MSHRM MICHIGAN SOCIETY OF HEALTHCARE RISK MANAGEMENT

The "Real" HIPAA Privacy Rule in 2018

Chad P. Brouillard, Esq.
Partner
Foster & Eldridge
cbrouillard@fosteld.com
617-252-3366

Conflict of Interest Disclosure

Chad P. Brouillard, Esq. does not have any real or apparent conflict(s) of interests or vested interest(s) that may have a direct bearing on the subject matter of the continuing education activity.

Learning Objectives

This presentation will enable participants to:

- Differentiate between real HIPAA Privacy concerns and the myths of HIPAA Privacy.
- Define disclosures under HIPAA Privacy Rules.
- Avoid an OCR audit for violation of HIPAA Privacy Rules.

HIPAA is NOT a Code of Silence

Hipaa's Use as Code of Silence Often Misinterprets the Law

"What many people don't realize is that HIPAA not only protects personal health information from misuse, but *also* enables that personal health information to be accessed, used, or disclosed interoperably, when and where it is needed for patient care." Office of National Coordinator's Health IT Buzz

HIPAA - Timeline

- HIPAA (1996)
- Privacy Standards (1999)
- Security Rule (2005)
- HITECH ACT (2009)
- Omnibus Rule (2013)
- Final Rule Effective Date: September 23, 2013

Omnibus Rule

- Permitted Uses/Disclosures
- Updated Privacy Practices
- Business Associates and Subcontractors
- Breach Notification Analysis Shifted
- Electronic Copy of Records on Demand
- Increased Enforcement Standards

HIPAA Security (Data Breach)

- HIPAA Security Rules (Federal)
- HITECH enhancements
- FTC Red Flag Rules
- State Laws

HIPAA Privacy

- Protection of PHI
- Patient Rights
- Use & Disclosure Requirements
- Big Concern During Litigation
- OCR Enforcement
- Meaningful Use Privacy Audits

OCR Privacy Reviews…

Non-Breach Compliance Reviews

This page shows the enforcement results by calendar year according to the type of closure, which includes the percentage of the total resolutions for each category. This represents the number of compliance reviews that OCR has resolved.

YEAR	INVESTIGATED: NO VIOLATION		INVESTIGATED: CORRECTIVE ACTION OBTAINED		RESOLVED AFTER INTAKE AND REVIEW		OTHER		TOTAL RESOLUTIONS
2013	1	4%	21	84%	3	12%	0	0%	25
2014	2	7%	27	90%	0	0%	1	3%	30

vs. Security Reviews

Breach Compliance Reviews

This page shows the enforcement results by calendar year according to the type of closure, which includes the percentage of the total resolutions for each category. This represents the number of compliance reviews that OCR has resolved.

YEAR	INVESTIGATED: NO VIOLATION		INVESTIGATED: CORRECTIVE ACTION OBTAINED		RESOLVED AFTER INTAKE AND REVIEW		OTHER		TOTAL RESOLUTIONS
2013	44	14%	237	78%	15	5%	8	3%	304
2014	11	2%	415	90%	16	3%	20	4%	462

HIPAA - Permitted Use

- Permitted Uses v. Authorized Use
- Permitted Uses
  - A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:
  - (1) To the Individual (unless required for access or accounting of disclosures);
  - (2) Treatment, Payment, and Health Care Operations;
  - (3) Opportunity to Agree or Object;
  - (4) Incident to an otherwise permitted use and disclosure;
  - (5) Public Interest and Benefit Activities; and
  - (6) Limited Data Set for the purposes of research, public health or health care operations.

HIPAA- TPO

- **Treatment, payment, and health care operations** activities
- HIPAA also permits the covered entity that collected or created the PHI to disclose it to another covered entity **for treatment, payment, the health care operations** of the *recipient* covered entity.

HIPAA - TPO & Interoperability

- Quality assessment and improvement activities
- Clinical guidelines
- Patient safety activities
- Population-based activities relating to improving health or reducing health care cost
- Protocols
- Case management and care coordination (including care planning)

HIPAA - TPO & Interoperability

- Contacting health care providers and patients with information about treatment alternatives
- Reviewing qualifications of health care professionals
- Evaluating performance of providers and/or health plans
- Conducting training programs or credentialing activities
- Supporting fraud and abuse detection and compliance programs.

HIPAA - TPO & Interoperability

- Both covered entities must have or have had a relationship with the patient (can be a past or present patient)
- The PHI requested must pertain to the relationship
- The discloser must disclose only the minimum information necessary for the health care operation at hand.

Poll Time – Family Matters

- A) Mandatory
- B) Permissible
- C) Impermissible
- D) Addressable

HIPAA - Family & Friends

- The Privacy Rule permits covered entities to disclose limited information to family members, friends, partners or other persons regarding an individual's care, even when the individual is not present.
- Use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed.

HIPAA - Family & Friends

- HIPAA does not apply to family & friends, it applies to healthcare entities and providers.
- Listening is not a violation of HIPAA.
- Using it to shutdown conversation may set an adversarial relationship.

HIPAA - Family & Friends

- 2016 Orlando Nightclub Shooting
- Is unmarried same sex-couple included in definition?
- What if same sex marriage is not recognized in that state?
- "The Privacy Rule defers to a covered entity's professional judgment in these cases and does not require the entity to verify that a person is a family member, friend, or otherwise involved in the patient's care or payment for care." HHS Guidance

HIPAA - Family & Friends

- Not providing a personal representative information would be a violation of Privacy Rule
- Some states may confer automatic personal representative status on spouses.

HIPAA - Permitted Use

- (5) Public Interest and Benefit Activities;
  - ***Judicial and Administrative Proceedings.***
    - Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.

HIPAA - Permitted Use

- (5) Public Interest and Benefit Activities;
  - ***Required by Law.*** Covered entities may use and disclose protected health information without individual authorization as required by law (including by statute, regulation, or court orders).

HIPAA OMNIMBUS RULE UPDATE – MARKETING USES

- **Marketing**: The Omnibus Rule imposes stricter limitations on marketing communications made in exchange for financial remuneration. Specifically, written communications promoting purchase or use of a third party's products or services require prior individual authorization if the covered entity receives financial remuneration in exchange for sending the communication.
- **Fundraising**: The Omnibus Rule provides a limited set of circumstances in which a covered entity can use and disclose certain PHI for fundraising without an authorization. Regardless of whether an authorization for fundraising was required or obtained, covered entities must provide an individual with an opt-out of receiving future fundraising communications.
- **Sale of PHI**: The Omnibus Rule prohibits the sale of PHI unless the individual has authorized it.

HIPAA - Authorized Use

- Authorized Uses
  - A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for a Permitted Use.
  - An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party.
  - Examples that require an individual's authorization:
    - Life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.
  - All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.

Who is Requesting

- Patient
- POA
- Health Care Proxy
- When no executor or administrator of the estate exists who, if anyone can receive the medical information of the deceased
- Guardianships

HIPAA - Personal Representative

- **Other HIPAA Provisions: Personal Representatives**
- The Privacy Rule requires a covered entity to treat a *"personal representative"* the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.
- A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate.
- The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

HIPAA OMNIMBUS RULE UPDATE – Disclosure of Decedent's PHI

- Baseline HIPAA Rule is that PHI must be protected for 50 years after patient's death.
- Permitted Exception: A Covered Entity may disclose PHI of a decedent if they have reasonable assurances that disclosure is made to those "involved in the individual's care" and payment.
- **But: Not if the Decedent had previously expressed a preference to the contrary.**
- Suggests a Health Care Proxy executed prior to death may be enough.

HIPAA - Minors

- **Other HIPAA Provisions: Special Case: Minors**
  - In most cases, parents are the personal representatives for their minor children.
  - When the parent is not the personal representative, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children.

Minors

- State Laws
- Emancipated Minors
- Pregnant Minors
- Notification Laws

What is Requested

- Records
  - Designated Records Set
  - Sensitive vs. Protected information
  - Minimum Necessary Rule

Designated Record Set

- Medical records and billing records about individuals maintained by or for a covered health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.
- Not audit trails!

Sensitive Information

- Substance abuse treatment records (SAMHSA vs. HIPAA)
- Blood alcohol test results
- Venereal Disease
- AIDS/HIV Test Records
- Genetic Information
- Records of Minors Competent to Consent to Care
- Psychologist Communications
- Social Workers Records and Communications
- Allied Mental Health/Human Services Professional Communications
- Psychotherapist Communications
- Sexual Assault Counselor Communications
- Domestic Violence Counselor Communications

St. Luke's-Roosevelt Hospital Center Inc. (Spencer Cox Center) (May 2017)

- $387K, AIDS/HIV treatment center
- Faxed sensitive diagnostic testing to employer instead of sending to PO Box as instructed.
- This impermissible disclosure included sensitive information concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse.
- One prior incident nine months prior with a different patient.

Sensitive Information

- Mental Health Records - Special Concerns
  - Ideally, release full records to the patient
  - However, if, in the physician's reasonable judgment, providing the entire medical record would adversely affect the patient's well-being, the provider may provide a summary of the record.
  - If the patient continues to request the entire record, the physician may make it available to either the patient's attorney, with the patient's consent, or to another psychotherapist, as designated by the patient.

Minimum Necessary Use

- The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.
- Does not apply to release to patient, to other health care providers, legal requests, OCR, etc.
- Generally would apply to TPO uses and disclosures.
- Example: role based access of an EHR.
- Enforcement via audit trail review

Triple-S Management Corporation Resolution Agreement - Part 1 (November 2015)

- 3.5 Mil, Insurance Holding Company
- Started as Security Rule breach notification case, but during audit, noted Privacy Rule violations.
- Cited for failing to adhere to minimum necessary rule.

Memorial Healthcare System (MHS) Resolution Agreement - $5.5M fine

The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals.

HIPAA OMNIMBUS RULE UPDATE – Limitations on disclosure

- Out of Pocket Payments: Patients have a right to restrict disclosure of medical information relative to services they have paid for completely out of their own funds (no insurance.)
- Genetic Information: Mostly directed at health plans, clear that genetic information is PHI, and cannot be disclosed to underwriting.

How is the Request Made

- Authorization
- Subpoena vs Court Order
  - Beware orders or subpoenas from out of state
- Board of Medicine

When to Release

- Time frame required for response to request
  - Typically, 30 days
  - However, if the medical records are not maintained or are not accessible on-site, then a 60 days to provide the records.
  - A physician may extend the time for production once—for an additional 30 days by providing the requestor with a written statement of the reason(s) for the delay and the date by which the physician will produce the records.
  - In the case of a medical emergency or Social Security claims, records should be provided as soon as possible.

Cost of Release

- Fees for records:
  - The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) 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; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual. See 45 CFR 164.524(c)(4). 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 above even if such costs are authorized by State law.
  - Providers may not withhold medical records from a patient with unpaid medical services.
  - Providers may require that the patient pay the copying costs before providing records.
  - Do not forget your state's laws!

Right to Access (2016 Guidance)

- Covered entities should be able to readily produce electronic information in electronic form and provide protected health information (PHI) via mail and email.
- Many barriers to access are contrary to the Privacy Rule, such as requiring a physical visit or use of a web portal to make requests, charging inappropriate fees, or requiring that individuals provide a reason for their request.
- Patients can request hard copy materials to be scanned and converted to electronic.

Right to Access (2016 Guidance)

In addition, two categories of information are expressly excluded from the right to access:

- **Psychotherapy notes**, which are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session, that are maintained separate from the rest of the patient's medical record. See 45 CFR 164.524(a)(1)(i) and 164.501.
- **Litigation materials**, or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. See 45 CFR 164.524(a)(1)(ii).

Right to Access (2016 Guidance)

Other exceptions:

- Reasonable likelihood of harm
- The requested PHI is in a designated record set that is part of a research study that includes treatment (e.g., clinical trial) and is still in progress, provided the individual agreed to the temporary suspension of access when consenting to participate in the research. The individual's right of access is reinstated upon completion of the research.
- The requested PHI is in Privacy Act protected records (i.e., certain records under the control of a federal agency, which may be maintained by a federal agency or a contractor to a federal agency), if the denial of access is consistent with the requirements of the Act.
- The requested PHI was obtained by someone other than a health care provider (e.g., a family member of the individual) under a promise of confidentiality, and providing access to the information would be reasonably likely to reveal the source of the information.

Denial

- Generally 30 days
- In writing
- Plain English for denial reasons

Privacy Rule Violation Examples

- Celebrities
- Facebook Case
- Delivering Diagnosis in the Waiting Room
- Withholding Medical Records

HIPAA Privacy Exceptions

- Required by law
- Health Care Operations
- Public health authorities
- Health research
- Abuse, neglect, or domestic violence reports
- Law enforcement
- Judicial and administrative proceedings
- Health Oversight Agencies
- Worker's compensation

Memorial Hermann Health System (May 2017)

- $2.4M, Fraudulent ID case
- Patient was caught trying to use a fraudulent ID during medical care. Patient info was shared with authorities relative to the crime (permissible.)
- Hospital administrators then approve a press release with patient's name in the title.
- Corrective action plan included attestation re HIPAA compliance from all affiliated hospitals in system.
- Overkill anyone?

University of California at Los Angeles Health System (UCLAHS) Resolution Agreement (July 2011)

- Celebrity Cases – two celebrity patients filed OCR complaints
- UCLAHS employees repeatedly and without permissible reason looked at the electronic protected health information of these patients.
- $865,500 fine
- The corrective action plan requires UCLAHS to implement Privacy and Security policies and procedures approved by OCR, to conduct regular and robust trainings for all UCLAHS employees who use protected health information, to sanction offending employees, and to designate an independent monitor who will assess UCLAHS compliance with the plan over 3 years.

Facebook X-Ray Case

Shasta Regional Medical Center (SRMC) Resolution Agreement

- Senior leaders speak to Newspaper about specifics of treatment
- In response to public allegations of Medicare Fraud
- 275K fine

Complete P.T., Pool & Land Physical Therapy, Inc. Resolution Agreement (Feb 2016)

- Privacy Rule Violation
- 25K fine
- Posting testimonials with patient pictures
- No patient authorizations
- No Security component

Cignet Health Resolution Agreement (July 2011)

- 4.3 Mil, first sanction after HITECH
- Essentially a technical Privacy Rule violation
- The HIPAA Privacy Rule requires that a covered entity provide a patient with a copy of their medical records within 30 (and no later than 60) days of the patient's request. The CMP for these violations is $1.3 million.
- Remainder of the fine for willful neglect and failure to cooperate with investigation.

Business Associates

HIPAA OMNIBUS BAA UPDATE

- Expanding definitions of Business Associates
- Direct Liability for Business Associates
- Obligations flow from all BAs to subcontractors
- BAA must be updated accordingly to address subcontractors!

Triple-S Management Corporation Resolution Agreement - Part 2 (November 2015)

- 3.5 Mil, Insurance Holding Company
- Started as Security Rule breach notification case, but during audit, noted Privacy Rule violations.
- Cited for not using appropriate business associate agreements.

HIPAA OMNIMBUS RULE UPDATE – Notice of Privacy Practices

- Out of Pocket Payments
- Genetic Information
- Restrictions on Marketing & Fundraising
- Will Not Sell PHI
- Duty to Report Breach

Responding to a Privacy Rule Based Breach

- If involves an HIT, privacy rule complaints may also have a security component. (Why did this person have access? Technical means to limit access, or monitor use?)
- Treat it as a potential Security Rule breach.
- Policies, training, auditing.
- If involves an Employee, a criminal/background check may be key.

Audit Preparedness

- Update and redistribute Notices of Privacy Practices;
- Revise Business Associate Agreement template forms;
- Evaluate existing (sub)contractor arrangements re need for Business Associate Agreements;
- Revise HIPAA Policies and Procedures, including modifications to address response to potential breaches involving unsecured PHI;
- Analyze current arrangements for compliance with restrictions on the sale of PHI, and marketing and fundraising restrictions; and
- Train employees on updated obligations.

MSHRM MICHIGAN SOCIETY OF HEALTHCARE RISK MANAGEMENT

Questions?