time
- ✓ Always log-off and lock computer when away from work station
- ✓ Escort visitors in areas where PHI is contained
- ✓ Remove PHI from printer immediately when printing

HIPAA Privacy/Security Quick Tips! (Cont.)

❖ Confidential Information

- ✓ Confidential member information includes all PHI
- ✓ Employee information obtained during or through employment is also confidential information
- ✓ Health Care Provider information obtained by FCL Dental is also confidential information
- ✓ Proprietary Information related to FCL Dental business strategies and operation is also confidential information

❖ Uses and Disclosures of PHI – Minimum Necessary

- ✓ FCL Dental will limit the collection, use or disclosure to the minimum amount of PHI necessary to accomplish the intended purpose of the business or task at hand
- ✓ Access to PHI is based upon job duties and responsibilities
- ✓ Only the minimum necessary amount of PHI may be printed, downloaded, faxed or emailed when absolutely necessary for business purposes
- ✓ Minimum necessary PHI can be released to a covered entity if the request is a routine and reasonable request

HIPAA Privacy/Security Quick Tips! (Cont.)

- ❖ Use & Disclosures of PHI/Verification of Requestor of PHI
- ✓ Employees should verify a member, provider and the member's personal representative before releasing PHI
- ✓ Verify a member by:
 - Full name
 - Date of Birth
 - Member ID
 - SS#/ Phone or address
- ✓ Verify a provider by:
 - Tax ID number
 - A know place of business
 - Phone or fax number
- ✓ Personal representative:
 - Verify the Personal Representative in the memo section of QNXT
 - The personal representative can act on behalf of the member
 - A Durable Power of Attorney, Living Will or Proof of guardianship can be used to name a personal representative

HIPAA Privacy/Security Quick Tips! (Cont.)

- ❖ Use & Disclosures of PHI/Disclosure to Individuals involved in the member's care
 - ✓ Employees may disclose PHI directly relevant to the member's care to family members, or any person identified by the member.
 - ✓ FCL Dental employee must verify the identify of the person to whom they disclose the member's PHI.
 - ✓ If a member is present or otherwise available (phone) the member can orally authorize PHI disclosure
 - ✓ An oral authorization is ONLY valid for 14 days.
 - ✓ In specific circumstances, FCL Dental staff may reasonably exercise professional judgment to determine whether the disclosure is in the best interests of the member.
 - ✓ PHI disclosure made on the basis of professional judgment or for disaster relief purposes must be made on a case specific basis at the time of each encounter.
 - ✓ Knowledge of violation or potential violation of this policy must be reported directly to the Privacy Official or Compliance Officer.

HIPAA Civil Monetary Penalties (CMPs)

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did not Know	\$100 - \$50,000	\$1,500,000
Reasonable Cause	\$1,000 - \$50,000	\$1,500,000
Willful Neglect – corrected in 30 days	\$10,000 - \$50,000	\$1,500,000
Willful Neglect – Not Corrected	\$50,000	\$1,500,000

Do Your Part to Protect & Secure PHI

- **Never remove PHI** from the premises of FCL Dental without the proper authorization from your supervisor.
- **Never leave** documents with Protected Health Information (PHI) unattended. Lock your file cabinets and log off your computer when leaving to go to a meeting, lunch or home.
- **Never throw away** PHI in your waste basket. Destroy the document if it is no longer needed. Only secure shredding bins should be used for disposing of PHI. (Secure Recycle bin, i.e., one with a locked lid)
- **Always use** the Send Secure button when transmitting any PHI by e-mail outside FCL Dental's network. If you do not have a Send Secure button in your Outlook, you must call immediately the IT Department to resolve this issue as soon as possible.
- **Complete all** assigned HIPAA related trainings and classes in a timely manner.
- **If you are manually** mailing a document, make sure that no PHI information is visible in the envelope window or on the envelope labels.

Do Your Part to Protect & Secure PHI (Cont.)

- **If you are faxing** the document, always use a Fax Cover Sheet with an approved confidentiality statement and verify that the fax number of the intended recipient is correct .
- **Remember** the “Minimum Necessary Rule.” Only disclose PHI to individuals who have a legitimate business need to receive the information. ** Limit the PHI you share.
- **Limit** the amount of sensitive information that is discussed about a member in person or on the phone. Never leave sensitive messages on voice mail devices.
- **Report any/all** potential HIPAA violation immediately to your department manager/supervisor or to the Compliance department.

HIPAA Incident Reporting

FCL Dental Privacy & Compliance Department

Eleanor “Ellie” Gillis

101 Parklane Blvd., Suite 301

Sugarland, TX 77478

Direct Phone : 281-276-1033

Email: egillis@fcl dental.com

Test Your Knowledge

Match the risk areas with the correct safeguards

Risk Areas	Safeguards
Computer screens	Always lock and secure the keys
Emailing PHI	Use a secure shredder bin.
File cabinets/ drawers	Use a confidential coversheet
Disposing of documents	Lock or logoff when you leave you work area
Faxing PHI	Always use the “Send Secure” button

Test Your Knowledge

Match the risk areas with the correct safeguards

Verbal authorization are valid for 21 days.	True/ False
A member can be verified using the member telephone #.	True/ False
Professional judge can be used at all times when releasing PHI without the member's authorization.	True/ False
FCL Dental business strategies and operational plans are confidential information and should never be disclosed.	True/ False
Employees only have to report HIPAA incidents when they are 100% sure it happened.	True/ False

Questions??

