HEALTHCARE INFORMATION SECURITY

Tsung-Ting (Tim) Kuo

HOUSEKEEPING

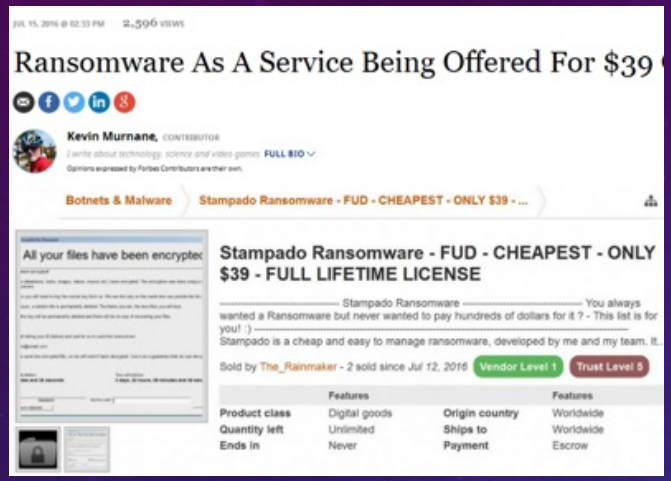
- Assignments are due 11:59pm on Tuesdays

PollEv.com/renawu484

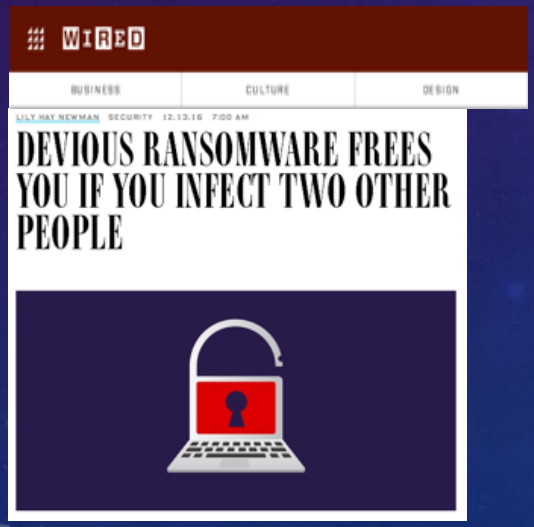
AGENDA

- Information security
  - What it is, How it fits into Healthcare, our Relationships.
  - General Concepts of Information Security
- Challenges specific to healthcare information security
- Defending against the risks
- HIPAA and other laws
- Homework 3

THE BUSINESS OF CYBERSECURITY



Guaranteed ROI, merchant takes 20%.



9 Call Centers, 600 Employees.

Trustwave calculated the ransomware ROI based on the following:

- Costs of a ransomware payload (CTB Locker in this example), infection vector (RIG exploit kit, which was most common), camouflaging services (encryption), and traffic (20,000 visitors) totaled $5,900 per month.
- Earnings for a 30-day campaign, assuming a 10 percent infection rate, a payout rate of 0.5 percent, and a $300 ransom, would total $90,000.
- That's a profit of $84,100 and a ROI of 1,425 percent.

Ransomware: A $Bn Dollar Industry…..

Cyber-extortion losses skyrocket, says FBI - Apr. 15, 2016 - CNN Money
money.cnn.com/**2016**/04/15/technology/**ransomware**-cyber-security/
Apr 15, 2016 - Cyber-criminals collected $209 million in the first three months of **2016** by extorting businesses and institutions to unlock computer servers. At that rate, **ransomware** is on pace to be a $1 billion a year crime this year.

Not to mention Identity Theft…

Health Care Fraud — FBI
https://www.fbi.gov/investigate/white-collar-crime/**health**-care-**fraud**
Health care **fraud** costs the country tens of billions of dollars a year. … **health** care **fraud**, with jurisdiction over both federal and private **insurance** programs. … in the **Healthcare Fraud** Prevention

SOME EXAMPLES…

HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

- On paper for 10 days.
- Paid $17k in Ransom (Original figure was $3.4M
- Increase in Overmedication after the systems came back.

METHODIST HOSPITAL
A Deaconess Network Affiliate

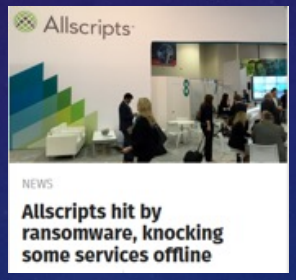
- On paper for 5days.

MedStar Health

- Shut down computers Monday at ten hospitals area
- Turned away patients.
- Days to start recovery.
- Months to fully recover.

HancockHealth

- Paid Ransom – 4 Bitcoin, then $55k
- 4 Day's on downtime procedures.
- Paying the ransom was the quickest recovery.

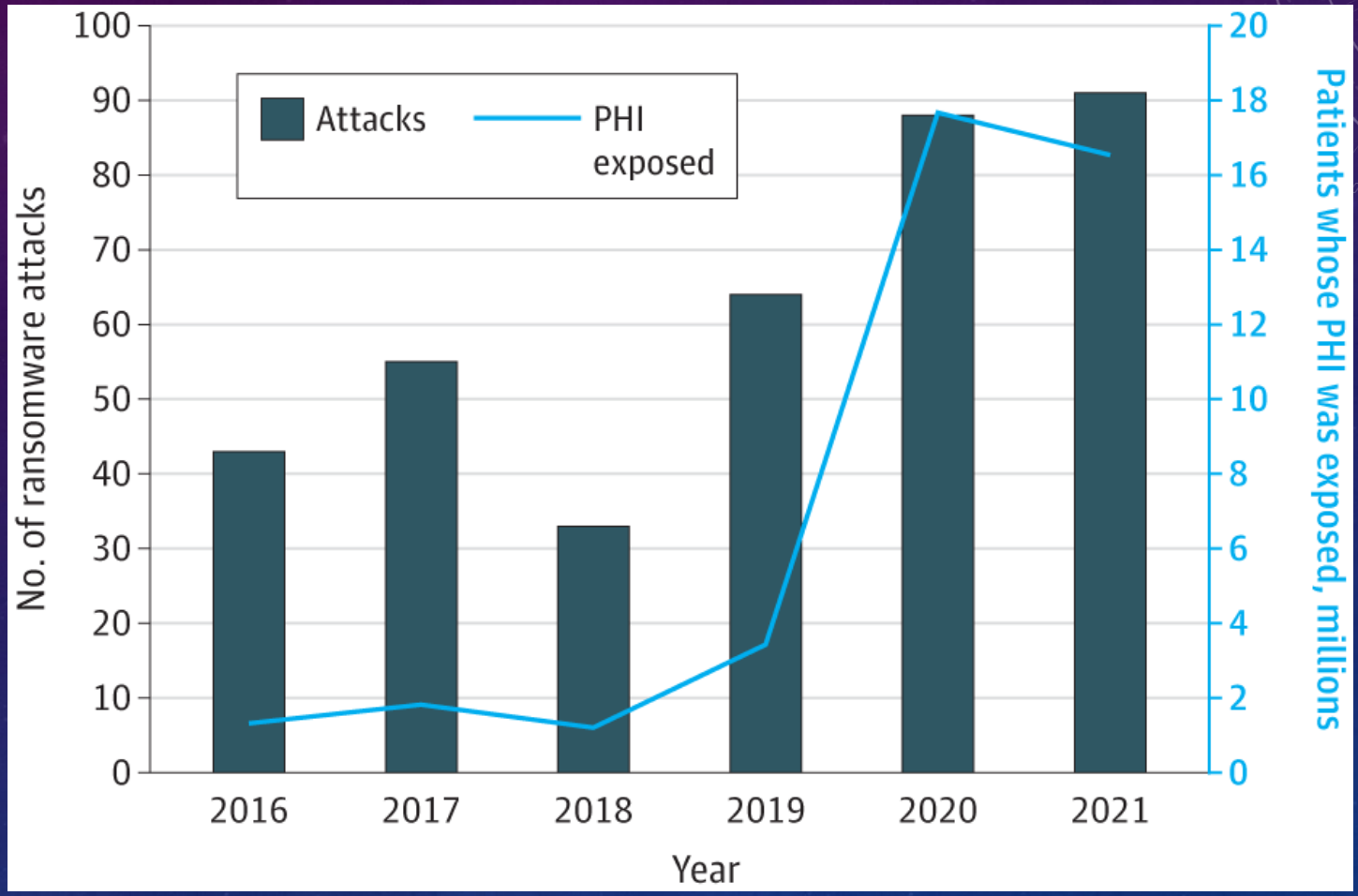


- Customers without EHR for 8 days

Three U.S. Hospitals Hit in String of Ransomware Attacks - NBC News
https://www.nbcnews.com/.../three-u-s-hospitals-hit-string-ransomware-attacks-n5443...
Mar 23, 2016 - Three U.S. hospitals were hit hard this week by "**ransomware**" attacks that ... The servers for **Chino Valley** Medical Center and Desert Valley ...

TRENDS

US Hospitals, Clinics, and Other Health Care Service Delivery Organizations



Neprash HT, McGlave CC, Cross DA, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum.* 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873

DENIAL OF SERVICE ATTACKS…

DDoS Assault on Boston Hospital

Hacktivist Group Suspected of Attacking Children's Hospital

Marianne Kolbasuk McGee (@HealthInfoSec) · April 25, 2014 · 0 Comments

Twitter · Facebook · LinkedIn · Credit Eligible · Get Permission

Boston Children's Hospital

To date, **distributed-denial-of-service** attacks have been relatively rare in the healthcare sector, especially compared with DDoS assaults in the financial sector. But DDoS attacks on Boston Children's Hospital's **website** have security experts debating whether these attacks could become far more common in healthcare.

See Also: Sunset of Windows Server 2008: Migrate with Docker

In a April 25 statement provided to Information Security Media Group, Boston Children's Hospital confirmed a report published by the ***Boston Globe*** that the hospital's public website had been undergoing cyber-attacks for nearly a week, which made some online services, such as patient appointment scheduling, sporadically inaccessible.

WHAT IS INFORMATION SECURITY

Elements of Information Security "CIA"

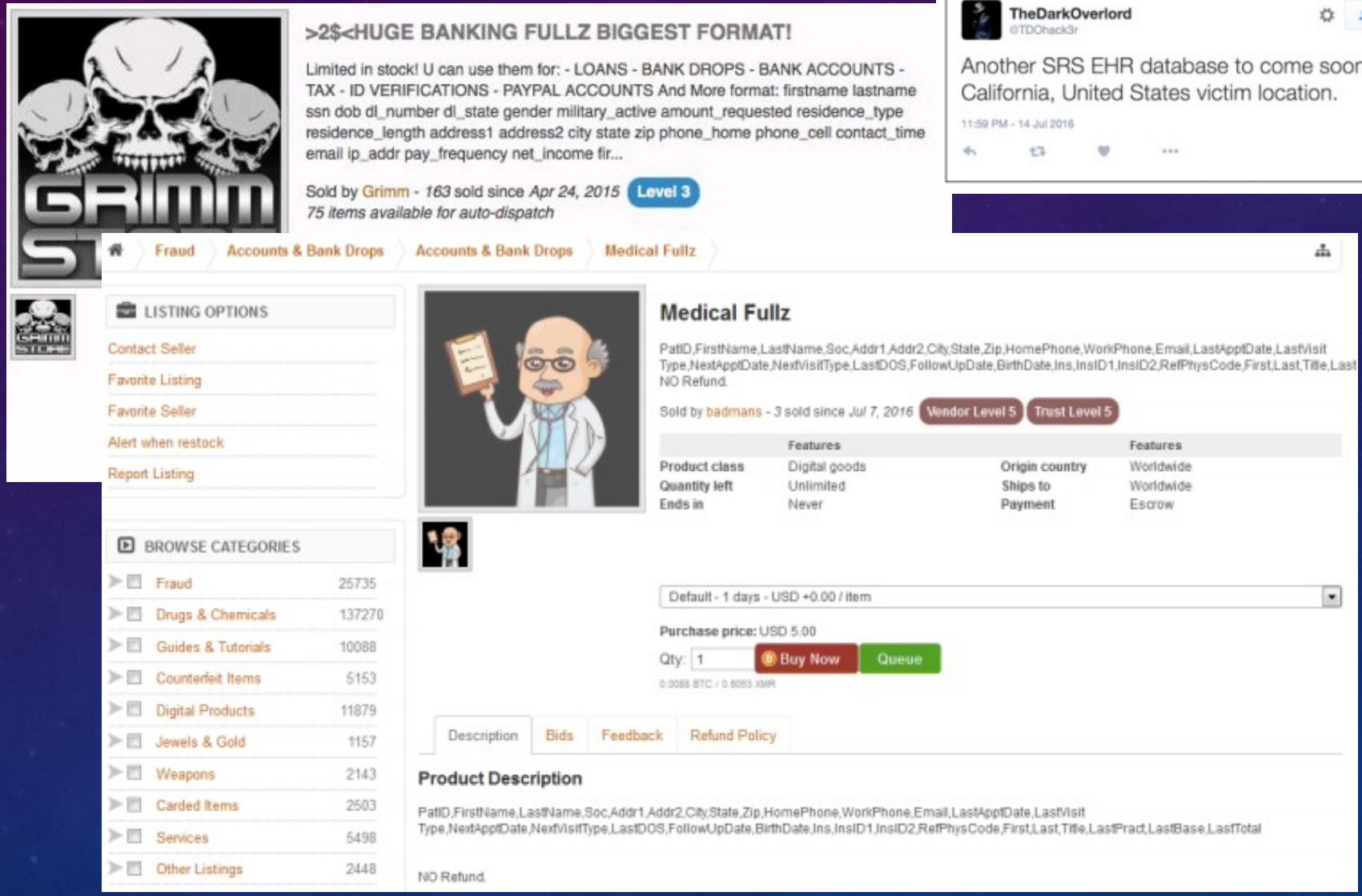
- Confidentiality (authorization)
- Integrity (accuracy)
- Availability (accessibility)

AGENDA

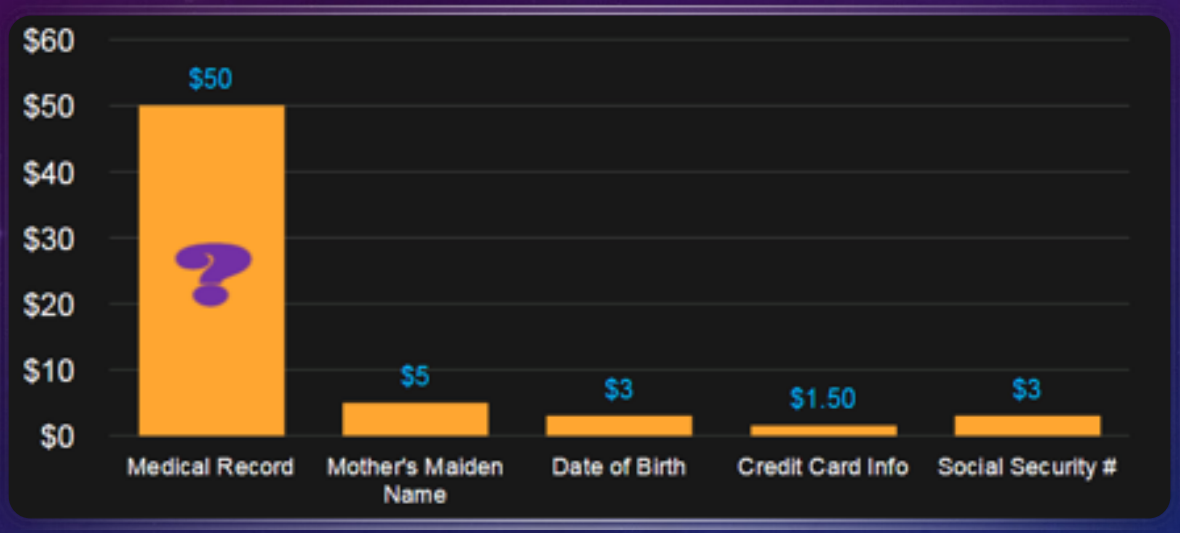
- Information security
  - What it is, How it fits into Healthcare, our Relationships.
  - General Concepts of Information Security
- Challenges specific to healthcare information security
- Defending against the risks
- HIPAA and other laws
- Homework 3

DATA IS A COMMODITY ITEM

- Sold on the Dark Web…



WHAT'S IT WORTH ?



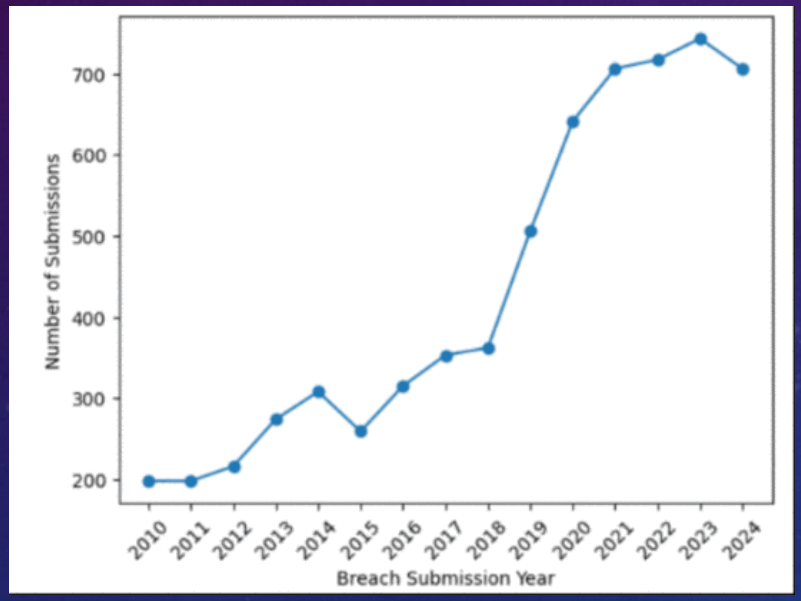
- Prices fluctuate wildly
- CC: $1.50 typical, but 10-15c after the Target and Home Depot Breaches
- Medical Record: $50 typical, but $120 with controlled substances

UNDER ATTACK…

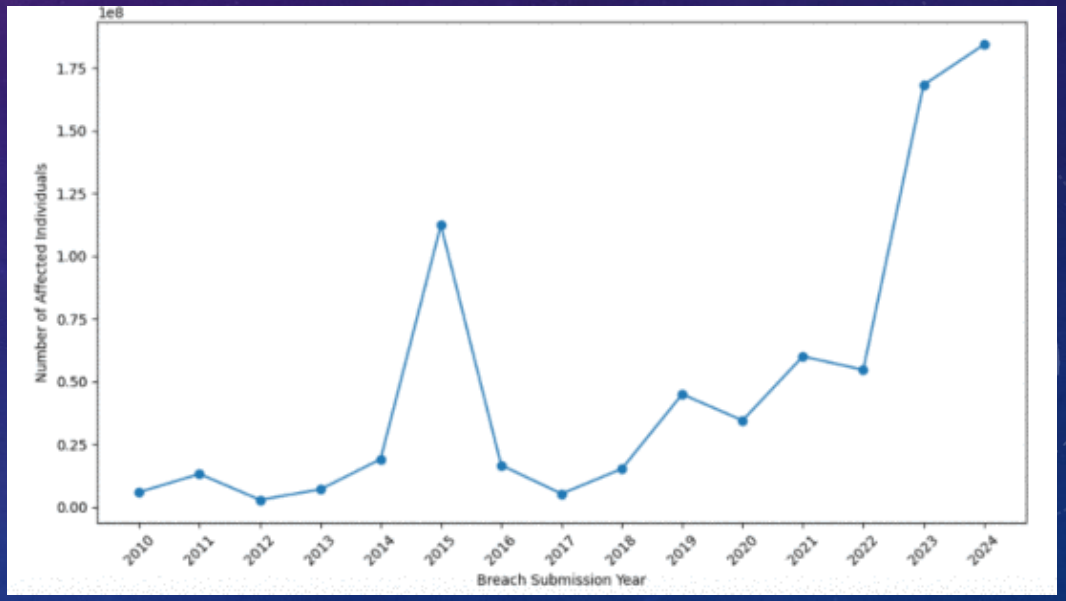
Healthcare Data Security - HIPAA Journal

HIPAAJournal.com › category › healthcare-data-security ▾

Causes of August 2019 Healthcare **Data** Breaches **Hacking** and other IT incidents ..... Cybercriminal gangs and **nation-state** sponsored **hacking** groups are investing ..... First, a patient's DNA is sequenced and their **genome** is mapped. ..... American Medical Association (AMA), and the American Hospital Association (**AHA**).



Breach Submissions



Affected Individuals (100M)

L. Xu, "Trends in US Healthcare Data Breaches," *2025 IEEE International Conference on AI and Data Analytics (ICAD)*, Medford, MA, USA, 2025, pp. 1-8, doi: 10.1109/ICAD65464.2025.11114030.

TARGETS

Intellectual Property (IP)

- Commercial advantage
- Theft of research data

Drug/clinical trial data

- $$

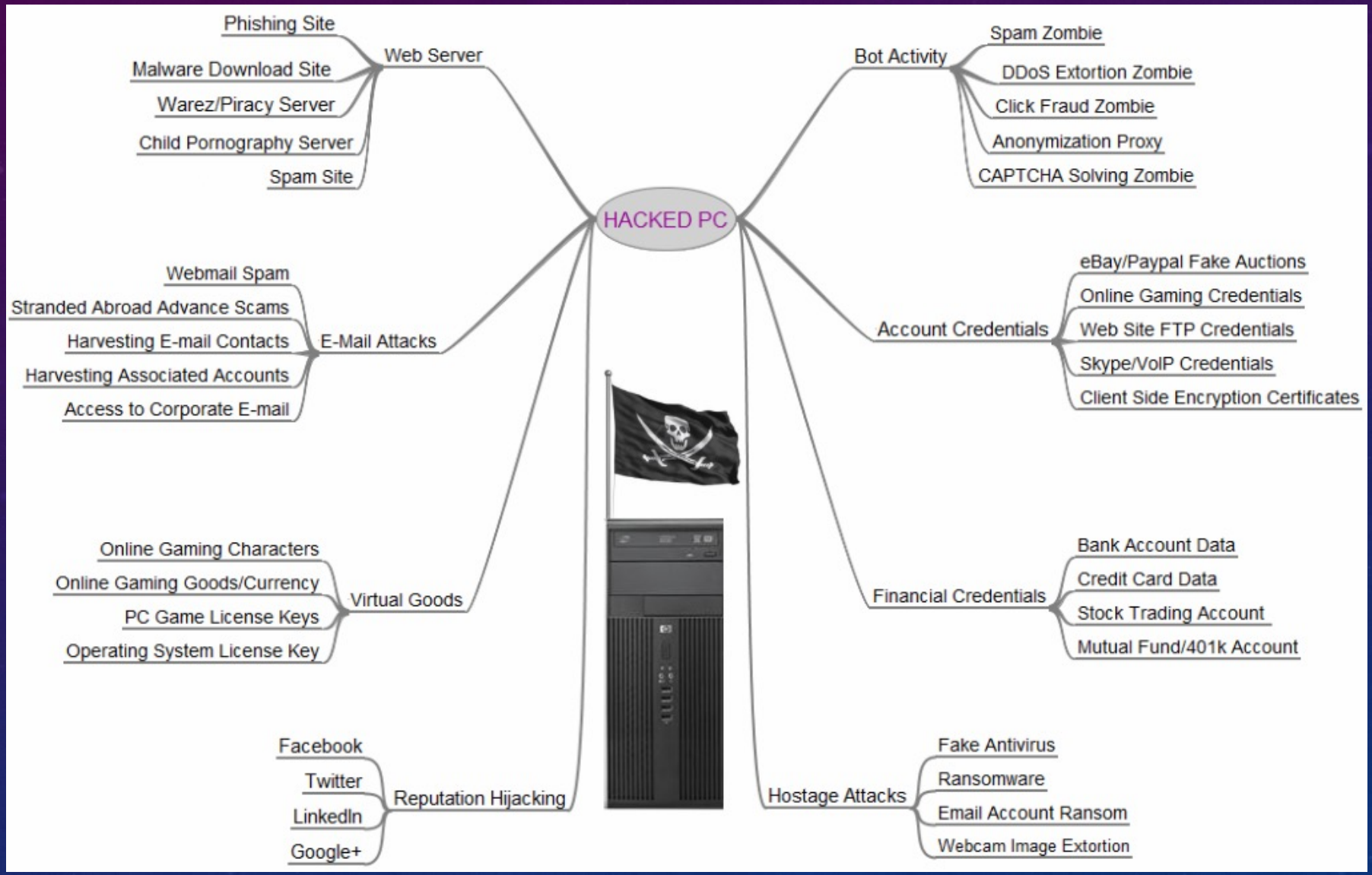
Genomic Data

- Tailored Biological Weapons

HACKERS

- Fun and profit
- Hacking as a Subculture
  - Conferences such as BlackHat
  - Private chat rooms
- Hacking tools
- Use of social media

THREAT LANDSCAPE



Credit: Brian Krebs

BIGGEST TREATS

- Malware (malicious software)
- Ransomware
- Social engineering / phishing

MALWARE

Used for financial gain and business spying/espionage

Spyware (adware, trojans, keystroke loggers, etc.)

Botnets for Distributed Denial of Service (DDoS)

- Collection of compromised “zombie” computers ready to deliver malware

Viruses spread via Instant Messaging (IM), Twitter, Facebook, etc.

Highly sophisticated – features now equivalent to software companies

- Licensed Malware
- Rent a Bot
- Pay per… user account, Credit Card, SSN, identity.

RANSOMWARE

How it happens:

- Downloaded attachment
- Such as PDF, DOCX, etc.
- Click on wrong link

Then:

- Downloads the keys and encryption software
- Silently Encrypts the data
- Tells the user to pay usually using Bitcoin

SOCIAL ENGINEERING

- Phishing
  - Mass information stealing effort
- Spear Phishing
  - Highly targeted information stealing effort
- Password stealing
- Physical access

HOW THEY DO IT… EMAIL PHISHING

From: Marna P. Borgstrom Marna.Borgstrom@ynhh.org [mailto:twright72@aol.com]
Sent: Wednesday, February 20, 2019 12:15 PM
Subject: ACTION REQUIRED - Yale New Haven Health System Employee Engagement Survey 2019 (February 20)

EXTERNAL EMAIL: Do NOT click links or open attachments unless you trust the sender AND know the content is safe.

From: Marna P. Borgstrom
Sent: Wednesday, February 20
To: All Employees
Subject: Yale New Haven Health System Employee Engagement Survey 2019 (February 20)

YaleNewHavenHealth
Yale New Haven Hospital

Dear Yale New Haven Health System Staffs,

On behalf of Yale New Haven Health System and the entire leadership team, you are cordially invited to participate in the 2019 Employee Engagement Survey. We have once again partnered with the consulting firm to administer the survey. It will only take about 5 minutes to complete and will provide valuable information on how well employees are engaged at Yale New Haven Health System.

Click here to take the survey <Link redacted>

When completing the survey, please express your opinions frankly as the survey is completely confidential, and only aggregated data will be presented. However, please be aware that all written comments will be reported as stated.

Open in Docs <link redacted>

Please complete your survey no later than February 21, 2019.

Your participation in the survey is encouraged and will be greatly appreciated. Thank you in advance.

HOW THEY DO IT… EMAIL PHISHING

From: Amerlcan Express [mailto:americanexpressglobalcardservices.amex@amx.globalindinc.com]
Sent: Tuesday, December 18, 2018 8:43 AM
To: americanexpressglobalcardservices.amex@amx.globalindinc.com
Subject: Last Reminder on Refund Acknowledgement of $1728.18

EXTERNAL EMAIL: Do NOT click links or open attachments unless you trust the sender AND know the content is safe.

American Express ®

Dear Amex Client,

It has come to our notification that your card is eligible to some refunds from previous activities during the year 2018, that did not return as reward point to your card during the time you reported unauthorized activities on your card, due to long term investigation. We have finally acknowledge the refund of $1728.18,which is pending now.

To enable us proceed with your refund, please follow the steps bellow:

*** Download the Refund Form**
*** Open the form and follow the instructions on your screen**
*** Submit Form and Your refund will be process in 24 to 48hours**

Your refund can be delayed for a variety of reasons. For example submitting invalid information or sumbitting different information twice.

American Express Customer Services

HOW THEY DO IT… EMAIL PHISHING

From: Amazon.com [mailto:Amazon_1@Devora2290.hostpilot.com]
Sent: Tuesday, October 24, 2017 6:33 PM
Subject: We could not confirm the address associated with your Amazon account

amazon

Address Verification

Hello Customer

We could not confirm the address associated with your Amazon account. As a result, we have disabled the ability for anyone to login to your account to avoid account misuse. To resolve this, a verification process is required to be completed.

Verify Account Information now

Note that this is required to be completed to enable us re-enable access to your Amazon.com account. And all information should be provided as contained on file.

Thanks
Amazon.com Security Team

amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

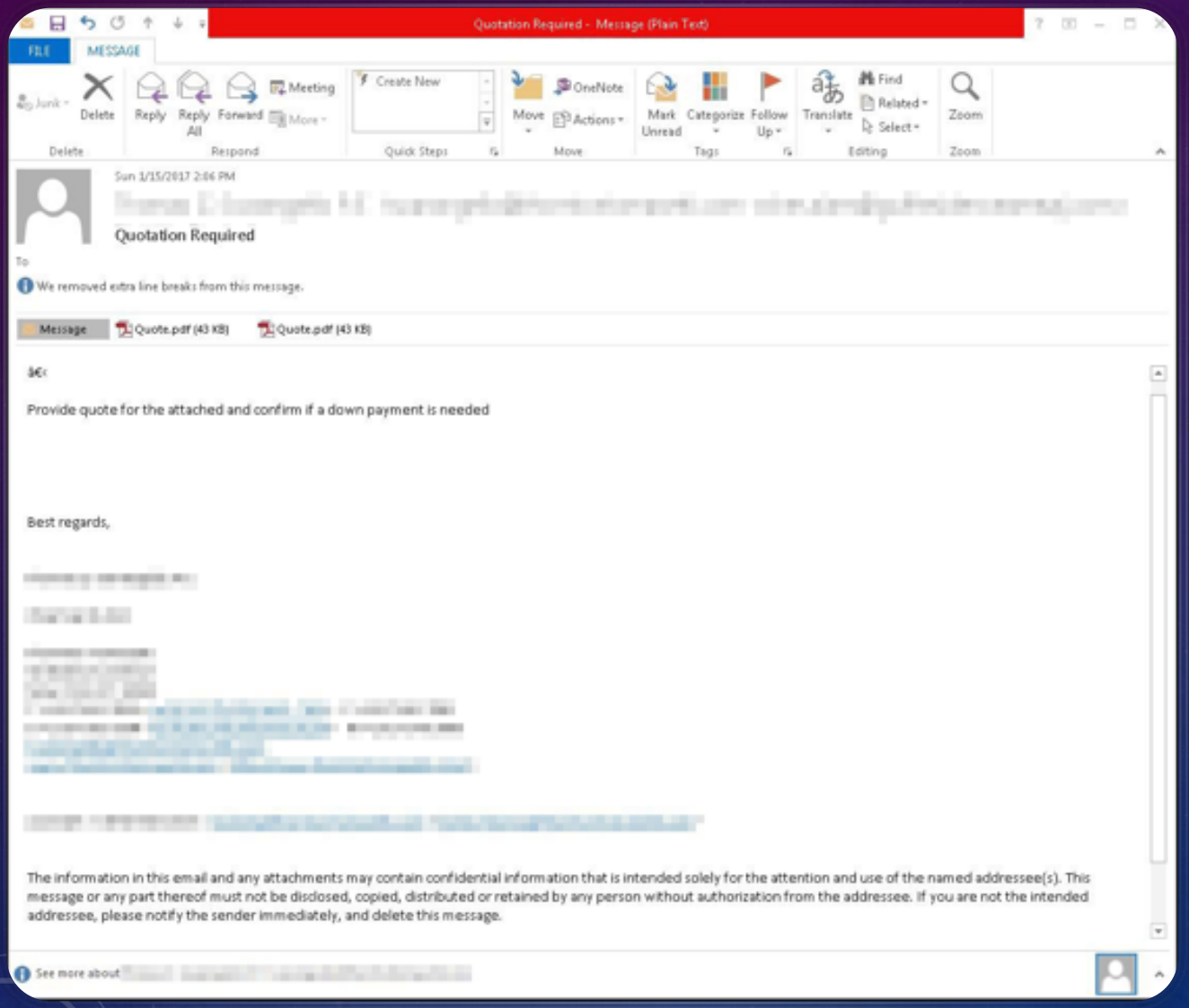
We hope to see you again soon.
Amazon.com
Email ID:

ATTACHMENTS WITH LINKS IN THEM

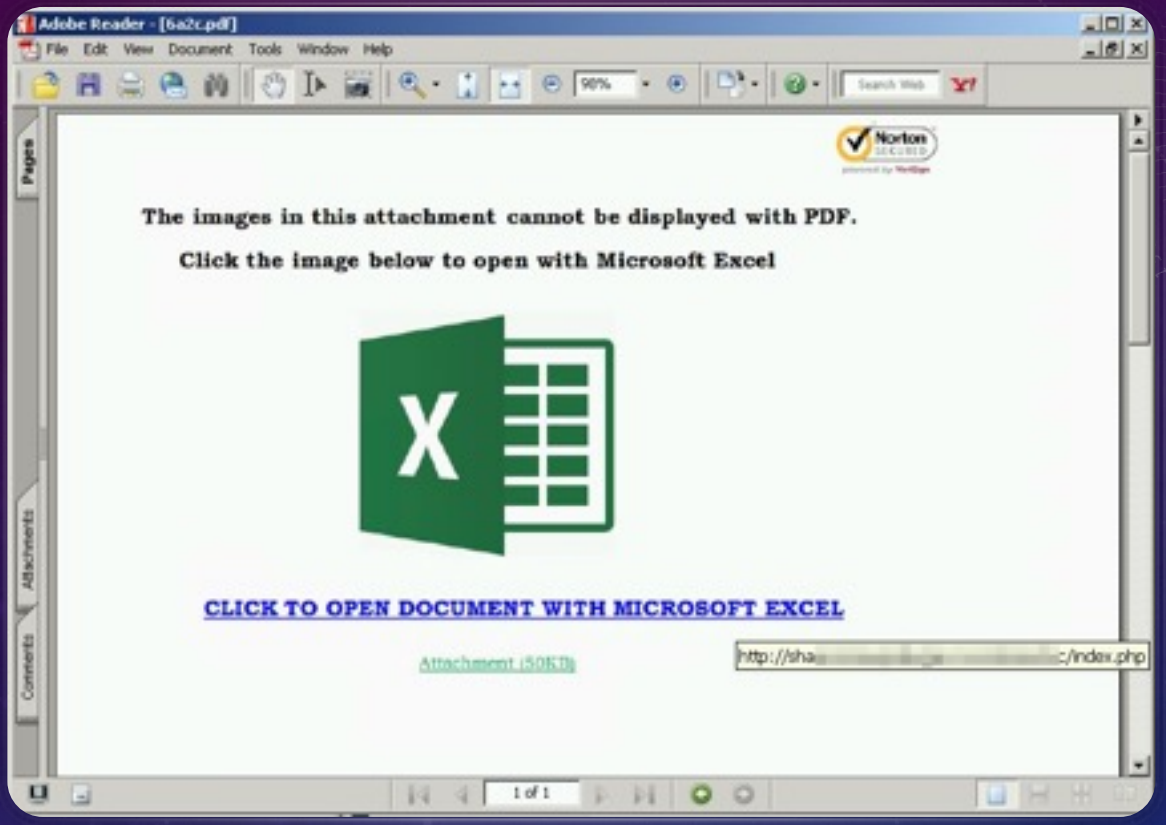
If the email has an attachment.

You open the attachment, and it tells you to click a link.

You really click the link.



ATTACHMENTS WITH LINKS IN THEM



ATTACHMENTS WITH LINKS IN THEM

AGENDA

- Information security
  - What it is, How it fits into Healthcare, our Relationships.
  - General Concepts of Information Security
- Challenges specific to healthcare information security
- Defending against the risks
- HIPAA and other laws
- Homework 3

DEFENDING METHODS

- Anti-Virus
  - Software-pattern (“signature”) scanning
- Intrusion Detection/Prevention System
  - Also used similar scanning techniques
  - Behavior anomaly
- Vulnerability assessments
  - Need to cover technical, physical, and administrative aspects
  - Penetration (“Pen”) testing
- Web filtering
  - Prevent access to suspicious web sites

DEFENDING METHODS

- Special VPN
- Firewalls
- Encryption
- Secure hashing
- Human-based detection

SPECIAL VPN

Personal VPN

- Designed for an individual user

Site-to-Site VPN

- Designed to connect two different organizations
- Usually over the Internet
- Requires both Firewalls to agree on protocols/keys
- Requires paperwork and lead time
- For example, vendor support

FIREWALLS

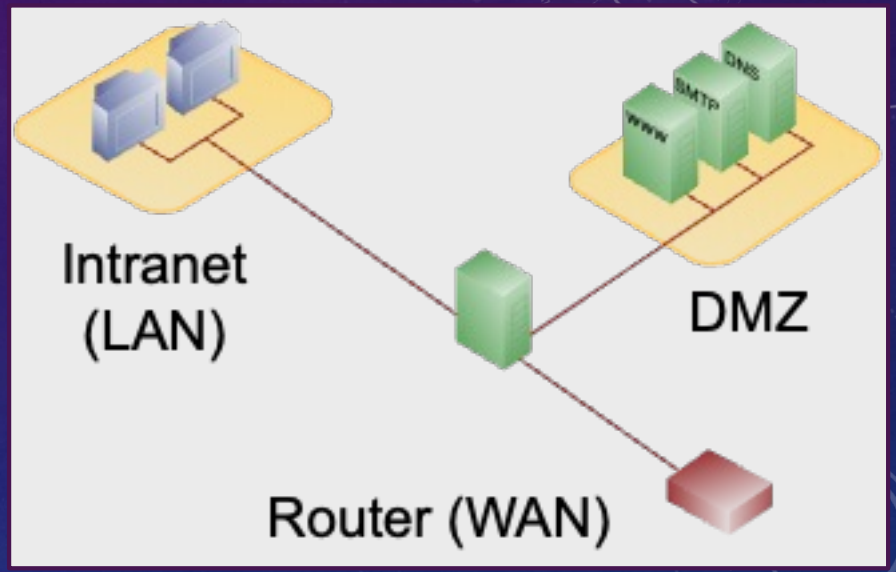
Separates networks of differing security policies

Enforces which systems can connect to other systems and how

Incorporates different types of protection technologies

- Deep inspection
- Anomaly control
- Intrusion prevention

Creates De-Militarized Zone (DMZ) as “buffer” of public-facing servers



Reference: https://en.wikipedia.org/wiki/DMZ_(computing)
https://en.wikipedia.org/wiki/DMZ_(computing)#/media/File:DMZ_network_diagram_1_firewall.svg

ENCRYPTION: SYMMETRIC KEY

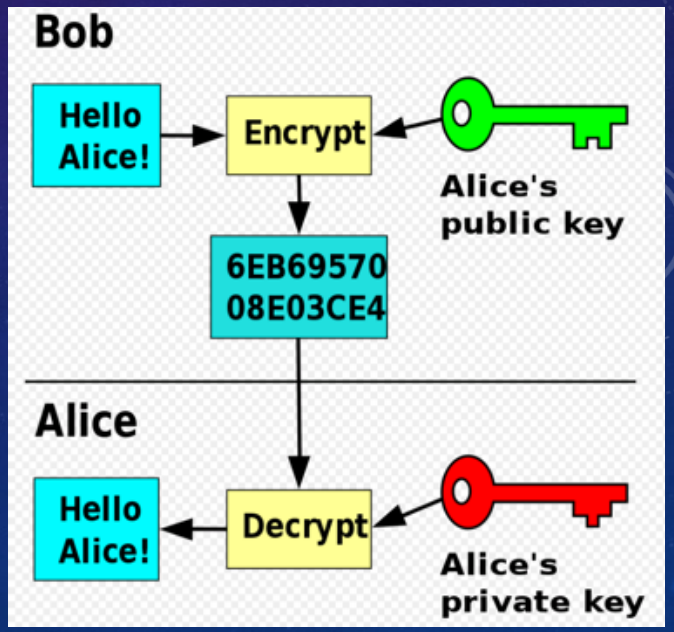
- Symmetric
  - Both sides know the ‘key’
  - Both sides encrypt and decrypt with the same ‘key’

- Very Basic example
  - The ‘key’ is KEYWORD
  - YALE encrypts to XKGO
  - If both sides know the algorithm and the ‘key’ they can successfully communicate encrypted messages.

ENCRYPTION: ASMMETRIC KEY

- Avoid key sharing
  - One Key can be used to encrypt the message (the public key)
  - One Key can be used to decrypt the message (the private key)

- Also used to ‘digitally sign’
  - Alice encrypts a message with private key
  - Can be decrypted with the public key
  - Assuring that the sender was Alice



ENCRYPTION: ALGORITHMS

- Avoid writing your own encryption method
  - May not be robust against attacks
  - Plenty of library functions available
- Lots of encryption routines such as Advanced Encryption Standard (AES)
  - AES128 – 128 bit key
  - AES192 – 192 bit key
  - AES256 – 256 bit key
- National Security Agency (NSA) considers
  - 128 and above suitable for Secret Information
  - 256 for Top Secret
- Longer the key the more secure yet slower

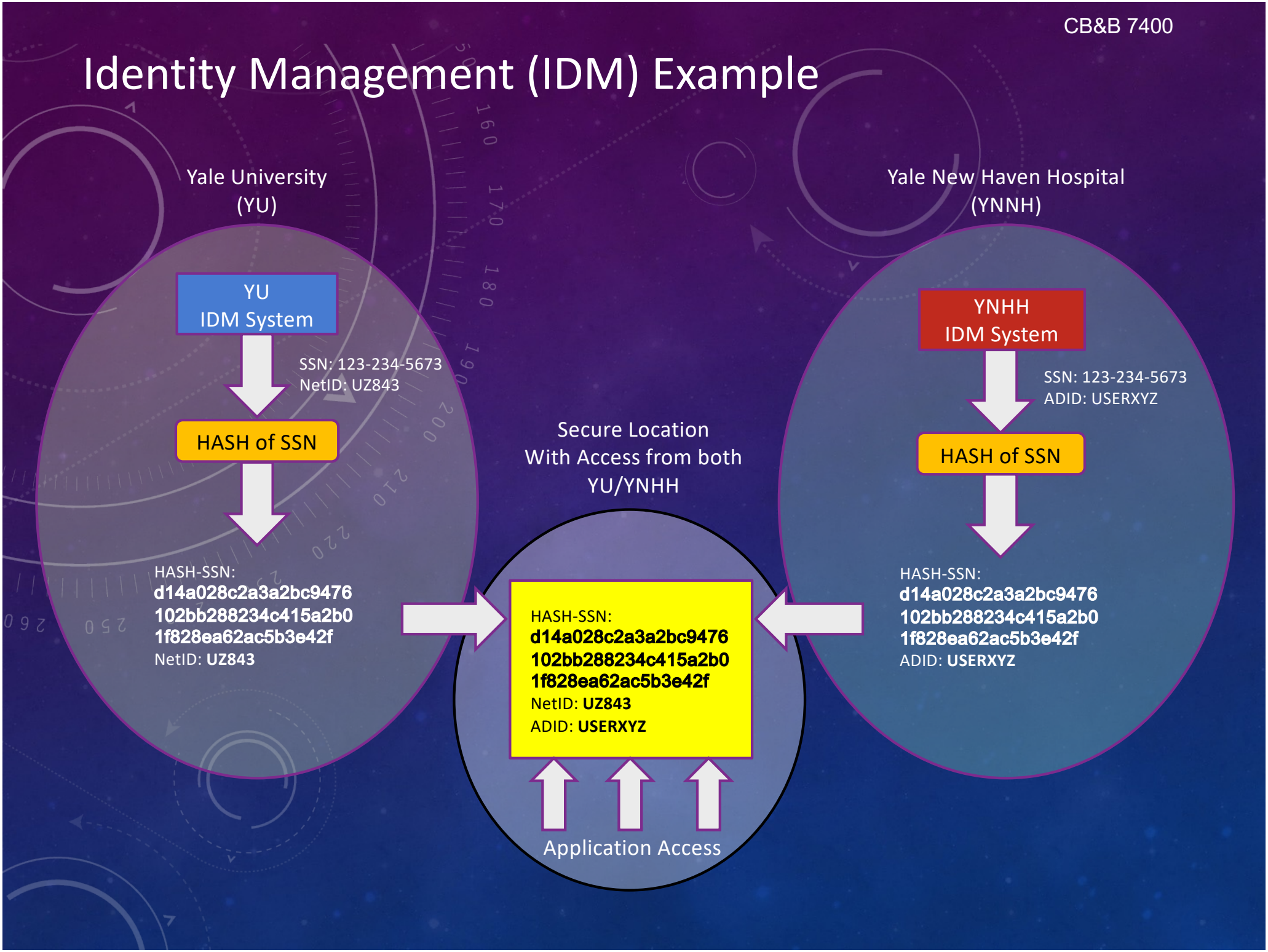
SECURE HASHING

Example Hash Functions
- **123 mod 10 = 3**
- **4256 mod 10 = 6**

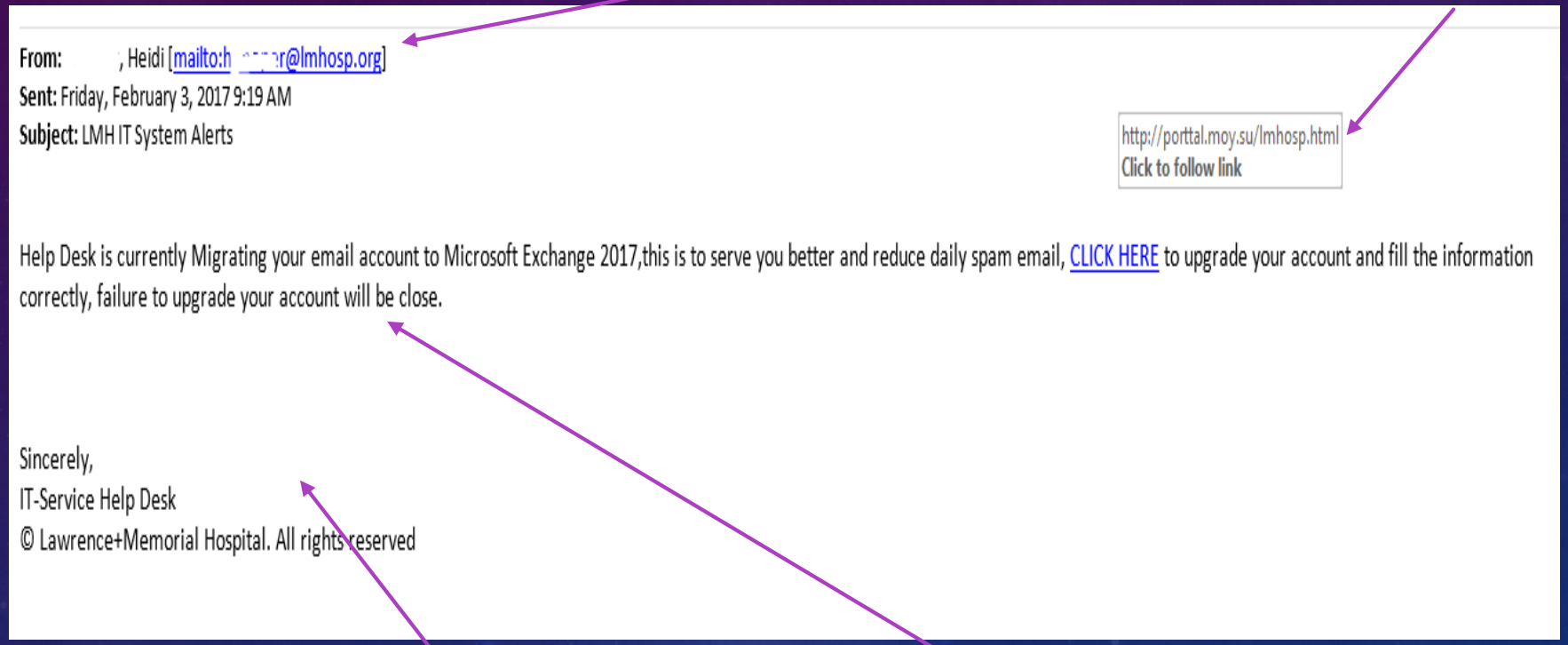
- Turns any amount of data into a fixed-length ‘fingerprint’
- Provides different output for different input
- Is one-way function (i.e., cannot be easily reversed)
- Therefore, is useful for de-identification
- Example: Secure Hash Algorithm (SHA)

```
hash("hello") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
hash("hbllo") = 58756879c05c68dfac9866712fad6a93f8146f337a69afe7dd238f3364946366
hash("waltz") = c0e81794384491161f1777c232bc6bd9ec38f616560b120fda8e90f383853542
```

Identity Management (IDM) Example



HUMAN-BASED DETECTION: EMAIL PHISHING



Used a compromised login
But not from 'helpdesk'

'Hover trick' –
link looks 'odd'

From: , Heidi [mailto:h r@lmhosp.org]
Sent: Friday, February 3, 2017 9:19 AM
Subject: LMH IT System Alerts

http://porttal.moy.su/lmhosp.html
Click to follow link

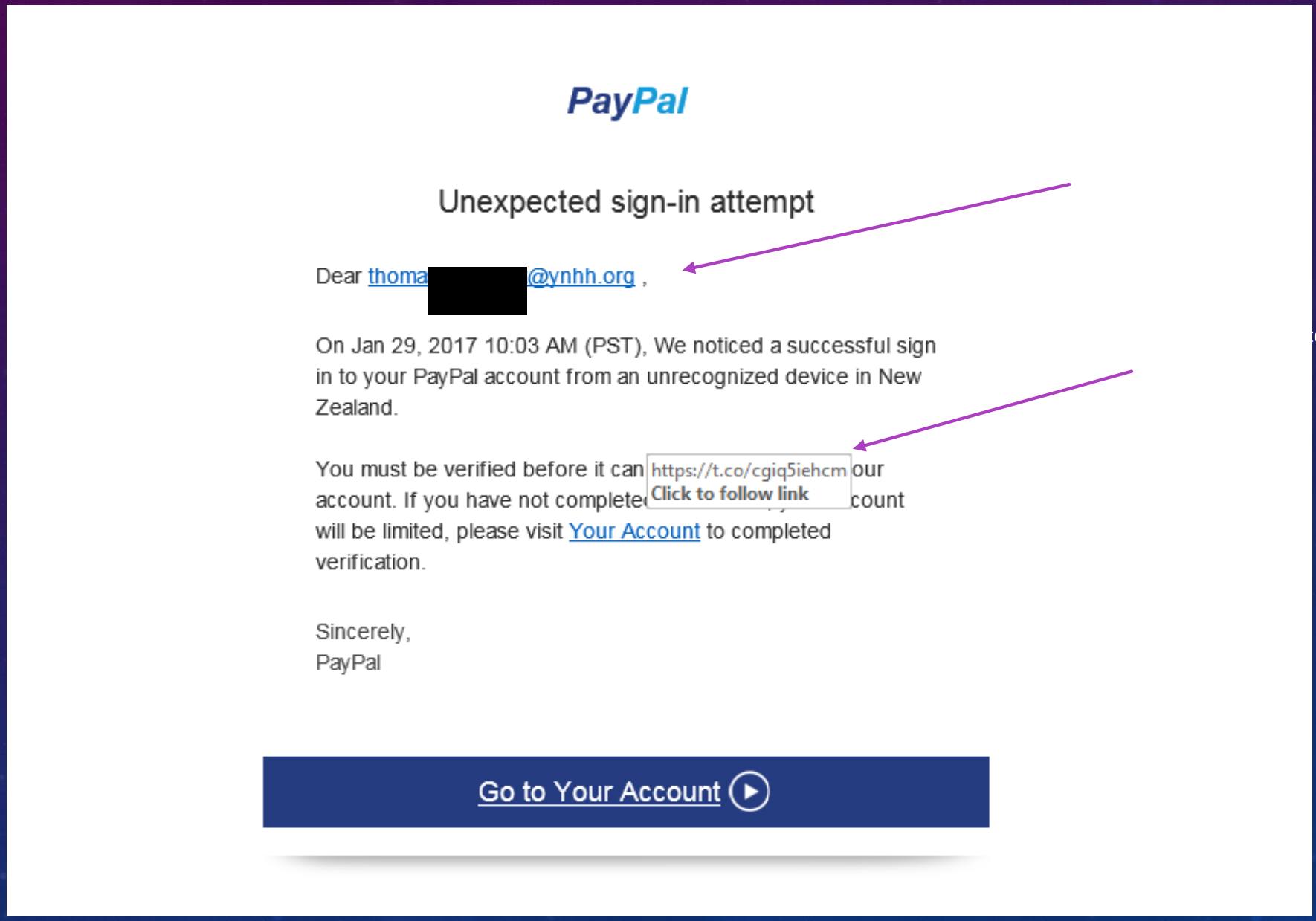
Help Desk is currently Migrating your email account to Microsoft Exchange 2017,this is to serve you better and reduce daily spam email, CLICK HERE to upgrade your account and fill the information correctly, failure to upgrade your account will be close.

Sincerely,
IT-Service Help Desk
© Lawrence+Memorial Hospital. All rights reserved

No contact
phone or way
to validate.

Poor Grammar

HUMAN-BASED DETECTION: EMAIL PHISHING



PayPal

Unexpected sign-in attempt

Dear thoma[redacted]@ynhh.org ,

On Jan 29, 2017 10:03 AM (PST), We noticed a successful sign in to your PayPal account from an unrecognized device in New Zealand.

You must be verified before it can https://t.co/cgiq5iehcm our account. If you have not complete Click to follow link count will be limited, please visit Your Account to completed verification.

Sincerely,
PayPal

Go to Your Account

AGENDA

- Information security
  - What it is, How it fits into Healthcare, our Relationships.
  - General Concepts of Information Security
- Challenges specific to healthcare information security
- Defending against the risks
- HIPAA and other laws
- Homework 3

HIPAA/HITECH

HITECH – "The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the Health Insurance Portability and Accountability Act (HIPAA) rules.'

- HIPAA – "It's the Law" – 1996
- Separated into two "Rules" – Security Rule and the Privacy Rule
- Typically, compliance or "privacy officer" responsible for implementing the Privacy Rule
- The Security Rule in general falls into IT responsibility

HIPAA COVERAGE

Covered Entities (CEs):

- Health Plans: includes private insurance, VA, Medicare, Medicaid, self-funded employee insurance plans
- Health Care Providers who bill electronically
- Healthcare Clearinghouses (intermediate between providers and insurance companies)
- Business associates of any of the above
- HIPAA Final rule adds: their subcontractors

BUSINESS ASSOCIATES

Require a “Business Associate Agreement” – BAA

When is a 3rd Party a Business Associate..?

- They need access to Protected Health Information (PHI)
  - They do something ‘on behalf’ of the Covered Entity
  - Usually commercial contract

OTHER RELEVANT LAWS…

State laws related to Personally Identifiable Information (PII)

- SSNs tend to be the most important data element
- Bank account information (with additional information e.g. pin/password)
- Every state has a different law and need to be careful

GDPR – European privacy law

PCI (Payment Card Industry)

- Credit card data

ELEMENTS OF PHI..

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;

ELEMENTS OF PHI..

7. Social Security numbers;

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;

ELEMENTS OF PHI..

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);

15. Internet Protocol (IP) address numbers;

16. Biometric identifiers, including finger and voice prints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

SSN

Unless necessary - just don't.

Triggers all kinds of laws and requirements for notification, e.g. State Attorney General.

First 4 - Last 4… still better to avoid it

Did you know…

If I know the state, I can predict the first 3 numbers ?

Before 2011, the first 3 numbers were assigned geographically.

- 010-034 – Massachusetts
- 040-049 – CT
- 050-134 - NY

Now randomized to protect privacy and allow more numbers to be used

PHI, LIMITED DATA SET (LDS), & DE-IDENTIFIED

If it contains the 18 identifiers it's PHI.

If it is a subset of the 18 identifiers (specifically, time and location), then it's LDS – still need to be protected in the same way as PHI

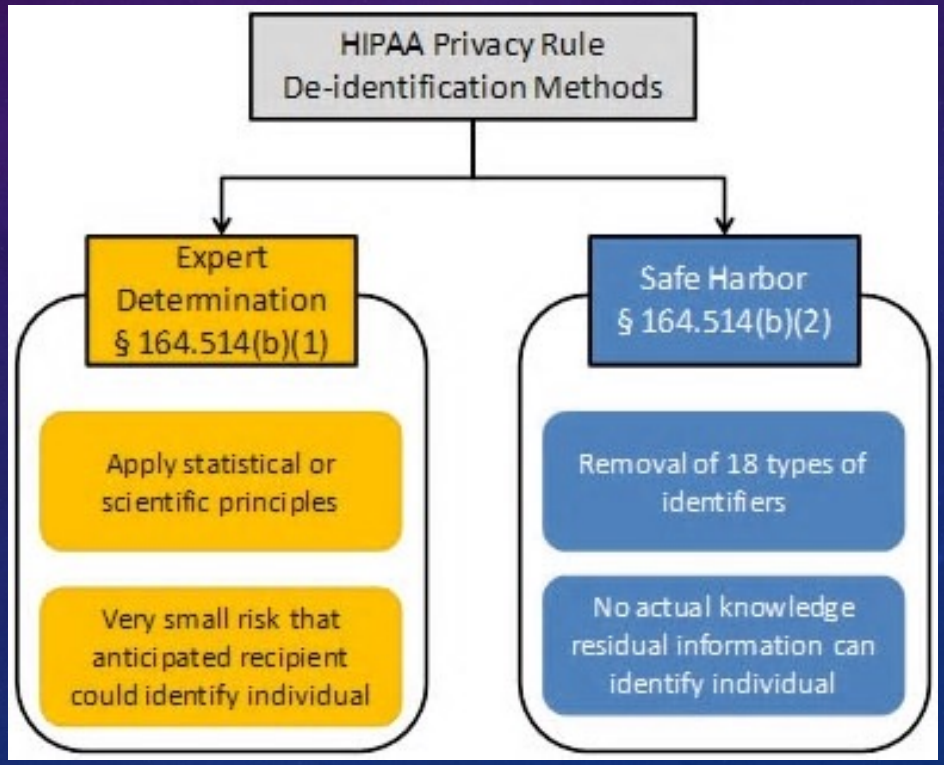
A de-identified data set removes all 18 identifiers

EASY!!!

- HIPAA is easy to understand on this point
- It's also simple
- Just need to be very careful

THERE ARE ONLY TWO OPTIONS..

You remove the 18 Identifiers (The **Safe Harbor Method**)
OR
The "**Expert Determination" Method**
That's it.. There is no discussion. It's the easy way or the hard way



Reference: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

EXPERT DETERMINATION

The "Expert Determination" method:
(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:
*(1) **A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:***
(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
(ii) Documents the methods and results of the analysis that justify such determination;

We are usually not "the person"

HIPAA PROTECTS US

Privacy of medical data is a CIVIL RIGHT, guaranteed to you by the HIPAA law.

Oversight by OCR – the Office of Civil Rights!

So how could we do our job ?

GENEARL RULES

1) You are allowed to use patient data for TPO purposes

- Treatment
- Payment
- Operations

2) If you fully de-identify the data or it's truly de-identified (expert determination), you can use it

3) If you have approval to use the data for research (IRB approval) – typically this means that the patient has agreed (opted in or not opted out)

4) With approval, PHI may be used within an institution for internal Quality Improvement (QI)

- **What you should NOT do….**
- Independent research projects
- Create independent data stores of PHI
- Take it off approved systems
- Save in USB drives, make local copies, etc.

If unsure for research, always consult with Yale Human Research Protection Program (HRPP) Office

SHARING THE DATA

1) PHI may be shared with another COVERED ENTITY for TPO purposes

- Treatment
- Payment
- Operations

2) For a non-covered entity, OR, when shared for any other reason …

- BAA – Business Associate Agreement. Generally, commercial terms, e.g. a Vendor
- DUA – Data Use Agreement. Generally, Research, QI or other

3) Sharing with Government entities. Need to ask:

- Are they requesting the data based on 'statutory authority' i.e., a law exists
- If NOT – requires a DUA

HIPAA contains a clause that states "Minimum Necessary", so only the minimum data required must always be shared

AGENDA

- Information security
  - What it is, How it fits into Healthcare, our Relationships.
  - General Concepts of Information Security
- Challenges specific to healthcare information security
- Defending against the risks
- HIPAA and other laws
- Homework 3

HOMEWORK 3

- De-identify and annotate 3 clinical texts

Jared Gentry starred in The Lord of the Rings, released on 1975. 16 51975-01-06.

- Using Python-based PyDeid tool
  - https://doi.org/10.1093/jamiaopen/ooae152
  - https://doi.org/10.1186/1472-6947-8-32
  - https://github.com/GEMINI-Medicine/pyDeid

- Due date: 11:59pm on Tuesday 9/30

Questions?