HIPAA Privacy, Security & Compliance

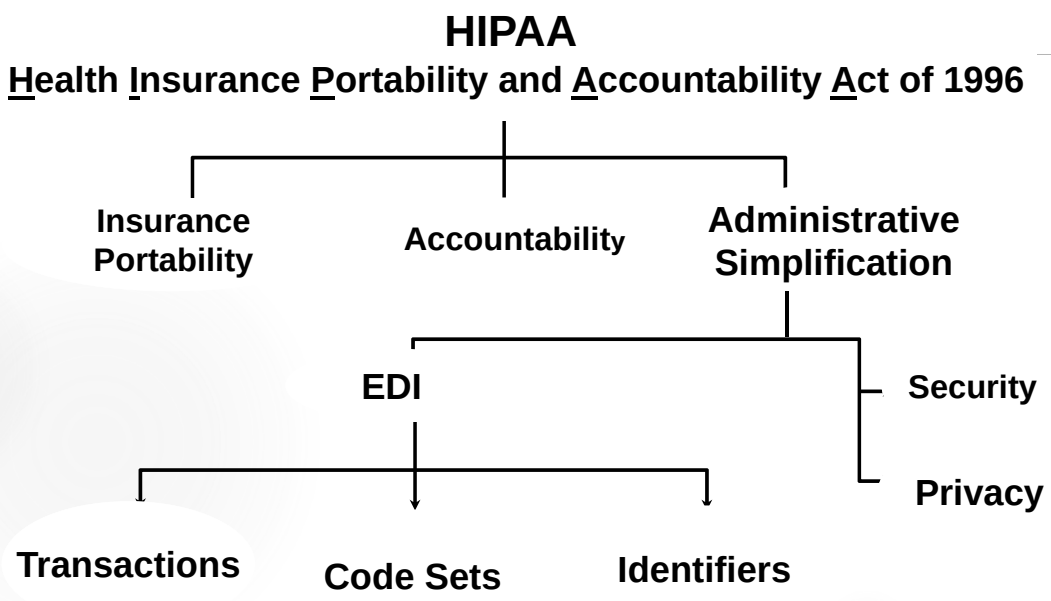
DARRELL W. CONTRERAS, ESQ., LHRM, CHC, CHRC, CHPC
CHIEF COMPLIANCE OFFICER
MILLENNIUM HEALTH
DARRELL@JDHCP.COM (863) 797-9917

SHAWN Y. DEGROOT, CHC-F, CCEP, CHRC, CHPC
PRESIDENT, COMPLIANCE VITALS
SHAWN@COMPLIANCEVITALS.COM (605-430-9291)

HIPAA –
Health Insurance Portability and Accountability Act

- HIPAA = Patient Privacy
- HIPPA =

Female Hippopotamus



Enforcement

- Office for Civil Rights (OCR) – Privacy and Security Civil complaints
  - Entity must allow OCR access to facilities, books, records, accounts, and other sources of information
- Centers for Medicare and Medicaid Services (CMS) – Transactions and code sets
- Department of Justice (DOJ) – Privacy Criminal complaints

4

HIPAA Privacy Rule

5

HIPAA – General Rule (164.502)

A **covered entity** may not **use or disclose protected health information**, except as **permitted** or **required**

6

Covered Entities (160.103)

- **Health Plans**: A plan that provides or pays the cost of medical care. Includes Medicaid, Medicare and self-funded plans. Does NOT include health plans with less than 50 participants administered by the employer.
- **Providers**: A provider of medical or health services such as SNFs, home health, hospitals, physician clinics, etc. that transmits any health information in electronic form.
- **Clearinghouses**: Process health information from a non-standard content into standard data elements or to a standard transaction. Such as billing services, health information systems, etc. NOT third party administrators.

7

HIPAA – General Rule (164.502)

A covered entity may not use or disclose protected health information, except as permitted or required

8

Protected Health Information (160.103)

- 2 Part Test:
  1. Health Information?
  2. Does it reasonably identify the individual?

9

HIPAA – General Rule (164.502)

A covered entity may not use or disclose protected health information, except as permitted or required

10

"…Except as permitted or required."

1. Uses and Disclosures for Payment, Treatment and Healthcare Operations (164.506)
2. Required disclosures (164.502(a))
3. Uses and Disclosures with an Authorization (164.508)
4. Uses and Disclosures with an opportunity to object (164.510)
5. Uses and Disclosures for which an authorization or an opportunity to object is not required (164.512)

HIPAA Security Rule

12

Security versus Privacy

- Privacy rule identifies **what** is to be protected and outlines the individual's rights to control access to their PHI
- The security rule defines **how** to protect PHI in electronic form
  - The security rule only applies to PHI maintained or transmitted in electronic form, called ePHI

13

Security Rule - Breakdown

- Three safeguards broken down into 18 standards:
  - Administrative
  - Physical
  - Technical
- 42 Implementation specifications
  - 20 Required
  - 22 Addressable

14

Intent of the Security Rule

- Intended to be technology neutral
- Intended to be scalable.
- Intended to protect the confidentiality, integrity and availability of ePHI
  - **C**onfidentiality – ensures that only those individuals who are supposed to access ePHI do
  - **I**ntegrity – ensuring that the ePHI input today is the ePHI that is retrieved tomorrow, next week, next year, etc.
  - **A**vailability – ensuring that ePHI is available to those who need it when they need it.

15

Is this a HIPAA violation?

A Covered Entity sends an unsecured email containing PHI to another Covered Entity.

- Is this a HIPAA violation?

What if the Covered Entity sent the unsecured email containing PHI to someone who should not have received it?

- Is this a HIPAA violation?

16

Breach Notification

17

Breach Notification Requirements
New for the Omnibus Rule

- To have a “reportable breach” there must be:
  1. A privacy breach
  2. Unsecured PHI

  Presumptive reportable breach unless there is a “Low probability of compromise.”

18

Breach Notification Requirements

1. All breaches require written notification.

2. >500 in a single state or jurisdiction: Media notification.

3. Report breaches to DHHS 60 days after year end
   - ▶500 or more: Immediate notification

19

Civil Monetary Penalties Changes From ARRA

Violation Standard	Minimum Penalty (per violation)	Maximum Penalty (per violation)
Not known by the entity and could not have been discovered with reasonable diligence	$100	$50,000
Reasonable cause, but not from willful neglect	$1,000	$50,000
Willful neglect, but corrected within 30 days of discovery	$10,000	$50,000
Willful neglect and not corrected within 30 days	$50,000	$50,000

20

- Penalty cap = $1,500,000

Penalty Example

A Covered Entity sends an unsecured email containing PHI of 1000 patients from one facility to someone who should not have received it.

1. How many violations?
2. How many patients?
3. What level of prevention occurred?
4. Over what period did it occur?

21

Focus on Phishing

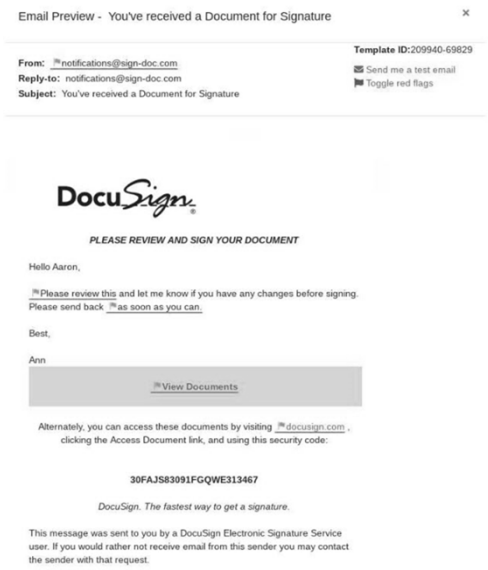
22

Anthem OCR Settlement

- $16M Settlement
- 79 million people's records in <2 months
- Resulted from a phishing email
- At least one employee responded

23

Phishing


Email Preview - You've received a Document for Signature

From: notifications@sign-doc.com
Reply-to: notifications@sign-doc.com
Subject: You've received a Document for Signature

Template ID:209940-69829
Send me a test email
Toggle red flags

DocuSign

PLEASE REVIEW AND SIGN YOUR DOCUMENT

Hello Aaron,

Please review this and let me know if you have any changes before signing. Please send back as soon as you can.

Best,

Ann

View Documents

Alternately, you can access these documents by visiting docusign.com , clicking the Access Document link, and using this security code:

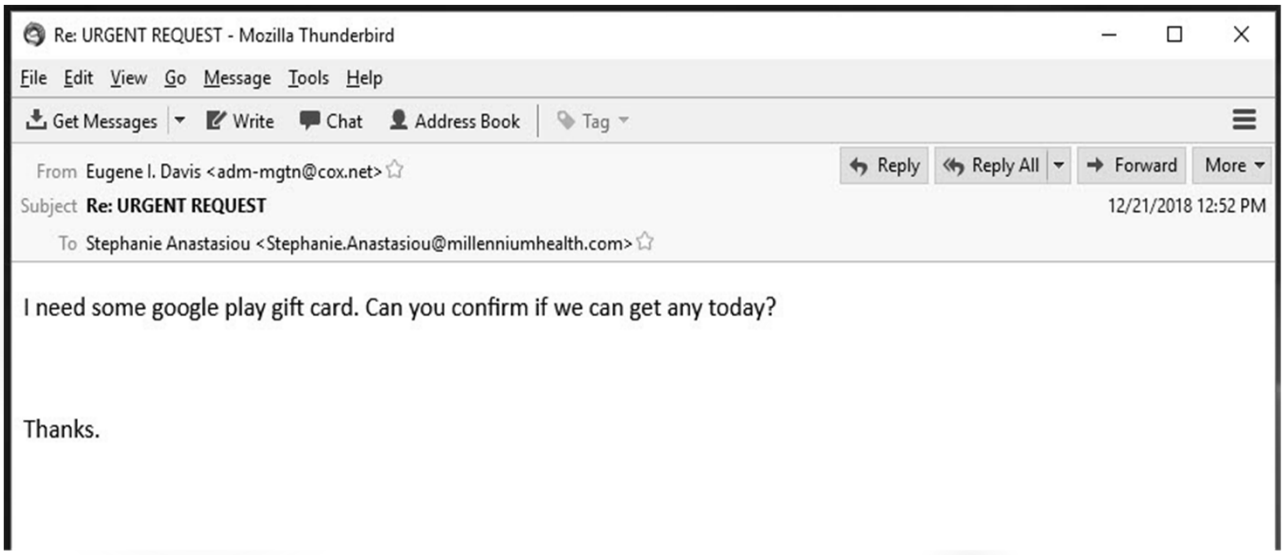
30FAJS83091FGQWE313467

DocuSign. The fastest way to get a signature.

This message was sent to you by a DocuSign Electronic Signature Service user. If you would rather not receive email from this sender you may contact the sender with that request.

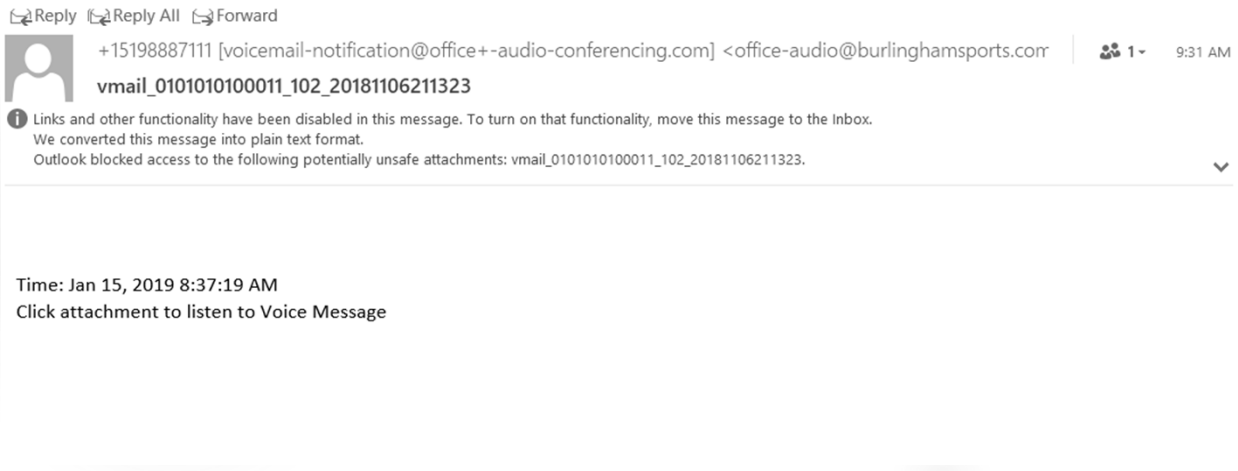
24

Phishing



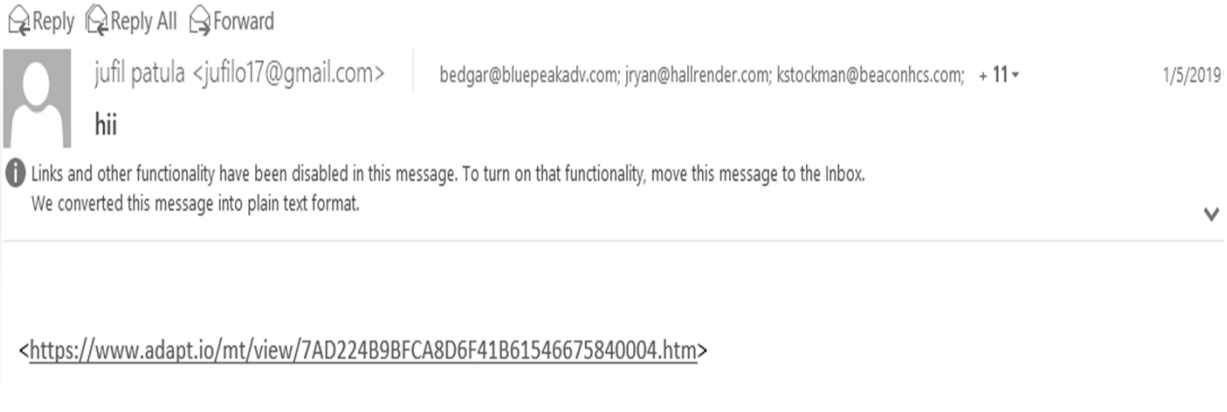
Board Responsibility

- Awareness and Knowledge



Board Responsibility

- Awareness and Knowledge



Board Responsibility

From: CCO@abchealthsystem.com
To: Jane@abchealthsystem.com
Date: Monday, January 15, 2019 2:00 a.m.
Subject: Report

As you no, I am on vacation and you have handled the matter below.

http://www.Microsoft'.outlook.com

Board Responsibility

29

Board Responsibility

- Risk is defined by the breach
- The Privacy and Security Programs are only a safeguard
- Once the breach occurs, then the structure of the Programs will be questioned

30

Board Notification -

- When does Board notification occur?
  - Breaches of 500 individuals or more
  - Internet posting required
  - DOJ involvement
  - OCR investigation v. letter
  - Lawsuit potential

31

32

Appendix

33

Board Privacy Risk Questions

1. Is there a process for reviewing information leaving the organization to determine whether it is PHI?
2. What is the current status of our Privacy Program
3. What were the results of the last Privacy Risk Assessment?
4. How many Reportable Breaches have we had?
   - What trends have been observed?
5. Have the sources of PHI leaving this organization been identified and what has been done to safeguard them?

34

Board Security Risk Questions

1. Is there a process to terminate access of separated employees and contractors?
   - ▶Has that been tested?
2. What were the results of the last Security risk assessment?
   - ▶Has a plan been developed to address identified risks?

35

Board Security Risk Questions (cont.)

3. Have we identified all the ways that an unauthorized person could get access to our data?
4. What is our level of encryption?
   - ▶Link to PHI leaving the organization
5. What is the current status of our Security Program?

36