HIPAA

Everyone’s Right to Privacy

OMNISURE
Risk Management Consulting

This program is made possible by

Today we will…

- Review the elements of HIPAA
- Understand who is a “covered entity”
- Take a look at who is fined, and why
- Take a look at actual cases of HIPAA violations
- Discuss steps to be in compliance with HIPAA

OMNISURE
Risk Management Consulting

HIPAA: Health Insurance Portability and Accountability Act

- HIPAA is a National law that establishes standards for the protection of certain health information.
- It has been in effect since 1996.
- Updated in 2013 to cover Electronic Medical Records.
- Impacts any agency or individual who transmits health information in an electronic format.
  - Prescriptions
  - Orders
  - Insurance Billing
  - Records
  - Photos
  - Notes

HIPAA: Covered Entities

Entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

- Physicians
- Therapists
- Clinics
- Dentists
- Psychiatrists
- Nursing Homes
- Assisted Living Facilities
- Mental Health
- Home Health

HIPAA Enforcement

- The **Office of Civil Rights** is responsible for monitoring and enforcing HIPAA regulations.
- The Office of Civil Rights can inspect facility documents, policies, procedures, reports and training records to make sure HIPAA is being properly implemented.
- The Office of Civil Rights can place large monetary fines against facilities when a health care facility violates HIPAA.

Office of Civil Rights Fines

The General Hospital Corporation and Massachusetts General Physicians Organization Inc. (Mass General) has agreed to pay the U.S. government $1 million to settle what the feds are calling "potential violations of the HIPAA Privacy Rule," according to a statement issued by the U.S. Department of Health and Human Services. The case involves patient information that an employee left on the subway.

Office of Civil Rights Fines

2016:

Advocate Health Care (Downers Grove, Ill.): $5.55 million. HIPAA payment involving one entity, Advocate agreed to pay $5.55 million to HHS' Office for Civil Rights to settle claims that it violated HIPAA.

In 2013, the OCR launched an investigation after Advocate submitted three different data breach reports on behalf of its subsidiary, Advocate Medical Group. In total, the breaches comprised the ePHI of 4 million individuals and included their names, demographic information, addresses, credit card numbers, dates of birth, clinical information and health insurance information.

Office of Civil Rights Fines

University of Mississippi Medical Center (Jackson): $2.75 million. The medical center agreed to pay $2.75 million and adopt a corrective action plan to resolve HIPAA violations concerning a stolen laptop that breached the information of approximately 10,000 individuals.

OCR launched an investigation into UMMC in March 2013 after the health system reported a password-protected laptop was missing from the Medical Intensive Care Unit. UMMC's internal investigation suggested a visitor who had previously inquired about borrowing one of the laptops had stolen it.

Increased in HIPAA violation investigations:

HHS Reports:

- OCR has investigated and resolved over 25,167 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates.
- To date, OCR has settled 52 cases resulting in a total dollar amount of $72,929,182.00.
- In another 11,256 cases, investigations found no violation had occurred.
- In 21,247 cases, OCR has intervened early and provided technical assistance to HIPAA covered entities, their business associates, and individuals exercising their rights under the Privacy Rule, without the need for an investigation.

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

HIPAA and Social Media

- A nursing assistant made a video of an incontinent resident's bowel movement on the bathroom floor and shared it on Snapchat with two staff members. The resident's leg was visible in the video. One of the staff members asked the assistant who was in the video and the assistant identified the resident by first name.
- Police arrested a nursing aide for allegedly posting photos showing a sleeping elderly woman with her hand covered in what looked like feces. Another photo shows someone touching the woman's nose with a tissue or feather, apparently with the hope that the woman would touch her face with her dirty hand. A third photo shows the woman touching her face with her fingers with the brown matter on them.

OMNISURE
Risk Management Consulting

HIPAA and Social Media

The 26-year-old nursing assistant, convicted of invading personal privacy. She was accused of taking graphic pictures of patients using bed pans at the Regency Pacific Nursing & Rehab Center near Portland, Oregon and posting them on Facebook. The pictures date back to April of last year.

She spent eight days in jail, and must write a thousand-word apology to a patient that the judge says should be an insightful look at why the defendant did what she did. If it doesn't meet that standard, the judge ruled she could be charged with violating her probation. And she's forbidden from working in a job that would require her to work with children or the elderly for two years.

OMNISURE
Risk Management Consulting

DOJ US Attorney

- July 2013: Hospital Employee and Accomplice Sentenced to 40 months for Tax Refund Fraud Using Stolen Patient Information.

- According to documents filed in court, from January through June 2012, a woman possessed and used stolen personal identifying information of others to file federal income tax returns claiming tax refunds to which she was not entitled. She was employed as a scheduler at the Boca Raton Regional Hospital in Boca Raton, Florida. As a scheduler, she had access to personal identification information of Boca Raton Regional Hospital patients, including their names, dates of birth, social security numbers, and other sensitive personal information. In total, at least 57 fraudulent tax returns were filed with the IRS, requesting $306,720 in federal tax refunds.

http://www.justice.gov/usao/fls/PressReleases/130729-02.html

Office of Civil Rights

- Patients have the right to file a complaint with the Office of Civil Rights.
- Patients are not required to complain to the physician prior to contacting the Office of Civil Rights.
- Complaints filed with the government may result in a compliance review.
- Practices will be required to comply with all requests from agents conducting the review.

HIPAA

OMNISURE
Risk Management Consulting

What do criminals do with stolen PHI?

- PHI can be used to obtain products and medications which can be sold on the black market, although the data can also be used to submit false tax returns, obtain tax refunds and make bogus insurance claims.
- Ransomware, holding information for ransom.
- The healthcare industry is becoming a much riper target because of the ability to sell large batches of personal data for profit.

What do criminals do with stolen PHI?

- The data for sale includes names, birth dates, policy numbers, diagnosis codes and billing information. Fraudsters use this data to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers, according to experts who have investigated cyber attacks on healthcare organizations.

- Some Home Health operators file fake Medicare claims using stolen identities.

Stolen Identities

- **Brooklyn Pharmacy Owner/Operator Charged With Defrauding Medicare and Medicaid Programs of Approximately $9 Million**
- KUMAR – while owning one pharmacy herself and operating a second pharmacy, both located in Brooklyn, New York – conducted a multimillion-dollar scheme to defraud Medicare and Medicaid programs by fraudulently seeking reimbursements for prescription drugs. Specifically, KUMAR engaged in a scheme to obtain prescriptions for medications, for which her pharmacies billed and received reimbursement from Medicare and Medicaid, but which she did not actually dispense to customers. From in or about January 2015 through in or about December 2016, KUMAR obtained approximately $9 million in reimbursements from Medicare and Medicaid for prescription drugs that her pharmacies never actually dispensed.

https://www.justice.gov/usao-sdny/pr/brooklyn-pharmacy-owneroperator-charged-defrauding-medicare-and-medicaid-programs

Stolen Identities

- **Participant in $100 Million Medicare Fraud Sentenced in Manhattan Federal Court to 135 Months In Prison**
- From 2006 through 2010, BAGHOUMIAN and others participated in a nationwide Medicare scam that fraudulently billed Medicare for over $100 million. As part of the conspiracy, the defendant created dozens of “phantom clinic” health care providers that existed only on paper, had no doctors, and treated no patients. The scheme involved at least 118 fraudulent Medicare providers that were located in approximately 25 states, and that submitted fraudulent bills for at least approximately $100 million, and received approximately $35.7 million in reimbursements from Medicare.

https://www.justice.gov/usao-sdny/pr/participant-100-million-medicare-fraud-sentenced-manhattan-federal-court-135-months

Common Causes

1. Impermissible uses and disclosures of protected health information;
2. Lack of safeguards of protected health information;
3. Lack of patient access to their protected health information;
4. Use or disclosure of more than the minimum necessary protected health information; and
5. Lack of administrative safeguards of electronic protected health information.

Impermissible Use of Protected Health Information

- Social uses, posting identifiable information.
- Providing data to researchers.
- Providing information to companies to permit marketing to patients.
- Advertising.
- Social Media.
- Print Media (TV, Movie, News reports)
- Website advertisements.

Lack of Safeguards

- Laptops that do not require password access.
- Thumb Drives that are unencrypted.
- Retention and disposal of outdated patient files.
- Destruction methods that fail to protect PHI.
- Access to computers by hackers.

Lack of patient access to their protected health information

- Patients have the right to their personal information.
- The entity cannot ask the purpose of the access by the patient.
- Electronic records must be printed and provided to the patient in a reasonable amount of time (30 days).
- Entities may charge a reasonable fee for copying.
- Entities are hesitant to reveal specific entries that may be contentious.

Use or disclosure of more than the minimum necessary protected health information

- Individuals working in medical settings are restricted from viewing records unrelated to their job, and job assignment.
- Job assignments restrict access to specific data: the X-ray Department staff do not need to access psychiatrist notes.
- Minimum Necessary is the restriction that the professional access the minimum necessary information to enable them to conduct a competent service.

Providing Data to Researchers

- Research data is available through access to ICD 10 codes in “scrubbed” data.
- When the entity provides information to researchers that includes names, social security numbers, ages, or any identifiable information, it is a breach.
- Researchers cannot reveal data gathered for the purpose of research if it contains identifiable information.

Business Associates

- Business Associates are individuals who work with the physician, hospitals, nursing homes, Home Health and staff to provide additional services.

- When Business Associates have contact with protected health information, there must be a properly executed Business Associates Agreement.

- If the Business Associate has protected health information, at the termination of the arrangement the Business Associate must return all patient information to the practice where feasible.

What Information is Protected?

Individually Identifiable Health Information:

The Privacy Rule protects all *"individually identifiable health information"*. The Privacy Rule calls this information **"protected health information".**

ALL information pertaining to the health conditions of patients is protected health information and cannot be shared with anyone who does not have a "need to know" to be able to provide care.

What Information is Protected?

- Protected information includes:
  - the individual's past, present or future physical or mental health or condition,
  - the provision of health care provided to the individual, or
  - the past, present, or future payment for the provision of health care to the individual.

•Individually identifiable health information includes many common identifiers **(e.g., name, address, birth date, Social Security Number, diagnosis).**

Patient's Rights under HIPAA

Patients have the right to:

- Review their own medical information
- Ask that the information in the record be corrected.
- Know who has reviewed the record.
- Know how health information has been used.
- Restrict portions of the record from being shared with specific individuals or Business Associates.
- Ask for the Covered Entity to contact you in places other than your own home.

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf

What Information is Protected?

Patients can request copies of their medical records under certain circumstances:

- It is possible to charge reasonable cost-base fees for copying the file.
- A summary of difficult to understand information is allowable.
- A copy of an authorization is allowed, as long as all elements are included.
- An authorization can be revoked as long as no action had already been taken.

Changing the Medical Record

- Patients have the right to ask for corrections to be placed in their own medical record.
- Simply because a request is made, the physician is required to review the chart for content and accuracy. If the physician discovers information that should be changed, proper documentation may be entered into the record at the patient's request.

- If the request is made by the patient, the physician should respond within 60 days.

Minimum Necessary Test

"*use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request*"

"a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose"

When talking about patient, be careful to use only the information necessary to provide full and proper care. Information that is not part of the patient's care, is information that is not necessary to know. Caring for a patient means protecting their privacy too.

Here is a tidbit fit for party talk…did you know?

- UCLA hospitals to pay $865,500 for breaches of celebrities' privacy:
  - UCLA Health System has agreed to pay $865,500 as part of a settlement with federal regulators announced after two celebrity patients alleged that hospital employees broke the law and reviewed their medical records without authorization.
  - Federal and hospital officials declined to identify the celebrities involved. The complaints cover 2005 to 2009, a time during which hospital employees were repeatedly caught and fired for peeping at the medical records of dozens of celebrities, including Britney Spears, Farrah Fawcett and First Lady of California Maria Shriver.

http://articles.latimes.com/2011/jul/08/local/la-me-celebrity-snooping-20110708

Minimum Necessary Test

When professionals need to provide services to patients, they are only entitled to read information that is necessary to care for the patient.

Does a Podiatrist need to read the notes written by the Psychologist?

No, the Podiatrist only needs information directly related to the care of the patient's feet, e.g., diagnosis, circulation problems and medications because a Podiatrist needs to know about the risk of injuries and infections of the feet, not mental health treatments.

Minimum Necessary Test

When professionals need to provide services to patients, they are only entitled to read only the information that is necessary to care for the patient.

Does the Dietician need to read the History of the patient?

Yes. The Dietician needs information that is important to prescribe the proper nutrition for the patient based on diagnoses, and disorders that may impact the patient's weight and over all health.

HIPAA: Your Responsibilities

Never reveal any information about a patient to anyone who does not have a need to know.

OMNISURE
Risk Management Consulting

Disclosures or Breach?

“A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:”

Disclosure or Breach?

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Breach Notifications

Individual Notice: Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. In no case later than 60 days following the discovery of a breach.

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

Breach Notifications

Media Notice: Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.

Breach Notifications

Notice to the Secretary: If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis.

Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

HIPAA: Your Responsibilities

Never post any information on any computer, social network, cell phone or any device about your workplace, patients, or specifics about treatments provided.

HIPAA: Your Responsibilities

Know where you are when you are talking; strangers who hear conversations are not part of the care team.

Never speak in a public place about patients and what care they need.

HIPAA: Outside of Work

NEVER

Never tell anyone about patients, their diagnoses or their names.

Never post any information about patients on Social Networks such as Twitter or Facebook.

Never take work out of the facility that has patient information on it.

Never have phone conversations that uses the patient's name in an area than can be overheard by others.

Never talk about a patient in a public place by stating their name (for example over lunch in a restaurant).

Penalties

Penalty Amount

Depending on the severity of the violation between $100 and $50,000.

Most commonly fines are $5,000 per occurrence.

Fines can run into the millions.

Staff may be fired for disclosing confidential information.

Inspectors can review the facility's practices and fine the facility if they cannot prove that all staff comply with HIPAA rules.

HIPAA DOs

- Test competencies.
- Create a “test” to determine if knowledge is applied.
- Track computer data to determine employee’s access to files.
- Create “sign-out” forms for access to hard copy records.
- Design a HIPAA Disclosure Log for each record.
- “Crawl” through Facebook pages of employees to determine if violations occur.
- Prohibit computers from leaving the workplace unless protected by passwords.

OMNISURE
Risk Management Consulting

HIPAA TO DOs

- Use only encrypted thumb drives.
- Prohibit physicians and staff from texting orders and test results.
- Inform all patients regarding their rights in language that is easy to understand.
- Conduct a HIPAA Audit. Tools may be found at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry	Req-uired/ Address-able
Privacy	§164.502(a)(5)(i)	Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes	§ 164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a	Does the health plan use or disclose for underwriting purposes, "Genetic Information" as defined at § 160.103, including family history? Inquire of management.	

OMNISURE
Risk Management Consulting

CONCLUSION

- Know your Privacy Policy.
- Know how to protect the privacy of all patients.
- Know how to report privacy violations to your managers.
- Know who can be informed about patients.
- Protect the privacy of every patient, whether or not they are on your unit.
- Be the employee who stands out as the professional who knows how to comply with HIPAA.

Resources

HHS http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

Summary of Privacy Act

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

HITECH

http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

OMNISURE
Risk Management Consulting