

HEALTH INSURANCE PORTABILITY
and ACCOUNTABILITY ACT

HIPAA

ADMINISTRATIVE SIMPLIFICATION:
PRIVACY, SECURITY, TRANSACTIONS

LECOM
2018 Primary Care Conference
HIPAA, HITECH, Headaches:
Having the Viability to Escape
Liability


Richard Ferretti, Esquire
General Counsel and Risk Mgmt. Dir.
Jeffrey Myers, Esquire
Associate General Counsel

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Top Secret

CONFIDENTIAL


2



HIPAA

1. Designed to protect the privacy of personal (*Protected*) health information (PHI) and to control how it is used, transmitted and disclosed. Enforced by the Office of Civil Rights of the Department of Health and Human Services (HHS/OCR).
2. What is “Protected Health Information”?
 - a. “Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - b. Relates to the past, present, or future physical or mental health condition of an 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; and
 - i. That identifies the individual; or
 - ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.”

<https://www.hhs.gov/ocr/index.html>
<https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/>



HIPAA (CONT.)

3. HIPAA has 3 main components:
 - a. Electronic transaction standards (e.g. certain formats and code sets must be in place for electronic transmissions);
 - b. Security standard (for electronically receiving, storing and using PHI, etc.); and
 - c. Privacy standard: how you communicate with and about patients.

<https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>




HIPAA (CONT.)

4. Who does HIPAA cover?
 - a. Health care providers;
 - b. Health plans;
 - c. Health care clearinghouses (information processors);

Collectively “CE”— Covered Entities and


 - d. Trading partners (CE w/ whom access is shared);
 - e. Access vendors (Limited/inadvertent access from CE);
 - f. Business associates of covered entities; and
 - g. Subcontractors of business associates.

https://privacyruleandresearch.nih.gov/pr_06.asp



HIPAA – Rights and Obligations


1. Individual rights created by HIPAA.
 - a. Receive **notice** of a CE’s privacy practices – prior to the first instance of treatment, including:
 - i. A description of permitted uses/disclosures;
 - ii. A statement of individual rights;
 - iii. Rules on marketing and fundraising;
 - iv. CE duties;
 - v. Rights to complain to HHS;
 - vi. A contact person w/ the CE; and
 - vii. Effective dates of the practices.



HIPAA – Rights and Obligations (CONT.)

1. Individual rights created by HIPAA (cont.).
 - b. Restrict use of PHI.
 - c. Access and copy their own PHI (30 days on site/60 days for off site records).
 - d. Amend their own PHI.
 - e. Receive an accounting of uses/disclosures of PHI – up to 6 years back.
 - f. Put restrictions on disclosure of PHI.
 - g. Request/receive confidential communication in a particular way.
 - h. File complaints w/ HHS/OCR.


<https://www.privacyrights.org/consumer-guides/hipaa-privacy-rule-patients-rights>



HIPAA – Rights and Obligations (CONT.)


2. CE Obligations.
 - a. Post the notice of privacy practices on web site.
 - b. Develop privacy procedures and policies.
 - c. Name a privacy officer.
 - d. Sanction offenders.
 - e. Make required disclosures of PHI – to HHS/individual.
3. Information that can make data “PHI”.

a. Name	e. URL's/IP
b. Address	f. Biometric
c. Numbers – phone/SSN/Health Plan	g. Photos
d. Vehicle identifiers	h. “Catch all”



HIPAA – Rights and Obligations (CONT.)


4. Allowable third party access to PHI.
 - a. Basic rule: “need to know.”
 - b. “Minimum Necessary Rule”, e.g., between employees of a covered entity or between a covered entity and a business associate.
 - c. Verification of the identity of an intended (legitimate) recipient required.
 - d. For information involving “Treatment/Operations/Payment” – with consent of the patient (optional, except if state law makes it mandatory).
 - e. Governmental; litigation; and public health demands allow disclosure without consent or authorization.
 - f. Individual patient always has a right to access.



HIPAA – Rights and Obligations (CONT.)


5. Other disclosures—for research, marketing, fundraising—must be *authorized* by patient or parent/guardian; such that:
 - a. Information must be described.
 - b. Purpose of the authorization is stated.
 - c. Disclosers and recipients are listed.
 - d. Dates of authorization and use are indicated.
 - e. Right to revoke is made clear.
 - f. Remuneration to be received listed.
 - g. Plain language utilized.
 - h. A signature is required.

<https://www.hhs.gov/hipaa/for-professionals/faq/authorizations>



HIPAA – Rights and Obligations (CONT.)

6. Some disclosures are allowed after only an opportunity to agree or object is given; for example:
 - a. Directories;
 - b. To individuals known to patient, e.g. waiting family members; or
 - c. To disaster relief agencies.



11




HIPAA – Rights and Obligations (CONT.)

7. Some disclosures require no authorization:
 - a. To the patient;
 - b. Public health authorities (disease prevention/investigations);
 - c. To prevent/end abuse;
 - d. To oversight agencies;
 - e. In judicial/administrative proceedings;
 - f. For law enforcement purposes;
 - g. To coroners/medical examiners;
 - h. For organ donations;
 - i. Within correctional institutions; or
 - j. In connection with workers' compensation claims.

<https://www.law.cornell.edu/cfr/text/45/164.512>




12




HIPAA – Rights and Obligations (CONT.)

8. Records to which access need not be given.
 - a. Psychotherapy notes;
 - b. Information compiled in anticipation of litigation;
 - c. Information compiled by research labs that do not report patient-specific results; or
 - d. Requests to correctional institutions.

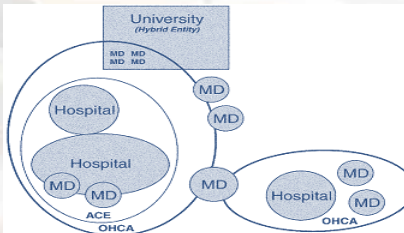


13



HIPAA – Business Associates

1. What is a “Business Associate”?
 - a. It is a person or entity outside of the Covered Entity (CE);
 - b. Which performs services for or on behalf of the CE;
 - c. Which involves the use or disclosure of PHI (claims processing, utilization review, billing, etc.).
 - d. Could be an entity that is itself a CE;
 - e. But not an affiliated entity or another element of an “Organized Health Care Arrangement”.



<https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>

14



Business Associates (CONT.)

2. Obligations with Business Associates.
 - a. A covered entity must have a written business associate *contract* or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do.
 - b. The contract must require the business associate to comply with HIPAA.
 - c. CEs must ensure HIPAA compliance.

<https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>

15



HIPAA – Business Associates (CONT.)

3. Elements of a proper BA Agreement.
 - a. Identify the permitted use/disclosures of PHI.
 - b. Prohibit any uses/disclosures of PHI violative of HIPAA.
 - c. Prohibit any uses/disclosures inconsistent with the agreement.
 - d. Require safeguards by BA and subs.
 - e. Require disclosures of breaches.
 - f. Cover subcontractors.
 - g. Require recognition of and compliance with all individual rights.
 - h. Require return/destruction of PHI upon termination or the contract/relationship.
 - i. Require cure of any breach.
 - j. Notice to HHS, if necessary.

16

HITECH



The Health Information Technology for
Economic and Clinical Health Act
of the
American Recovery and
Reinvestment Act of 2009

17



HITECH

1. Key Aspects:
 - a. One word: PUNITIVE.
 - b. Enhances privacy and security provisions of HIPAA.
 - c. Does give a clear definition of "breach" (no damage required).
 - d. Has provisions for notification of breaches.
 - e. Puts greater burdens on business associates/subcontractors.
 - f. Increases penalties.
 - g. Provides for more enforcement.


18



HITECH (CONT.)

2. Definition of “breach”.
 - a. Unauthorized acquisition, access, use or disclosure;
 - b. Of protected health information;
 - c. Which compromises the security or privacy of the information;
 - d. Except:
 - i. Where the unauthorized person who received the information would not reasonably be able to retain it; or
 - ii. Where the breach is unintentional and in good faith and does not result in further use or disclosure; or
 - iii. If it is between covered persons working in covered entities or business associates and would not be further disclosed.


<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>



HITECH (CONT.)

2. Definition of “breach” (CONT.)
 - e. Presumption of breach upon unauthorized release/use of PHI unless low probability or compromise shown:
 - ✓ Nature and extent of PHI;
 - ✓ The person to whom the breach was made;
 - ✓ Whether there was an actual viewing or acquisition of the PHI; and
 - ✓ Whether there has been any *mitigation*.

Note: the terms “covered entity” (CE) and “business associate” (BA) have the same definition as under HIPAA.



HITECH (CONT.)

3. Required notification of breaches:
 - a. CE must notify each individual whose PHI has been or is reasonably believed to have been disclosed.
 - b. BA must notify CE of any breach and identify all individuals affected.
 - c. Breach is treated as known on the first day it is discovered or should have been discovered.
 - d. All notifications must be made no later than 60 days after notice of discovered breach.
 - e. Notice must be by first class mail unless the individual has expressed a preference for electronic notice.
 - f. If there are 10 or more individuals for whom a CE does not have contact information, then post notice on web site.
 - g. In cases of “imminent misuse”, notice is to be by phone.
 - h. In cases of 500 or more affected individuals, notice required to “prominent media outlets.”

21



HITECH (CONT.)

4. Content of disclosures:
 - a. A description of what happened;
 - b. When it happened;
 - c. What was disclosed;
 - d. What steps the individual should take;
 - e. The nature of the CE’s investigation; and
 - f. A contact person.

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

22



HITECH (CONT.)

5. Restrictions to disclosure to health plans
 - a. Cannot make disclosures to health care plans;
 - b. Even for purposes of payment or health care operations;
 - c. Where the total cost of the service(s) has been paid in full by the individual; and
 - d. The individual requests that disclosures not be made.

<http://bok.ahima.org/doc?oid=300415#.WWzTQlgrKUK>

23




HITECH (CONT.)

6. Other disclosure limitations.
 - a. All allowable disclosures of PHI (payment/treatment/healthcare operations) must be to the minimum extent necessary.
 - b. PHI is not to be disclosed through sale, except with individual consent.
 - c. A listing of disclosures must be provided upon request for as long as six years prior to the request.
7. Other individual rights.
 - a. To review all PHI in electronic format;
 - b. To refuse to allow PHI to be used for marketing; and
 - c. To be given an “opt out” on any fundraising communications.

<http://www.hipaasurvivalguide.com/hitech-act-summary.php>

24

A background image for the slide showing a pair of scales of justice and a stack of money, symbolizing law and finance.

HITECH (CONT.)

8. Application of security provisions to BAs.
 - a. Security provisions of HIPAA relating to PHI and the penalties for breach now apply to BAs;
 - b. Any use or disclosure of PHI by a BA is subject to the same limitations that apply to CEs; and
 - c. BAs should have agreements with subcontractors requiring HIPAA/HITECH compliance.


25

A background image for the slide showing a pair of scales of justice and a stack of money, symbolizing law and finance.

HITECH (CONT.)

9. Regulatory requirements for BA agreements
 - a. Must have BAA where BA provides data transmission of PHI;
 - b. BAA must explicitly require HIPAA compliance;
 - c. Must have a mandatory provision on reporting security incidents;
 - d. Must have assurance that BA will have similar agreement with subcontractors; and
 - e. Agreement must terminate in the event of a HIPAA violation.


26



HIPAA/HITECH - Enforcement

1. Enforcement is handled by HHS OCR. No private actions allowed.
2. Investigations mandated for all possible violations.
3. A portion of civil money penalties will go to affected individuals.
4. Statistics--# of cases and types of issues:

YEAR	INVESTIGATED: NO VIOLATION		RESOLVED AFTER INTAKE AND REVIEW		INVESTIGATED: CORRECTIVE ACTION OBTAINED		TECHNICAL ASSISTANCE PROVIDED		TOTAL RESOLUTIONS
2013	994	7%	7068	49%	3470	24%	2754	19%	14286
2014	668	4%	10653	60%	1288	7%	5128	29%	17737
2015	359	2%	12785	72%	730	4%	3820	22%	17694



Enforcement (CONT.)

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2015	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2014	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2013	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2012	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Minimum Necessary
2011	Impermissible Uses & Disclosures	Safeguards	Access	Notice to Individuals	Minimum Necessary



Enforcement (CONT.)

5. Penalties: amounts and examples (<https://www.truevault.com/blog/what-is-the-penalty-for-a-hipaa-violation.html>) :


Violation Category	Each Violation	Total CMP for Violations of an Identical Provision in a Calendar Year
Unknowing	\$100 – \$50,000	\$1,500,000
Reasonable Cause	\$1,000 – \$50,000	\$1,500,000
Willful Neglect – Corrected	\$10,000 – \$50,000	\$1,500,000
Willful Neglect – Not Corrected	At least \$50,000	\$1,500,000

29



Entity Fined	Fine	Violation
CIGNET	\$4,300,000	Online database application error.
Alaska Department of Health and Human Services	\$1,700,000	Unencrypted USB hard drive stolen, poor policies and risk analysis.
WellPoint	\$1,700,000	Did not have technical safeguards in place to verify the person/entity seeking access to PHI in the database. Failed to conduct a tech eval in response to software upgrade.
Blue Cross Blue Shield of Tennessee	\$1,500,000	57 unencrypted hard drives stolen.
Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates	\$1,500,000	Unencrypted laptop stolen, poor risk analysis, policies.
Affinity Health Plan	\$1,215,780	Returned photocopiers without erasing the hard drives.

30



Enforcement (CONT.)

6. The Big Two:
 - a. Advocate Health Systems: 2016, 5.55M.
 - i. Three incidents, 4M patients' records compromised.
 - ii. Two incidents involved stolen laptops; one a hack of a business associate.
 - iii. Key faults: poor risk assessment; access to IT systems; BA compliance.
 - b. NY Presbyterian Hospital and Columbia Univ.: 2014, 4.8M.
 - i. One incident where a *single* physician attempted to deactivate a personal computer that was connected to the New York-Presbyterian network that contained patient information.
 - ii. A lack of technical barriers then led to patients' health information being accessible through public search engines.

<http://www.beckershospitalreview.com/healthcare-information-technology/10-largest-hipaa-settlement-fines.html>




Enforcement (CONT.)

7. And people become guests of the state as a result of violations.
 - a. Joshua Hippler: from December 1, 2012, through January 14, 2013, while employed by a Texas hospital, he obtained protected health information with the intent to use the information for personal gain. He pled guilty, was sentenced to 18 months in jail, three years probation and had to pay restitution. Ironically, the court records are sealed.
 - b. A cardiothoracic surgeon, Huping Zhou, got four months in jail plus a fine for illegally accessing the UCLA medical records system over 300 times, viewing the health records of his immediate supervisor, his co-workers, and several celebrities, including Arnold Schwarzenegger, Drew Barrymore, Leonardo DiCaprio, and Tom Hanks.

<https://www.justice.gov/usao-edtx/pr/former-hospital-employee-pleads-guilty-criminal-hippa-charges>


<https://www.medprodisposal.com/20-catastrophic-hipaa-violation-cases-to-open-your-eyes/>



Enforcement (CONT.)

7. And people become guests of the state as a result of violations (cont.).
 - c. A former South Carolina state employee, was sentenced to three years of probation, plus community service, after he sent personal information about more than 228,000 Medicaid recipients to his personal e-mail account. He plead guilty to four counts of willful examination of private records by a public employee and one count of criminal conspiracy.
 - d. Sometimes, HIPAA offenses are involved in fraud and abuse cases as well. E.g., in October 2013, a former nursing assistant at a Florida assisted living facility, was sentenced to 37 months in prison after pleading guilty to several federal offenses, including conspiracy to defraud the U.S. government and wrongful disclosure of HIPAA protected information.
<http://www.inforisktoday.com/prison-term-in-hipaa-violation-case-a-7938>

33



Enforcement (CONT.)

8. Aggravating factors in penalty assessment.
 - a. Disclosures involving especially sensitive information:
 - I. HIV;
 - II. Psychiatric; and
 - III. Genetic data (also protected by the GINA law);
 - b. High number of patients affected;
 - c. Lack of truthfulness of CE; and
 - d. Past violations.

34




Enforcement (CONT.)

9. Mitigating factors in penalty assessment:
 - a. Disclosure despite good compliance plan;
 - b. Disclosure occurred in an effort to aid a patient;
 - c. Lack of real harm to patients;
 - d. Admission and cooperation in any investigation; and
 - e. Remorse.

<https://www.hipaa.com/hipaa-final-rule-enforcement-factors-for-determining-civil-money-penalties-for-hipaa-violations/>

35




Scenarios: HIPAA in Practice

1. Is it a good idea to talk about cases on social media, even if you do not name the patient?
 - ✓ An ER physician, who worked at Westerly Hospital in RI, “did not include the patient’s name, but she wrote enough that others in the community could identify the patient,” after caring for the patient following a car accident.
 - ✓ The hospital's solution? Terminate the doctor's privileges. On April 13, 2011, the Rhode Island Board of Medical Licensure found her guilty of "unprofessional conduct." The Board handed out a \$500 fine with instructions for her to attend a CME course dealing with physician-patient confidentiality issues.
 - ✓ That is a big NO!

<http://boards.medscape.com/forums/?128@@.2a090c48!comment=1>


36



Scenarios (CONT.)

2. May a physician or hospital "fax" a patient's medical information to other physicians or to an insurer?
 - ✓ Yes. The Privacy Rules do not prohibit a "covered entity" from faxing protected health information.
 - ✓ But, the minimum necessary rule may apply and adequate safeguards (technical, administrative, and physical) must be in place.
3. May a physician discuss information about a patient's treatment with other physicians using e-mail?
 - ✓ Yes. Physicians may use any method of communication — including e-mail, oral conversations, written letters, or other methods (including sending facsimiles) — so long as the physician uses "reasonable and appropriate safeguards" to protect the communication.

37




Scenarios (CONT.)

4. What about a Solo Practice — Basically, it's Just one doctor. Does the one doctor still Have to Comply with the Privacy Rule?
 - ✓ Yes, the Privacy Rule applies to *all* health care providers — from those in large multi-hospital systems to individual solo practitioners.
 - ✓ The administrative requirements of the Privacy Rule are "scalable," meaning that a covered entity must take "reasonable" steps to meet the requirements according to its size and type of activities.
 - ✓ In other words, the administrative burden on a psychologist who is a solo practitioner will be far less than that imposed on a hospital. For example, a hospital may be required to create a full-time staff position to serve as a privacy officer, while a psychologist in a solo practice may identify him or herself as the "privacy officer."


<http://www.apapracticecentral.org/business/hipaa/faq.aspx>

38



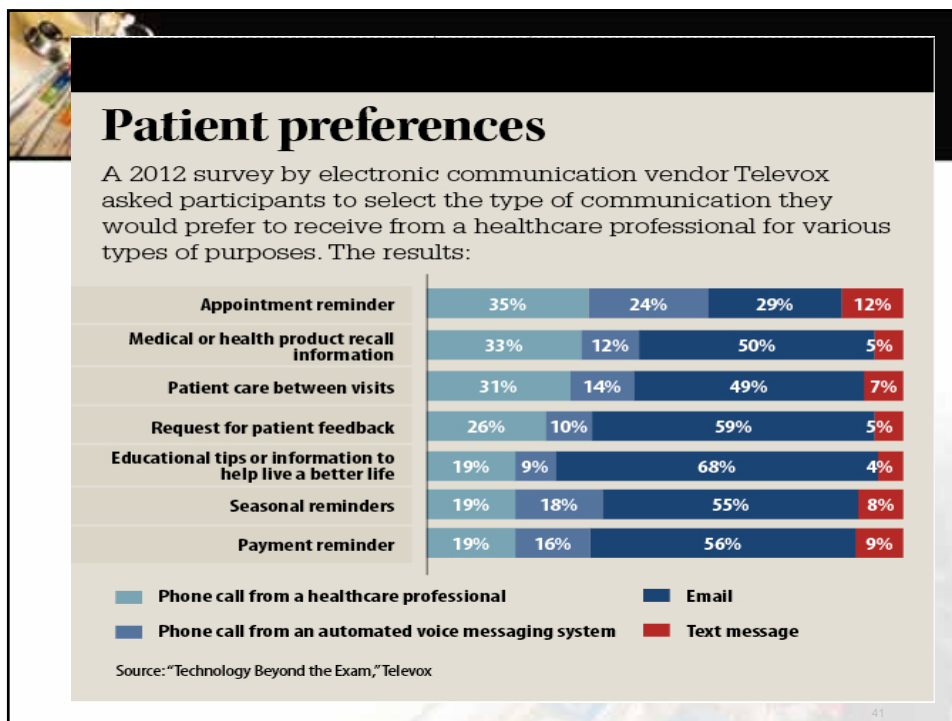
Scenarios (CONT.)

5. If a patient's family members call to ask how their loved one is doing, what can the treating physician disclose?
 - ✓ It depends. The Privacy Rules allow a physician to share a patient's information with the patient's family member or friend so long as the information is limited to information directly relevant to that person's involvement in the patient's care.
 - ✓ A physician should not share a patient's information with the patient's family or friends if the patient has asked the physician not to or if the physician believes, in his/her professional judgment, a disclosure would be inappropriate.



Scenarios (CONT.)

6. May a physician send out appointment-reminder postcards?
 - ✓ Yes. The Privacy Rules allow a physician to communicate with patients, including communications to the patient's home.
 - ✓ However, under HIPAA the patient dictates the means by which communication are to occur.
7. Leave messages on answering machines?
 - ✓ Yes; best to get patient's consent.
8. Verify appointment times with the patient's spouse or other living companion?
 - ✓ Yes.
 - ✓ But, if a patient has requested that the physician communicate in a confidential manner, the physician must accommodate the request if it is reasonable.



Scenarios (CONT.)


9. May a physician use a sign-in sheet?

- ✓ Yes. To the extent these activities result in other people learning a patient's name or other information, the disclosure would be considered "incidental" to the physician's treatment of the patient, and therefore acceptable under HIPAA.

10. Call out names in the waiting area?

- ✓ Yes.

<https://www.hhs.gov/hipaa/for-professionals/faq/199/may-health-care-providers-use-sign-in-sheets/index.html>



Scenarios (CONT.)

11. Place charts outside the patient's room while the patient is waiting to see the physician?
 - ✓ Yes, but the physician should take precautions such as turning the front of the chart towards the wall so others do not have the opportunity to read the front page while walking past the room.
12. May a sales representative sit in on a patient's exam or treatment?
 - ✓ No - unless the physician has obtained a valid authorization from the patient to share the information for these purposes. A sales representative may sit in on a patient's exam or treatment only if the patient has signed a valid authorization expressly allowing the sales representative to do so. The physician should provide the patient with sufficient opportunity to read the authorization form and ask questions before the patient decides whether to provide permission.



Conclusion— Best Practices

1. Have a clear policy in all units dealing w/ PHI (tie in w/ e-mail and social media policies).
2. Have a privacy officer.
3. Train all employees w/ access to PHI on security and privacy rules.
4. Have an accessible and clear violation reporting mechanism w/ a non-retaliation provision.
5. Vigorously enforce all HIPAA rules.
6. Establish, monitor and enforce BA agreements.
7. Have proper notices for all new patients and have it on your web page.
8. Have proper consent /authorization forms.
9. Be clear on how you will communicate with each patient.
10. Have your IT systems audited to ensure that proper security protocols are in place.

