

HIPAA Privacy Rule and Breach Notification Rule Training

Greater Kansas City Dental Society

June 4, 2019

Presented by David Holtzman, JD, CIPP

Executive Advisor, CynergisTek

Today's Presenter

- Executive Advisor, CynergisTek, Inc.
- Subject matter expert in health information privacy policy and compliance issues involving data protection and breach notification standards
- Experienced in developing, implementing and evaluating health information privacy and security compliance programs
- Former senior advisor for health information technology and the HIPAA Security Rule, HHS Office for Civil Rights



David Holtzman
CynergisTek, Inc.



What is HIPAA?

- Health Insurance Portability & Accountability Act of 1996
- Framework for protection patient confidentiality, security standards for electronic systems, standards for electronic transmission of health information
- Notification to individuals, government and media if there is a breach of protected health information (added in 2009)

Who is Subject to HIPAA Standards?

- Covered Entities and Business Associates are required to comply with the Privacy, Security and Breach Notification Rules
- Covered Entities (CE) are defined as:
 - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
 - Health plans
 - Healthcare clearinghouses

Who Must Comply With HIPAA

- **Business Associates**
 - Contractors and Vendors to Covered Entities that have access to PHI while performing a service or function for the Covered Entity
 - Examples
 - Billing company or practice management service
 - IT service provider or cloud computing vendor
 - Shredding and document management services
 - Dental implant and denture fabricators
 - Not Business Associates: US Mail and package delivery services

Business Associates

- Agents, contractors, and others hired to do the work of, or to work for, the CE, and such work requires the use or disclosure of protected health information (PHI)
- BA's required to have Privacy Rule policies & procedures regarding uses & disclosures and minimum necessary
- Assess unauthorized uses & disclosures to determine if a breach has occurred and to notify the CE of any breach.
- The Privacy and Security Rules require CE's and BA's to receive "satisfactory assurance"
 - Assurance usually takes the form of a contract
 - BA only use or disclose PHI as permitted by agreement
 - Safeguard PHI from unauthorized disclosure

What is Covered?

- Protected Health Information (PHI)
- Simply put, PHI is any information about patients that relates to the past, present or future physical or mental condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual
- PHI can be in any form or format:
 - Spoken
 - Written
 - Electronic (ePHI)
- HIPAA provides a list of 18 identifiers

Identifiers That Make Up PHI


1. Names
2. Postal address information
3. All elements of dates
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical Record numbers
9. Health Plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers (license plates, etc.);
13. Device identifiers and serial numbers;
14. URLs;
15. IP addresses;
16. Biometric identifiers;
17. Full face photos; and
18. Any other unique identifying number, characteristic, or code

Designated Record Set (DRS)

- Designated Record Set is a group of records maintained by a Covered Entity that is:
 - The medical records and billing records about individuals maintained by or for a dental practice used whole or in part, by the dental practice to make decisions about individuals
 - Examples
 - Examination and treatment records
 - Billing and appointment records
 - Insurance claims records

The Bottom Line

- The Privacy Rule requires a dental practice to safeguard all PHI from unauthorized use or disclosure unless it is permitted or required by the Rule
- The patient or their personal representative has the right to access, amend, and receive a disclosure of accounting of PHI maintained in the designated record set



Uses and Disclosures of PHI

Definitions

- **Use** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information **within an entity** that maintains such information
- **Disclosure** means the release, transfer, provision of, access to, or divulging in any other manner of information **outside the entity** holding the information

Use, Disclosure and Access

- Generally, you may only access, use or disclose patient information if you have a **business need** to do so.
 - What's a business need?
 - Treatment
 - Payment
 - Health care operations
- You may only disclose PHI to **authorized persons**.
 - Who is authorized?
 - The patient
 - Employees involved in the patient's treatment, payment or health care operations
 - Individuals specifically authorized by the patient
- There are additional permissible disclosures for specific situations, covered further in this presentation

Minimum Necessary Standard

- All members of a dental practice should make reasonable efforts to use or release only the “minimum necessary” PHI to achieve the intended purpose
- For example, if a health insurer needs PHI from a treatment encounter for health care services in order to process a claim for payment, the health records from that episode of care treatment would satisfy the minimum necessary
- Minimum Necessary does not apply when disclosing PHI to another health care provider for treatment of that person

Minimum Necessary

- Limit amount of information to amount reasonably necessary to achieve purpose
- Policies and procedures required for routine and recurring uses and disclosures
- Must identify workforce members who need access to PHI
- Must identify categories of appropriate PHI for each workforce member

Personal Representatives

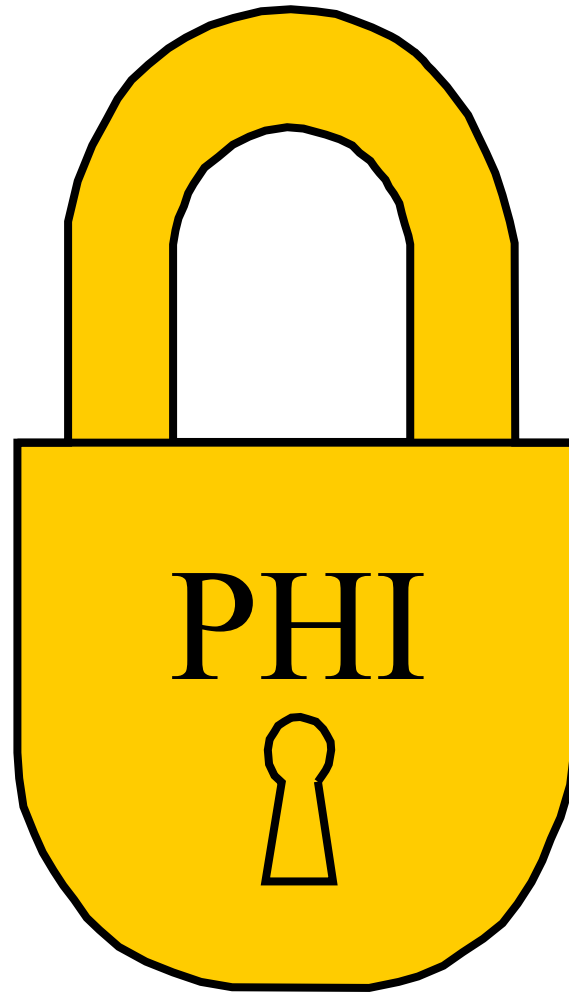
- Patients have the right to designate a personal representative to act on their behalf
 - In exercising their rights under the Privacy Rule to access and receive copies of PHI, request amendment of PHI, or accounting for disclosures
 - Make decisions on how PHI used or disclosed
- Adults and emancipated minors must designate the appointment of a personal representative in writing
 - The dental practice should require that the (adult) individual be required to make their appointment of a personal representative in writing
- The parents or court appointed guardians are the personal representative of children and unemancipated minors
- Executors and specified next of kin act as personal representative of deceased patients



Uses & Disclosures
for TPO



Uses & Disclosures in
the public interest



Uses & Disclosures
with an opportunity
to object



Authorization





Uses and Disclosures:
Uses and Disclosures that HIPAA
Permits or Requires Without
Authorization

Required Disclosures

- A dental practice is required to disclose PHI in two situations:
 - **To the individual:**
 - when requested as their right of access; and
 - through their request for an accounting of disclosures
 - **To the Secretary of the Department of Health and Human Services (HHS)** to investigate a Covered Entity's or Business Associate's compliance with the Privacy Rule

Uses and Disclosures Treatment, Payment, Operations (TPO)

- HIPAA allows use and disclosure PHI for treatment, payment or health care operations without an authorization from the patient
- Minimum Necessary applies when disclosing PHI except to another health care provider for treatment of that person
- All members of a dental practice should make reasonable efforts to use or release only the “minimum necessary” PHI to achieve the intended purpose

Uses and Disclosures Treatment, Payment, Operations (TPO)

- **Examples:**

- A dental hygienist discusses the patient's case with her colleagues or a supervising dentist to determine the best course of treatment
- A dental practice shares information with an insurer or health plan regarding payment for services
- An accountant or business office reviews medical and payment records for billing purposes or audits

Permitted Disclosures

- Public Health Activities
- Health Oversight Activities
- Law Enforcement
- Organ and Tissue Donation
- To Avert a Serious Threat
- Worker's Compensation
- To Report Abuse and Neglect
- Judicial and Administrative Proceedings
- Information about Decedents
- Research meeting specified provisions
- Specialized Government Functions

Permissible Disclosures Public Health Activities

- To prevent or control disease, injury or disability
- Vital statistics, birth & deaths
- Public health surveillance
- Public health investigations
- To an official of a foreign government agency acting in collaboration with with public health authority
- Report child abuse or neglect
- FDA reporting
- Alert individual of possible exposure to communicable disease
- Disclosures to schools
- Employers under limited circumstances
- People subject to the jurisdiction of the FDA

Permissive Disclosures: Health Oversight Activities

- Disclosures may be made to entities authorized by law to oversee
 - The health care system
 - Government benefit programs for which health information is relevant to beneficiary eligibility
 - Entities subject to government regulatory programs
 - Entities subject to civil rights laws
- **Exceptions:** This does not include investigations where the individual is the subject of the investigation if it is not directly related to:
 - The receipt of health care
 - A claim for public benefits related to health
 - Qualification or receipt of public benefit or service if health is integral to the claim

Judicial & Administrative Proceedings

- Health care providers may disclose PHI for:
 - Court orders
 - Limited to the PHI **expressly authorized**
 - Subpoenas, discovery requests or other lawful process if satisfactory assurances is received that either:
 - The subject of information has been notified & given a chance to object, or
 - A qualified protective order has been requested; or, alternatively:
 - Dental practice notifies the individual or seeks a protective order

Disclosures to Law Enforcement

- Dental practice may disclose PHI to law enforcement official for a law enforcement purpose if pursuant to process or otherwise required by law
- Identification and location
 - Limited to specific information
- Victims of a crime
 - If the victim agrees
- Decedents – if suspicion that death was result of criminal conduct
- Crime on the premises
 - Good faith belief that a crime has been committed on the premises of the dental practice
- Reporting crime in an emergency

Information about Decedents

- Coroners & Medical Examiners
 - Determine cause of death
 - Identification
 - Other duties authorized by law
- Funeral Directors
 - Information necessary to carry out their duties
 - If necessary for a funeral director to carry out their duties, dental practice may disclose PHI prior to, and in reasonable anticipation of, the individual's death
- Personal Representatives and Next of Kin
 - Executors and administrators of the individual's estate appointed by a court
 - Next of kin as specified under law
 - Information to family members or other person involved in the individual's care or payment for care, unless doing so is inconsistent with an expressed preference of the deceased individual

Organ and Tissue Donation

- The Privacy Rule permits a HIPAA Covered Entity to disclose an individual's PHI to a tissue bank or regional transplant organization to facilitate transplantation efforts.

Disclosures for Research

- Waiver approved by privacy board or Institutional Review Board (IRB)
- Reviews preparatory to research
- Research on decedents information
- De-identified data
- Limited data set used

De-identification of PHI: Two Accepted Methods

- De-identified PHI has been scrubbed of:
 - Individually identifiable health information from which are removed any identifiers of the **individual, relatives, employers, or household patients**
 - HIPAA protections extend to deceased individuals!
 - For 50 years from the date of death, that individual's PHI must be protected like any other patient
- If a **statistician** has determined that the PHI has a limited risk of re-identification, then the PHI may be freely disclosed

De- identification of PHI

- Two methods that PHI may be deidentified
- Data has been scrubbed of
 - Individually identifiable health information from which are removed any identifiers of the **individual, relatives, employers, or household patients**
 - HIPAA protections extend to deceased individuals!
 - For 50 years from the date of death, that individual's PHI must be protected like any other patient
- A **statistician** has determined that the PHI has a limited risk of re-identification, then the PHI may be freely disclosed
- Once deidentified, data not subject to HIPAA restriction on use or disclosure

Elements of Identifiable Health Information

1. Names, including initials
2. Street address, city, county, precinct, zip code, and equivalent geo-codes
3. All elements of dates (except year) for dates directly related to an individual and all ages over 89
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan ID numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers/serial numbers
14. Web addresses (URLs)
15. Internet IP addresses
16. Biometric identifiers, incl. finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

Data Use Agreement (DUA)

- Sets out the permitted uses and disclosures of the PHI in the limited data set (LDS)
- Identifies who is permitted to use or disclose the information
- Provides that the recipient will
 - Properly safeguard the data
 - Not use the information in a manner inconsistent with the DUA
 - Report any improper uses or disclosures to Salud
 - Not use the information to attempt to identify or contact individuals based on the information in the LDS
 - Require all agents and subcontractors to comply with the terms of the DUA

Disclosures to Avert a Serious Threat

- A dental practice may disclose PHI if the disclosure is made with a good faith belief that:
 - The disclosure is necessary to prevent or lessen a serious or imminent threat to a person or the public; **AND**
 - The disclosure is made to persons reasonably able to prevent the threat
- A dental practice **may not** disclose PHI if the information is learned by through:
 - The course of treatment to affect the likelihood to commit the conduct as a result of treatment, counseling or therapy; or
 - Through a request by the individual to initiate or be referred for treatment, counseling or therapy

Specialized Government Functions


- Military & veteran activities
- National security and intelligence activities
- Protection of the President & others
- Medical suitability determinations
- Correctional institutions
- Covered entities that are governmental entities providing public benefits
- National Instant Criminal Background Check System
- Workers' Compensation
 - May disclose to the extent necessary to comply with workers' compensation laws or other similar programs



Uses and Disclosures
Opportunity to Object
Required

Opportunity to Object

- Privacy Rule permits disclosure of limited PHI to “friends and family” when individual has not objected, or is incapacitated; AND,
- Covered entity believes disclosure in best interest of the patient
- Disclosures limited to the Minimum Necessary to achieve purpose to provide a caregiver or person responsible for payment of healthcare treatment needed information
- Example: Providing caregiver instructions on aftercare for a sedated patient



Uses and Disclosures Where an Authorization is Required

Uses & Disclosures Requiring Authorization

- All uses and disclosures of PHI that are not explicitly required or allowed by the Privacy Rule may only be done with a valid authorization.
 - Sale of PHI
 - Marketing
 - Dental Practice must obtain an authorization from the patient in order to use their PHI for marketing purposes
 - Activities That Are NOT Marketing
 - Sending of “patient newsletters” and information limited to services or treatments offered through the dental practice
 - Fundraising for an affiliated foundation
 - Must provide individuals opt-out from receiving future fundraising communications

Psychotherapy Notes

- Notes recorded by a mental health professional documenting or analyzing a conversation that occurs during a counseling session
- Does not include information about medication prescribing, results of clinical tests or a treatment plan
- Not made a part of a patient's medical record
- Psychotherapy notes receive special protection and authorization required for disclosures, even for TPO
- Dental practices generally do not create or maintain psychotherapy notes

A dark blue, irregularly shaped graphic with a splatter effect, containing white text. The graphic is centered on a white background and has a rough, ink-like border. The text is in a clean, sans-serif font.

What Is A Valid
Authorization?

Elements Required for a Valid Authorization

- A **description of the information** to be used or disclosed
- The **name of the person making the request**
- The **name or other specific identification of the person to which dental practice may send the PHI**
- A **description of each purpose of the requested use or disclosure**. The statement “at the request of the individual” is sufficient
- An **expiration date or an expiration event** that relates to the individual or the purpose of the use or disclosure
- **Signature of the individual and date**. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided

Required Elements for Authorization

- The authorization must also include the following statements:
 - The individual's right to revoke the authorization in writing, and either:
 - The exceptions to the right to revoke and a description of how the individual may revoke the authorization
 - The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating either:
 - Health care providers may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorization; or,
 - The consequences to the individual of a refusal to sign the authorization when dental practice can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization

Authorization Requirements

- Authorization must be written in plain language
- If a dental practice seeks an authorization from an individual for a use or disclosure of PHI, the practice **must** provide the individual with a copy of the signed authorization

Authorizations: Defective Authorizations

- An authorization is not valid if the document submitted to the health care provider has any of the following defects:
 - The expiration date has passed or the expiration event has occurred;
 - The authorization was not filled out completely;
 - The authorization has been revoked;
 - The authorization is not a permissible compound authorization or conditioned authorization; or
 - Any material information in the authorization is known by the dental practice to be false



Patient Rights

Dental practice must have policies to ensure that there is a record kept if a patient request to exercise any of these rights

Patient Rights Provided By HIPAA

- HIPAA provides the following rights to patients in regard to the use and disclosure of their PHI:
 - Right to Request Privacy Protection
 - Restrictions
 - Confidential Communications
 - Amendments to PHI
 - Access of Individuals to PHI
 - Accounting of Disclosures
 - Right to Receive a Notice of Privacy Practices

Patient Rights: Right to Request a Restriction on Disclosure to Health Plan

- A patient has right to restrict disclosure of PHI for purposes of TPO to their health plan or insurer when the treatment or service is paid for out of pocket.
 - If patient seeks restriction it is to be noted at time of payment for service
- In all other instances, a dental practice must allow and consider requests from patients for restrictions on use or disclosure of PHI for purposes of TPO.
 - The health care provider may choose to deny the request
 - If the request for restriction is granted, the dental practice must abide by the terms of the agreed upon restriction
 - **Example:** a patient requests that a particular dental practice employee be restricted from accessing their treatment records. The practice does not have to agree.

Patient Rights: Right to Request a Restriction on Use or Disclosure

- A health care provider may terminate an agreed upon restriction if:
 - The individual agrees to or requests the termination in writing;
 - The individual orally agrees to the termination and the oral agreement is documented; or
 - The dental practice informs the individual that it is unilaterally terminating its agreement to a restriction, except that such termination is:
 - Only effective with respect to PHI created or received after it has so informed the individual
- Example: a restriction was agreed to on 6/6/16 and the dental practice gave the patient notice it was ending the restriction on 1/1/17; all services rendered after 1/1/17 have no restriction but all restricted services rendered between 6/6/16 and 12/31/16 are still covered by the restriction.

Patient Rights: Confidential Communications

- A covered entity **must** permit individuals to request and **must** accommodate reasonable requests by individuals to receive communications of PHI from the dental practice by alternative means or at alternative locations, *if the individual clearly states that the disclosure of all or part of that information could endanger the individual*
- If the individual's request does not state that the disclosure will endanger the individual, then the dental practice may accept or deny the request
- Health care providers should develop a form titled "Confidential Communications Request" is available for patients/plan patients to fill out and return to the dental practice

Patient Rights: Access to PHI

- An individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set except for:
 - Psychotherapy notes; and
 - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- The Privacy Rule currently permits a covered entity to require the request for patient access be made in writing (electronic or paper)
- Dental practices should develop a standard “Request for Access to Personal Health Information” form is available for patients electronically to fill out complete and return

Patient Rights:

Access to PHI

- The Privacy Rule currently allows a covered entity up to 30 days to act on the patient's request for access to PHI (whether granting or denying)
 - If the request is granted, must inform the individual of the acceptance and provide the access
 - This can be a simple acknowledgement that accompanies the requested information
- If the dental practice is unable to take action within 30 days, they may exercise a one-time extension for another 30 days so long as notice of the extension is given to the requestor within the original 30 days along with an explanation for the delay

Denial of Access

- Grounds for denial
 - Certain limited circumstances dental practice may deny a patient's request for access to all or some of their PHI
 - In some of these circumstances, individual has the right to have the denial reviewed by a licensed health care professional who did not participate in the original decision to deny.
- Cannot require individual to provide reason for requesting access
- Cannot deny if PHI is maintained by a business associate
 - Dental practice must obtain records from contractor or direct them to send to patient

Grounds for Denial of Access

- Reviewable Grounds
 - Access reasonably likely endanger life or physical safety
 - Access requested reasonably likely to cause substantial harm to someone mentioned in the PHI
 - Access sought by personal representative reasonably likely to cause substantial harm to the individual
- Unreviewable Grounds
 - Request for access to psychotherapy notes or PHI compiled in anticipation of litigation
 - Requested PHI part of an ongoing research study
 - Requested PHI compiled obtained by someone other than treatment provider and under a promise of confidentiality

Patient Rights:

Access to PHI

- **Fees for copies of health records:**
- The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI. The fee may include only the cost of:
 - Labor for copying the PHI requested by the individual, whether in paper or electronic form
 - Supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media
 - Postage, when the individual requests that the copy, or the summary or explanation, be mailed
 - Preparation of an explanation or summary of the PHI, if agreed to by the individual.
 - The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed

Patient Rights: Access to PHI

- A dental practice may not withhold medical records because the patient has not paid for services
- The covered entity must make a reasonable effort to provide the requestor the information in the form and format requested
- A dental practice is not required to allow a patient to directly connect their electronic device to the practice's information network to access or inspect their PHI
- If patients inspect their own PHI, a health care provider may not charge them if they make their own notes, copies, or pictures using their own resources

Patient Rights:

Request an Amendment

- An individual has the right to have health care provider amend PHI or a record about the individual in the designated record set for as long as the PHI is maintained in the designated record set
- Dental practice must honor an individual's request for amendment unless it determines that the PHI or record that is the subject of the request:
 - Was not created by provider unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
 - Is not part of the designated record set;
 - Would not be available for inspection; or
 - Is accurate and complete
- **Health care provider must respond to request within 60 days**

Patient Rights:

Accounting of Disclosures

- An individual has a right to receive an accounting of disclosures of PHI made by dental practice in the six years prior to the date on which the accounting is requested, **except** for disclosures:
 - To carry out treatment, payment and health care operations
 - To individuals of PHI about them
 - Incident to a use or disclosure otherwise permitted or required
 - Pursuant to an authorization
 - For the facility's directory or to persons involved in the individual's care or other notification purposes
 - For national security or intelligence purposes
 - To correctional institutions or law enforcement officials
 - As part of a limited data set; or
 - That occurred prior to the compliance date for the covered entity

Patient Rights:

Accounting of Disclosures

- The accounting must include disclosures of PHI that occurred during the six years prior to the date of the request for an accounting, including disclosures to or by business associates of the dental practice
- The accounting must include for each disclosure:
 - The **date** of the disclosure;
 - The **name** of the entity or person who received the PHI and, if known, the address of such entity or person;
 - A **brief description of the PHI** disclosed; and
 - A **brief statement of the purpose of the disclosure** that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure
- **The request must be responded to within 60 days of receipt, with a one-time extension of 30 days available**

Patient Rights: Notice of Privacy Practices

- Privacy Rule provides that individuals have a right to a Notice of Privacy Practices that explains how dental office:
 - May use and disclose the PHI about the individual
 - Their rights under the Privacy Rule and how they may exercise them
 - The obligations to safeguard the privacy of the patient's PHI
 - Who to contact for more information about our privacy policies
 - How to file a complaint if they feel their rights under HIPAA are violated

Patient Rights: Notice of Privacy Practices

- Dental practice must provide the notice:
 - At the time of first visit for treatment or making an appointment for treatment
 - Must attempt to obtain an acknowledgement of receipt from the patient or their personal representative
 - The Notice of Privacy Practices will updated if health care provider's privacy practices are changed and new copies will be distributed if the notice is substantially revised
- Dental practice must also post the Notice of Privacy Practices in prominent locations in the facility and on their website

Verification In Order to Disclose PHI

Prior to disclosing PHI, verify that individuals to requesting the information is the patient or the person authorized to receive PHI

Telephone Encounters

- Name
- Patient Account Number
- Birthdate
- Current Address

Face to Face or In-Person Encounters

- Asking for confirmation of
 - Name
 - Date of Birth
 - Address
- Verified by reviewing
 - Driver's License
 - Passport
 - Military or Government Issued ID



Administrative Provisions

Administrative Requirements

- **Dental Practices must:**
 - Put into place administrative and technical safeguards to prevent unauthorized use or disclosure of PHI
 - Designate a privacy official
 - Train members of the workforce on privacy requirements
 - Safeguard PHI
 - Develop and apply sanctions for violations of the privacy policies and procedures
 - Establish process to receive for complaints about privacy violations and a process to investigate them
 - Develop and implement policies and procedures

Training Workforce on Policies & Procedures

- Every workforce member is required to receive training on the requirements of the HIPAA Rule and our policies & procedures to safeguard PHI
 - When first hired
 - When taking on a new role or responsibility that changes the policies and procedures they are to follow
 - When dental practice revises or updates its privacy policies and procedures
- Practice is required to document that training has been completed
- Take action against workforce members when they fail to take required training

Safeguards To Protect PHI

- **Administrative (examples)**

- Verification practices before releasing PHI;
- Maintain compliance office and privacy policies and procedures;
- Training

- **Physical (examples)**

- Documents to be properly shredded;
- Mail and fax transmissions are sent to the correct recipient; and
- PHI is not left out where visitors or other patients may see it

- **Technical**

- The storage of ePHI on secure network drives;
- Computers should be logged out of when not in use; and
- Passwords may not be written down or shared

Consequences for HIPAA Violations

- Civil Penalties
 - Fines and penalties against an organization
 - Range from \$100 to \$50,000 for each provision violated
 - Up to \$1.5 million per year
- Criminal Penalties
 - It can be a federal crime to make willful disclosure of PHI
 - Basic offense: \$5,000 and/or up to 1-year imprisonment.
 - Commercial advantage, personal gain, or malicious harm: \$250,000 and/or 10 years in prison
- Loss of Job
- Loss of professional license and/or hospital staff privileges

Changes to Policies and Procedures

- Dental practice is required to change its privacy policies and procedures when there has been a change in the law or the HIPAA Privacy Rule
- Provide copies of revised policies and procedures to workforce members
- Update Notice of Privacy Practices about how a change effects how we use or disclose PHI or provide individuals their rights.
- Notify patients when making significant changes to privacy practices



Breach Notification Rule

Breach Notification: Definition of Breach

- Breach means the acquisition, access, use, or disclosure of *unsecured* PHI in a manner not permitted, which compromises the confidentiality of the PHI
- Secured PHI is defined as PHI that is rendered unreadable, indecipherable, or unusable
 - **Example:** PHI was electronic and encrypted and the encryption key has not been compromised, then it is not a breach

Breach Notification: Exceptions to the Definition of Breach

- **There are exceptions...**
 - If the incident does not meet any of the following exceptions, then a breach assessment must be performed

Breach Notification: Exceptions to the Definition of Breach

- Any unintentional acquisition, access, or use of PHI **by a workforce member** if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted.
 - **Example:** an employee accidentally receives and opens an email containing PHI that was intended for a different employee

Breach Notification: Exceptions to the Definition of Breach

- Any inadvertent disclosure by a member of the dental practice who is authorized to access PHI at the **same** dental practice the information received as a result of such disclosure is not further used or disclosed
 - **Example:** a dental practice staff member sends another staff member the wrong patient's information, and the recipient does not further use/disclose

Breach Notification: Assessment to Determine Probability of Compromise

- The Breach Notification Rule requires a four-step analysis including, but not limited to, the following factors to determine if there is a **low probability of compromise**:
 1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 2. The unauthorized person who used the PHI or to whom the disclosure was made;
 3. Whether the PHI was actually acquired or viewed; and
 4. The extent to which the risk to the PHI has been mitigated
- If a low probability of compromise can be shown, then the incident is not a reportable breach under the HIPAA Privacy Rule

Breach Notification: Notification Requirements

- Notification to affected individual(s) must occur within 60 **calendar** days after the discovery of any breach
 - State laws may require a shorter notification time
- If breach affects >500 individuals
 - Notification to OCR through online breach notification portal
 - Notification to media
 - Within 60 days or when notification to individuals is made
- If breach affects <500 online breach notification to OCR through portal annually no later than February 28th

Breach Notification: Notification Requirements

- Notification shall include, in plain language, the following elements:
 - A brief description of what happened, the date of the breach, and date of the discovery, if known;
 - A description of the types of unsecured PHI that were involved in the breach;
 - Any steps individuals should take to protect themselves from potential harm resulting from the breach (if any);
 - A brief description of what the CE is doing to investigate the breach, to mitigate harm, and to protect against any further breaches; and
 - Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address

Breach Notification: Methods for Notification

- **Written notice:**
 - Written notification by mail to the individual at their last known address
 - If the individual agrees to electronic notice and such agreement has not been withdrawn, by email
 - The notification may be provided in one or more mailings as information is available
- If dental practice knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by mail to either the next of kin or personal representative



HIPAA Resources

Resources for Further Learning

- HHS Office for Civil Rights (OCR)
 - <https://www.hhs.gov/hipaa/for-professionals/index.html>
- HHS Office of the National Coordinator for Health IT (ONC)
 - <https://www.healthit.gov/topic/privacy-security-and-hipaa>
- Federal Trade Commission (FTC) Data Security for Small Businesses
 - <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security>



Questions?

Thank you for your attention and participation

David Holtzman, JD, CIPP/G

Executive Advisor

Cynergistek

David.Holtzman@cynergistek.com

Follow me on Twitter @HITprivacy