U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE FOR CIVIL RIGHTS

HIPAA Privacy Rule training

HIPAA Privacy Rule Training
For the
Indian Health Service

September 13, 2018

Presented By:
KAREL HADACEK, J.D.

Office for Civil Rights (OCR)

Headquarters - Washington, DC

- Policy and regulations
- Guidance materials
- Centralized Case Management Operations and Customer Response Center

Regional Offices – Denver, San Francisco/Seattle/Los Angeles, Dallas, Chicago/Kansas City, Philadelphia, Boston, New York City, Atlanta

- Investigations
- Technical Assistance
- Outreach

Who We Are

As an HHS law enforcement agency, OCR investigates complaints, conducts compliance reviews, vindicates rights, develops policy, promulgates regulations, provides technical assistance, and educates the public concerning our nation's civil rights, conscience and religious freedom, and health information privacy laws.

Complaint Process

Complaint

Possible Criminal Violation

DOJ

Accepted by DOJ

DOJ declines case & refers back to OCR

Intake & Review

Possible Privacy or Security Rule Violation

Investigation

Resolution

- OCR finds no violation
- OCR obtains voluntary compliance, corrective action, or other agreement
- OCR issues formal finding of violation

Resolution

- Entity is not covered by HIPAA
- Complaint was not filed within 180 days and an extension was not granted
- The incident described in the complaint does not violate HIPAA

Numbers at a Glance

- Over 186,453 complaints received to date
- Over 26,152 cases resolved with corrective action and/or technical assistance
- 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 Civil Monetary Penalties
- Expect to receive 24,000 complaints this year

Scope: Who is Covered?

- Covered Entities
- Health Plans
- Business Associates

Scope: Who is Covered?

- Tribes, Tribal organizations, and urban programs can be subject to HIPAA as covered health plans, covered health care providers, or both. In its definition of a "health plan" covered by HIPAA, Congress included "the IHS programs under the Indian Health Care Improvement Act (IHCIA)." -- *45 CFR § 160.103*

Business Associates

- Agents, contractors, and others hired to do the work of, or to work for, the covered entity, and such work requires the use or disclosure of protected health information ("PHI," see next slide).
- The Privacy Rule requires "satisfactory assurance," which usually takes the form of a contract, that a Business Associate (BA) will safeguard the PHI, and limit its use and disclosure.

45 CFR § 160.103

Business Associates

Provides that a business associate may use or disclose PHI only if such use or disclosure is in accordance with the HIPAA Privacy Rule's required terms for business associate contracts.

Requirements for Business Associates

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; liable for Security Rule violations

- BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule; criminal and civil liabilities attach for violations

Requirements for Business Associates

- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities

- Subcontractors of a BA are now defined as a BA; clarifying that BA liability flows to all subcontractors

Scope: What is Covered?

- **Protected Health Information** ("**PHI**"):
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held or transmitted by Covered Entities or their Business Associates
- Not PHI:
  - De-identified information
  - Employment records
  - FERPA records

45 CFR § 160.103

Uses and Disclosures: Key Points

- **No use or disclosure of PHI unless permitted or required by the Privacy Rule.**
- *Required* Disclosures:
  - To the individual who is the subject of the PHI.
  - To the Secretary of HHS in order to determine compliance.
- All other uses and disclosures in the Privacy Rule are *permissive.*
- Covered Entities may provide greater protections.

45 CFR § 164.502

Permissive Uses and Disclosures

- To the individual or personal representative
- For treatment, payment, and health care operations (TPO)
- With the opportunity to agree or object
- For specific public priorities
- "Incident to"
- Limited data sets
- As authorized by the individual

45 CFR § 164.502

To Individuals

- Besides making required disclosures, Covered Entities may also disclose PHI to their patients or enrollees. For example:
  - Health plans may contact their enrollees.
  - Providers may contact or speak with their patients.
- Covered Entities *must* treat a personal representative -- person who has authority to make decisions related to health care -- as an individual

Treatment, Payment, Health Care Operations (TPO)

- What is "**treatment**?"
- What is "**payment**?"
- What are "**health care operations**?"
- Using and disclosing for TPO
- Using and disclosing for TPO of another Covered Entity

45 CFR §§ 164.502 and 164.506

Opportunity to Agree or Object

- To use PHI in facility directories (name, location, general condition, religious affiliation to clergy)
- To disclose PHI to persons involved in care or payment for care and for notification purposes. For example:
  - Friends may pick up prescriptions.
  - Hospitals may notify family members of a patient's condition.
  - Covered entities may notify disaster relief agencies.

45 CFR § 164.510

Public Priorities

- Covered Entities may use or disclose PHI without authorization only if the use or disclosure comes within one of the listed exceptions and follows its conditions. Some examples:
  - As required by law
  - For public health activities
  - For judicial and administrative proceedings
  - For specialized government functions

45 CFR § 164.512

Incidental Uses and Disclosures

- The Privacy Rule permits uses and disclosures incidental to an otherwise permitted use or disclosure, provided minimum necessary and safeguard standards (discussed following) are met.
  - Examples: talking to a patient in a semi-private room; talking to other providers if passers-by are present; waiting-room sign-in sheets; patient charts at bedside.
- Allows for common practices if reasonably performed

45 CFR § 164.502

Minimum Necessary Standard

- Covered entities must make reasonable efforts to use, disclose, or request the minimum necessary ("MN") PHI based on purpose.
- Exceptions to the MN standard: e.g., disclosure of PHI for the purpose of treatment.
- Covered entities must identify classes of workforce members who need access to PHI to do their jobs.
- Covered entities must develop criteria to limit disclosures of and requests for PHI to the MN.

45 CFR §§ 164.502(b) and 164.514(d)

Authorizations

- Covered Entities *must* obtain an individual's authorization before using or disclosing PHI for purposes other than:
  - TPO;
  - Where the opportunity to agree or object is required;
  - Specified public priorities.

45 CFR § 164.508

Personal Representatives

- Personal representatives may sign authorization for information relevant to their representation. Generally, they are:
  - For adults/emancipated minors, persons with legal authority to make health care decisions on behalf of the patient
  - For unemancipated minors they are his/her parent or guardian

45 CFR § 164.508

Administrative Requirements

- Covered Entities must:
  - Designate a Privacy Officer
  - Designate a contact person or office to receive complaints and provide further information
  - Provide privacy training to all workforce members (document)
  - Develop and apply sanction policy for workforce members who fail to comply
  - Implement policies and procedures designed to comply with standards

45 CFR § 164.530

Administrative Requirements (cont.)

- Covered Entities must:
  - Implement administrative, technical and physical safeguards to protect privacy of PHI
  - Mitigate any harmful effect of a violation known to the covered entity to the extent practicable
  - Provide an internal complaint process for individuals;
  - Refrain from intimidating and retaliatory acts
  - Not require individuals to waive their rights

45 CFR § 164.530

Privacy Contacts

IHS Privacy Officer

Headquarters - Heather McClane

Area Privacy Coordinators

- Alaska - Diana Roberts
- Albuquerque - Maureen Cordova
- Albuquerque (Alternate) - Joel McIntosh
- Bemidji - Vacant
- Billings - Vacant
- California - Marilyn Freeman
- Great Plains - David Meservey
- Nashville - Kristina Rogers
- Navajo - Vacant
- Oklahoma - Jennifer Farris
- Phoenix - Vacant
- Portland – Roney Won
- Tucson - Robert Price

Individual Rights

Individual Rights

- Amendment
- Accounting
- Alternative Communications
- Request Restriction
- Notice of Privacy Practices
- Complaints to Covered Entity and Secretary
- Access to Copy of PHI

Amendment

An individual has the right to request that a covered entity (CE) amend protected health information (PHI) about the individual in a designated record set [DRS] as long as the DRS is maintained.

45 CFR § 164.526

Accounting

An individual has the right to receive an accounting of disclosures of PHI made by a covered entity in the six years or less prior to the request.

45 CFR § 164.528

Alternative Communication

- A covered health care provider must permit the individual to request and must accommodate reasonable requests to receive communications of PHI by alternative means and at alternative locations.

- The requirement applies to health plans if the individual clearly states that the disclosure could endanger the individual.

45 CFR § 164.522(b)

Right to Request Restrictions

- A covered entity must permit an individual to request that the covered entity restrict uses and disclosures of PHI for treatment, payment, or health care operations purposes, and for disclosures to family and friends (opportunity to agree or object disclosures).

- Covered entities are not required to agree to the request (unless to a health plan under certain circumstances).

45 CFR § 164.522(a)

Right to Request Restrictions

- Covered entity must agree to individual's request to restrict disclosure of PHI to health plan if:
  - PHI pertains solely to health care for which individual (or person on behalf of individual other than health plan) has paid the covered entity in full out of pocket
  - Disclosure is not required by other law

45 CFR § 164.522(a)

Notice of Privacy Practices

An individual has a right to adequate written notice of:

- uses and disclosures of PHI that may be made by the Covered Entity, and
- Individual's rights and Covered Entity's legal duties with respect to PHI

45 CFR § 164.520

Notice Elements

- Header – specific language in Rule
- Description of uses and disclosures
- Individual rights and how to exercise those rights
- Covered Entity duties and contact name or title & telephone number to receive complaints
- Effective Date

45 CFR § 164.520(b)

Notice of Privacy Practices

- Content must include:
  - Statements regarding sale of PHI, marketing, and other purposes that require authorization
  - For covered entities engaging in fundraising, statement that individual can opt out of fundraising communications
  - For providers, statement that covered entity must agree to restrict disclosure to health plan if individual pays out of pocket in full for health care service
  - Statement about individual's right to receive breach notifications
  - For plans that underwrite, statement that genetic information may not be used for such purposes

Provision of Notice

- **By Direct Treatment Providers**
  - First service delivery after compliance date
  - Good faith effort to obtain a written acknowledgment of receipt
- **By Health Plans**
  - At compliance date and thereafter at enrollment to new enrollees
  - Every 3 years, must tell enrollees of availability of Notice and how to obtain
  - *Health plans may distribute materially revised NPPs*:
    - By posting on web site by effective date of change and including in next annual mailing to individuals; or
    - Mailing to individuals within 60 days of material revision
- **By All Covered Entities**
  - On request to **any person**

Complaints

- Covered Entity must provide process for individuals to complain concerning Covered Entity's privacy and breach notification policies or procedures
- No provisions on how Covered Entity's complaint process must operate other than to document complaints and their disposition
- Individuals may also complain to OCR

45 CFR § 164.530(d)

Right of Access

- Access – **Scope**
- Designated record set broadly includes medical, payment, and other records used to make decisions about the individual
  - Doesn't matter how old the PHI is, where it is kept, or where it originated
  - Includes clinical laboratory test reports and underlying information (including genomic information)

45 CFR § 164.524

Right of Access

- Access – **Scope** (cont.)
  - Very limited exclusions and grounds for denial
    - E.g., psychotherapy notes, information compiled for litigation, records not used to make decisions about individuals (e.g., certain business records) BUT underlying information remains accessible
    - Covered entity may not require individual to provide rationale for request or deny based on rationale offered
    - No denial for failure to pay for health care services
    - Concerns that individual may not understand or be upset by the PHI not sufficient to deny access *45 CFR § 164.524(a)*

Right of Access

- Access – **Requests for Access**
  - Covered entity may require written request
  - Can be electronic
  - Reasonable steps to verify identity
  - BUT cannot create barrier to or unreasonably delay access
    - E.g., cannot require individual to make separate trip to office to request access

Right of Access

- Access – **Form and Format and Manner of Access**
- Individual has right to copy in form and format requested if "readily producible"
  - If PHI maintained electronically, at least one type of electronic format must be accessible by individual
  - Depends on capabilities, not willingness
  - Includes requested mode of transmission/transfer of copy
    - Right to copy by email (or mail), including unsecure email if requested by individual (plus light warning about security risks)
    - Other modes if within capabilities of entity and mode would not present unacceptable security risks to PHI on entity's systems

Right of Access

- Access – **Timeliness and Fees**
  - Access must be provided within 30 days (one 30-day extension permitted) BUT expectation that entities can respond much sooner
  - Limited fees may be charged for copy
    - Reasonable, cost-based fee for labor for copying (and creating summary or explanation, if applicable); costs for supplies and postage
    - No search and retrieval or other costs, even if authorized by State law
    - Entities strongly encouraged to provide free copies

Right of Access

No Fees Permitted For:

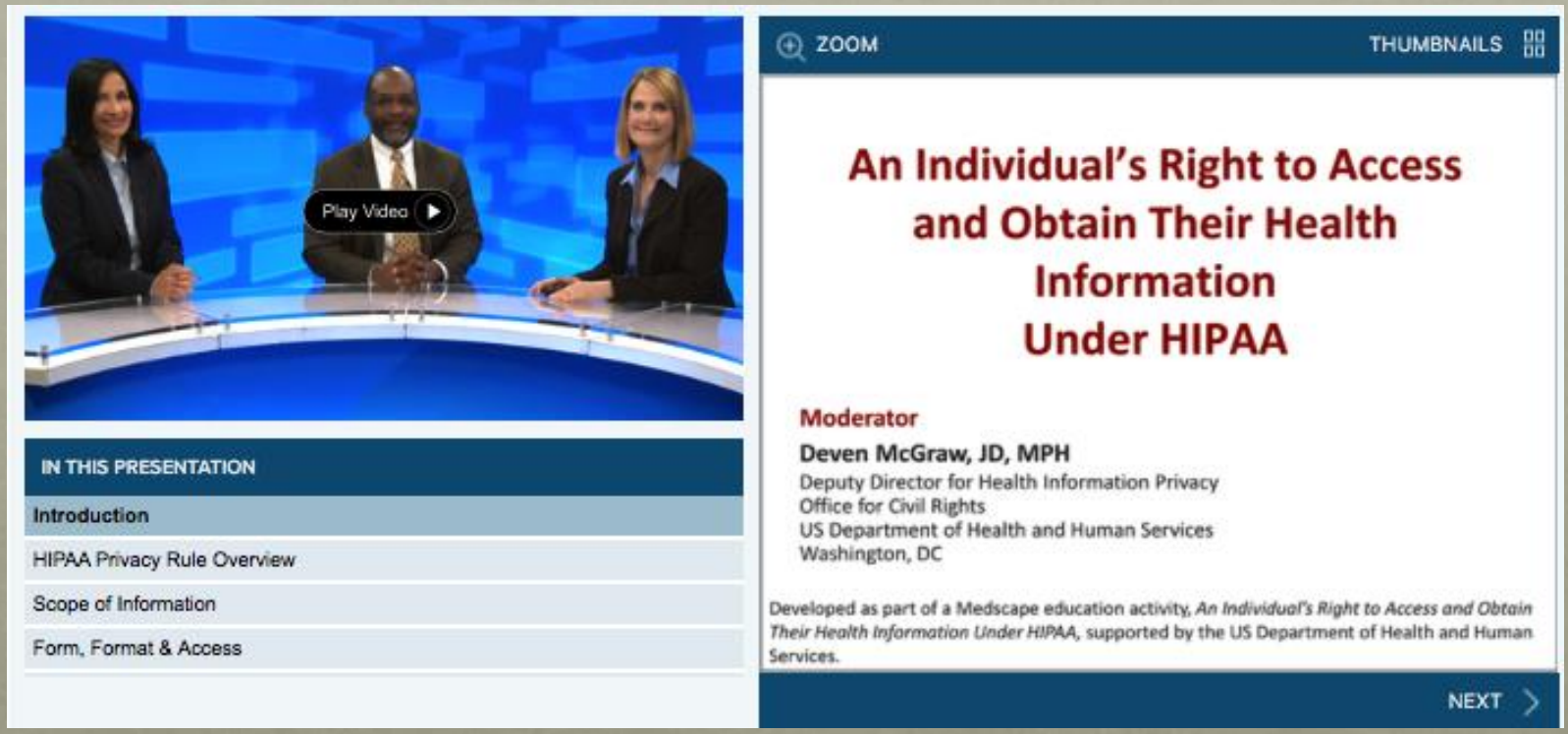
- Providing access through certified EHR technology (*i.e.,* View, Download, Transmit)
- Administrative overhead costs for outsourcing access requests to a business associate
- Viewing and inspecting PHI only

Access: Designated 3rd Party

- **Third Party Access to an Individual's PHI**
  - Individual's right of access includes directing a covered entity to transmit PHI directly to another person, in writing, signed, designating the person and where to send a copy (45 CFR § 164.524)
  - Individual may also authorize disclosures to third parties, whereby third parties initiate a request for the PHI on their own behalf if certain conditions are met (45 CFR § 164.508)

Web-based Training

Web-based Video Training for Free Continuing Medical Education and Continuing Education Credit for Health Care Professionals via Medscape



http://www.medscape.org/viewarticle/876110

Compliance Challenges

Lack of Business Associate Agreements

HIPAA generally requires that covered entities and business associates enter into agreements with their business associates to ensure that the business associates will appropriately safeguard protected health information. *See 45 CFR § 164.504(e).* Examples of Potential Business Associates:

- A collections agency providing debt collection services to a health care provider which involves access to protected health information.
- Attorney for covered entity or health plan
- Contractor

Enforcement

Enforcement Process

- https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html

- OCR reviews the information, or evidence, that it gathers in each case. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:
  - Voluntary compliance;
  - Corrective action; and/or
  - Resolution agreement.

Enforcement Process

- Letter of Opportunity with Resolution Agreement and Corrective Action Plan
- Notice of Proposed Determination
  - Entity may request a hearing before Administrative Law Judge
- Notice of Final Determination

Recent Enforcement Actions

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

St. Luke's Roosevelt Hospital Center

- Impermissible disclosure of sensitive PHI to individual's employer
- Prior related breach of sensitive information but failure to address vulnerabilities
- $387,200 Settlement with Corrective Action Plan

- **Memorial Hermann Health System**
  - Impermissible disclosure of patient's PHI in press release
  - Failure to timely document sanctioning of workforce members
  - $2,400,000 Resolution Agreement with Corrective Action Plan

Recent Enforcement Actions

Center for Children's Digestive Health

- OCR initiated compliance review after investigating its business associate
- Impermissible disclosure of PHI for several years to record storage vendor without a BAA
- $31,000 Resolution Agreement with Corrective Action Plan

General Enforcement Highlights

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 3 civil money penalties

Corrective Action

Corrective Actions May Include:

- Updating policies and procedures
- Training of workforce
- Mitigation
- CAPs may include monitoring

Good Practices

Some Good Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Dispose of paper PHI that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy

Questions?

Karel Hadacek, J.D.
OCR Investigator
Karel.Hadacek@hhs.gov
303-844-7836

Thank You!