HIPAA in the Context of COVID-19

October 15, 2020

This presentation has been prepared by Segal for educational purposes and is not complete without remarks provided at the meeting. Please remember that the presentation is for informational purposes only and should not be construed as legal advice. On all issues involving the interpretation or application of laws and regulations, all plan personnel should rely on counsel for legal advice.

Segal

Today's Presenters

Kathy Bakich
Senior Vice President

Lisa Simioni
Senior Consultant

Gisela de San Roman
Senior Consultant

Ashkon Roozbehani
Consultant

HIPAA – More Important Now Than Ever

Today's Workforce is Changing






Zeroing in on the Remote Work Environment

Protections for PHI were developed assuming an old model of control – have they been updated?

Are remote workers being monitored?

Did the employer or plan sponsor send equipment, or are employees relying on their own equipment?

If so, how are they protected?

How is remote equipment being catalogued?

Primary Goals for Today

- Outline key concepts of HIPAA Privacy and Security
- Explain why health information must be kept confidential and only certain people should be allowed to use/disclose it
- Understand what needs to be done to comply with HIPAA
- Identify Common Issues/Threats
- Address confidentiality and HIPAA in the age of COVID-19
- Answer your questions

Let's Refresh

Background on Privacy, Security, and HITECH

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification Provisions, and Compliance Dates:

- Electronic Data Interchange: October 15, 2002
- Privacy: April 14, 2003
- Security: April 20, 2005

The Health Information Technology for Economic and Clinical Health (HITECH) Act, was part of American Recovery and Reinvestment Act of 2009. Compliance dates are rolling:

- Certain provisions were effective “immediately” (February 17, 2009)
- Breach Notification was effective September 23, 2009

HIPAA Privacy and Security Rules

HIPAA Privacy Rule

Protects all types of PHI:

- Electronic
- Written
- Oral

HIPAA Security Rule

- Applies to electronic PHI (ePHI) only
- ePHI = transmitted by electronic media or maintained on electronic media
- Examples:
  - Sent or received via e-mail
  - Stored on computer network
  - Stored on computer (including laptops, netbooks or tablets)
  - Stored on electronic media such as CDs, disks, flash drives, tapes or memory cards (including those in smartphones)

Plan Responsibilities

The most important way to assure HIPAA/HITECH compliance is to do these five things:

1. Conduct periodic risk assessments every two years or when new technology, software or services are acquired,
2. Update policies and procedures, and
3. On-going training
4. Have process in place to detect and report HITECH Breaches
5. Contract with Business Associates, who are also independently responsible for complying with the rules

PHI and Covered Entities

Covered Entities

- Group health plans are “covered entities” and directly regulated by HIPAA
- Employers are not “covered entities” and are not directly regulated by HIPAA
  - Employers may not use information from health plans to make employment decisions (hiring, termination, etc.)

What is "Protected Health Information" or "PHI"?

- Health Information that relates to:
  - Past, present or future physical or mental health or condition of an individual, or
  - The provision of health care to an individual, or
  - Past, present or future payment for the provision of health care to an individual
- Is Individually Identifiable
- Is created, received or maintained by a covered entity (CE)

What Makes Health Information "Individually Identifiable"?

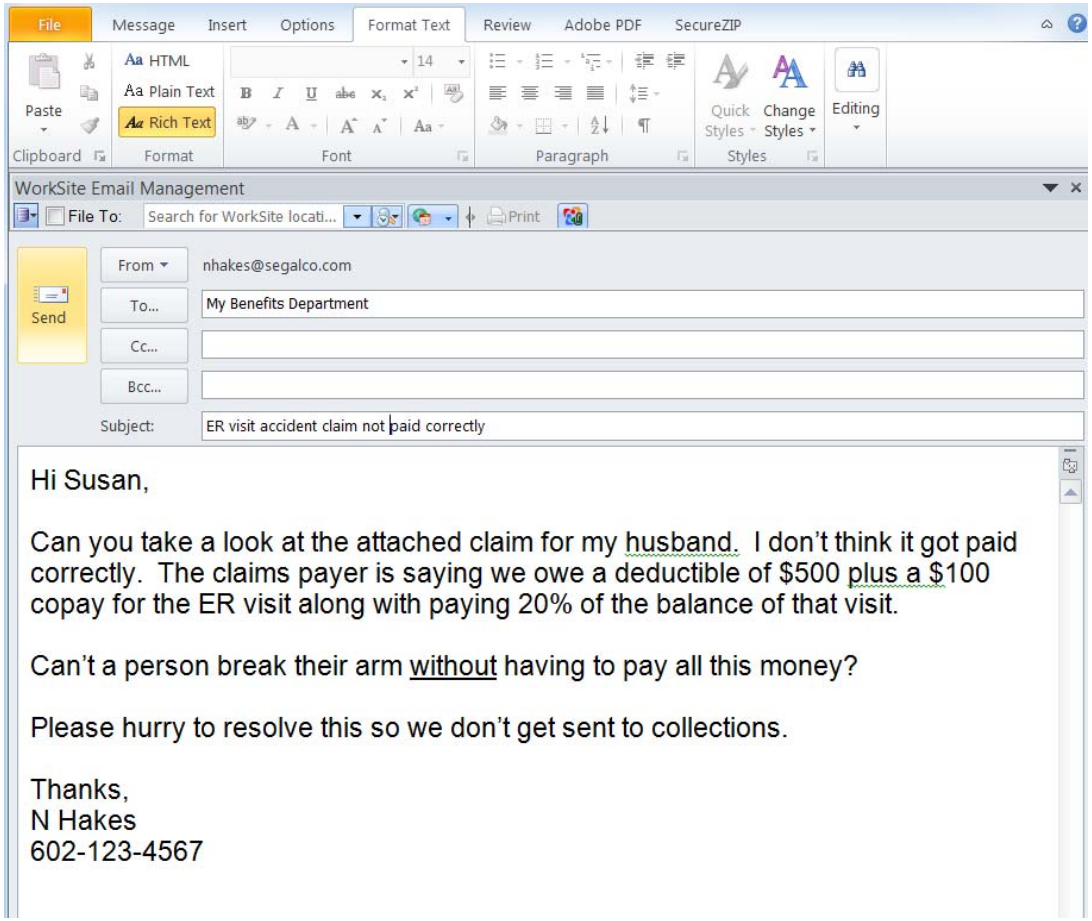
Health information is individually identifiable if it contains any HIPAA identifier

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers

What Makes Health Information "Individually Identifiable"?

8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locations (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned to code the data)
19. Having just ONE of these 18 identifiers is enough to make it individually identifiable

Emails Are Often Full of PHI



Email clearly contains an identifier (the email address of the sender) plus health information in the:

a. subject line,

b. body of email, and

c. in the attachment

Learn to recognize emails containing ePHI

Use and Disclosure of PHI by Group Health Plans

Treatment, Payment, and Health Care Operations

- Designated health plan staff may use or disclose PHI for “payment” or “health care operations” purposes
  - Designated individuals may engage in activities that are necessary to administer the health plans
- Examples of permissible “payment” or “health care operations” activities:
  - Enrollment
  - Eligibility determinations
  - Customer service
  - Claims adjudication and payment
  - Pre-certification and referrals
  - Utilization review
  - Coordination of benefits
  - Wellness programs

Minimum Necessary

The minimum necessary rule is a cornerstone of the Privacy Rule.

It requires plans to use reasonable efforts to:

- Use or disclose only the **minimum amount of PHI necessary** to accomplish the legitimate business purpose
- Request from another covered entity only the minimum necessary PHI

Authorization

Health plan employees (and Business Associates) generally cannot disclose PHI to people outside the entity (plan, fund or organization) or to employees with the entity who are not authorized to use or access PHI without a **signed written Authorization Form** from the individual who is the subject of the PHI

Social Media and Websites

- Website videos and testimonials
- Yelp
- Facebook
- News Media
- NO EXCEPTIONS to the Written Authorization Rule

Medical Surveillance Exception

- HIPAA permits an employer to contract with a health care provider to conduct tests and report test results to the employer
- Providers can disclose PHI to an employer without authorization if:
  - The provider is providing the health care service to the employee at the request of the employer or as a member of the employer's workforce,
  - The service is related to medical surveillance of the workplace or an evaluation of whether the individual has a work-related illness or injury, and
  - The employer has a duty under OSHA or similar state law to keep records on or act on the information.

The Provider must give the individual written notice that the information is to be disclosed to the employer. (The notice can also be posted in a prominent place at the worksite if the service is provided there.)

Business Associates

- The health plan is required to enter into a written Business Associate Agreement with each service provider that uses or discloses PHI
- The health plan will need to take action if it becomes aware of Privacy breaches by any of its BAs (e.g., require BA to mitigate damage of wrongful PHI disclosure)
- Failure to contract with and/or monitor a BA has led to many HIPAA enforcement actions and monetary settlements with HHS

Key Privacy and Security Requirements and Reminders

Administrative Requirements

The Privacy Rule requires the health plans to (partial list):

- Appoint a Privacy Official
- Send a Privacy Notice to participants
- Develop safeguards to protect PHI
- Develop Policies and Procedures on PHI use/disclosure
- Train employees on the Privacy Rule
- Develop sanctions for Privacy Rule violations

The Privacy Notice

- Once HIPAA P&P established, issue Notice of Privacy Practices—one per family
- Notice explains how the health plans will use and disclose PHI and what rights people have under the HIPAA Privacy Rule
- Notice was to be sent to all participants when Privacy Rule originally became effective
  - New participants should also receive a Notice
- Privacy Notice reminders must be provided at least every three years

Training

- HIPAA Privacy Rule requires all the employees who have access to PHI, including Privacy Official, to receive Privacy training (covering Privacy Rule, as well as health plans' Privacy P&Ps)
- The health plans must document that the training has taken place
- All employees should certify, in writing, their participation in any Privacy training
- A new employee may not use or disclose PHI until that employee has been trained

Risk Assessments, Remote Work and COVID-19

Safeguards

- The health plans must have in place appropriate safeguards to protect the privacy of PHI
- The Privacy Rule and Security Rule require the following types of safeguards:
  - Administrative (policies and procedures)
  - Technical (e.g., computer access controls)
  - Physical (e.g., locked file cabinets, secure servers)

How has COVID-19 Changed the Risk Environment?

- Remote workers
- Use of home equipment and cell phones
- Increased reliance on website communications with participants
- Lack of stable internet access
- Security of paper files and documents
- Heightened risk of cyber attacks

Assess Risk for Newly Implemented Technologies

- Remote Access: encrypted, monitored, strongly configured, must match employee access rights
- Laptops and Mobile Devices: encrypted, accounted for, members of the domain (antivirus, DLP, IDS, strong authentication, etc.)
  - To BYOD or not BYOD?
  - Consider a third-party evaluation
- Cloud Migrations: beware of cloud migrations in a hurry
  - Move to an enterprise-level platform
  - Evaluate, enable, and test appropriate security controls
  - Consider a third-party evaluation

The Remote Office

- Dedicated work space
- Asset protection
- Security reminders and refreshers
- Clear and concise policies and procedures for working remotely
- Provide support – technical and otherwise

Breach Notification

HITECH Notification of Breach Rule

General Rule

If security of unsecured PHI is breached, Covered Entity must provide notice without unreasonable delay and within 60 days after discovery of the Breach to impacted individuals, media (in certain instances) and HHS

Breach Notification Requirement

- HIPAA covered entities (i.e., the health plans) must now notify individuals when there's a breach of "unsecured PHI"
  - Applies to all PHI (e.g., oral, paper) not just ePHI
- Also requires notice to HHS and maybe the media
- Business Associate to notify Covered Entity

Unsecured PHI

PHI that is not secured through the use of a technology or methodology specified by the Secretary

Safe harbor to avoid breach notification:

Two exclusive methods to make PHI unusable, unreadable or indecipherable to unauthorized individuals (i.e., to make it secure):

1. **Encryption** (for ePHI in use, at rest and in transmission)
2. **Destruction** (for hardcopy PHI and ePHI)

Risk Assessment

- Type of PHI Disclosed
- Recipient of PHI
- Accessed; Viewed; Re-Identified; Re-Disclosed
- Intent of Recipient
- Steps Taken to Mitigate Risk to PHI

Enforcement

Enhanced Civil Penalties

- Covered entities and business associates may be subject to enhanced civil penalties
- Four-tiered penalty structure based on intent of violation:
  - Under old rule, penalties maxed out a $25,000 per year per standard violated
  - New tiered structure as amended in May 2019 by HHS

Violation Category	Amount of Penalty per Violation	Max Penalty for all Violations of Identical Provision per Year
Did Not Know	$100 – $50,000	$25,000
Reasonable Cause	$1,000 – $50,000	$100,000
Willful Neglect, Timely Corrected	$10,000 – $50,000	$250,000
Willful Neglect, Not Timely Corrected	$50,000	$1.5 million

Selected HHS Enforcement Actions

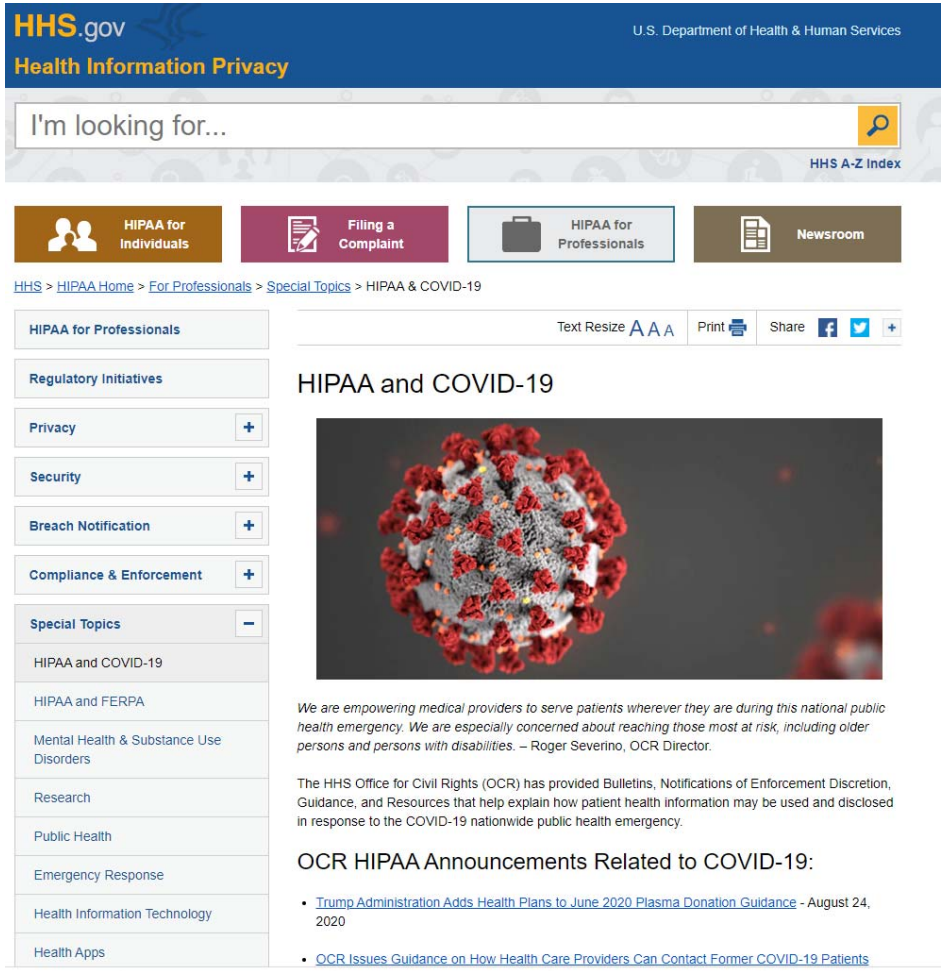
Entity	Incident	Result
Lifespan (July 2020)	Failure to Encrypt Laptop	$1,040,000 and corrective action plan
Metropolitan Community Health Services d/b/a Agape Health Services (July 2020)	Impermissible disclosure to an unknown Email account	$25,000 and corrective action plan
University of Rochester Medical Center (November 2019)	Failure to Encrypt Mobile Device	$3M and corrective action plan
Elite Dental Associates (October 2019)	Improper disclosures (social media)	$10,000 and corrective action plan

Selected HHS Enforcement Actions

Entity	Incident	Result
Medical Informatics Engineering, Inc. (May 2019)	Failure to appropriately identify risks (cyber attack)	$100,000 and corrective action plan
Pagosa Springs Medical Center (December 2018)	Failure to terminate former employee's access to ePHI	$111,400 and corrective action plan
Advanced Care Hospitalists PL (December 2018)	Failure to enter into a business associate agreement	$500,000 and corrective action plan
Firefax, Inc. (February 2018)	Improper disposal of PHI	$100,000 and corrective action plan

COVID-19 and HIPAA Privacy and Security

New HIPAA and COVID-19 HHS Web Page



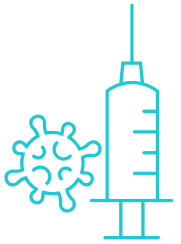
https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html

Enforcement Discretion

HHS will not penalize health care providers and health plans in light of the COVID-19 Public Health Emergency with respect to:

Providing telehealth services, even if the platform does not meet strict HIPAA security standards

Working with first responders to protect public health



Providing assistance to plan participants who want to donate plasma for COVID-19 research and treatment

Some Rules Stay in Force

HHS has announced several areas of increased enforcement

Thank You!

Kathy Bakich
KBakich@segalco.com

Lisa Simioni
LSimioni@segalco.com

Gisela de San Roman
GDeSanRoman@segalco.com

Ashkon Roozbehani
ARoozbehani@segalco.com