

Information Security in the Digital Era

Hye-Chung Kum (kum@tamu.edu)

Associate Professor

Population Informatics Lab (<https://pinformatics.org/>)

Course URL: <http://pinformatics.org/phpm631>

License:
Health Information Technology by Hye-Chung Kum is licensed under a
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

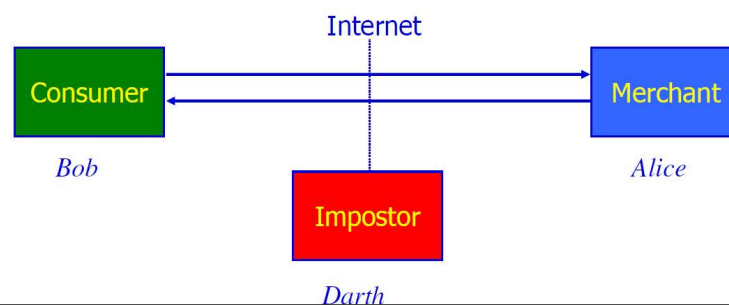


2

2

Communication security issues

- Encryption -How do I ensure the secrecy of my transactions?
- Authentication -How do I verify the true identity of my counterparts?
- Integrity -How can I be sure the message hasn't been altered?



3

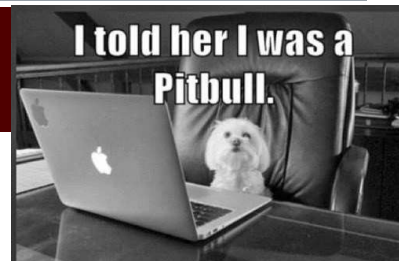
Encryption



- Secret key cryptography: Based on a secret key
 - Same secret key used for encryption and decryption
 - Problem: How to transmit key securely on the Internet??? (out of bandwidth communication)
- Public key cryptography: Two keys used
 - Public key known to everybody. Used for encryption.
 - Private key known only to owner. Used for decryption.
 - Reliable public key distributed
 - This is the most difficult problem!

4

Encryption is not enough: Spoofs (impersonate)



- Pretending to be someone else
- Hard to login without someone's password
- But can send out communications with someone else's name on it
 - Email
 - 1993: Dartmouth sent a message saying midterm exam was cancelled
 - Message appeared to come from the Professor!

5

Needed: Message Authentication

- Integrity: Make sure Bob gets the message unaltered
- Authentication: Don't let Alice deny sending the message
 - Guarantee No Plausible Deniability
- Don't care about eavesdropper Darth, unless Darth changes the message
- How can cryptography help?

6

Authentication: Who are you? Digital Identity?

WEBSITE IMPERSONATION ATTACKS.
WHO IS REALLY BEHIND THAT MASK?



7

7

Securing access to resources: Access Control

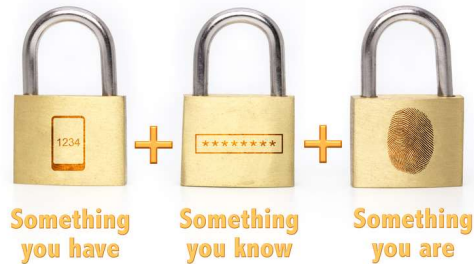
Who are you? - Authentication



- Something you have
 - Smart Cards:
 - Store user's digital certificate and/or private key
 - Smart Phone
 - YubiKey
- Something you know
 - Login Procedures
 - Password leaks
 - Passwords are inconvenient
 - Two-factor authentication
- Something you are
 - Biometrics: fingerprint, face & voice recognition

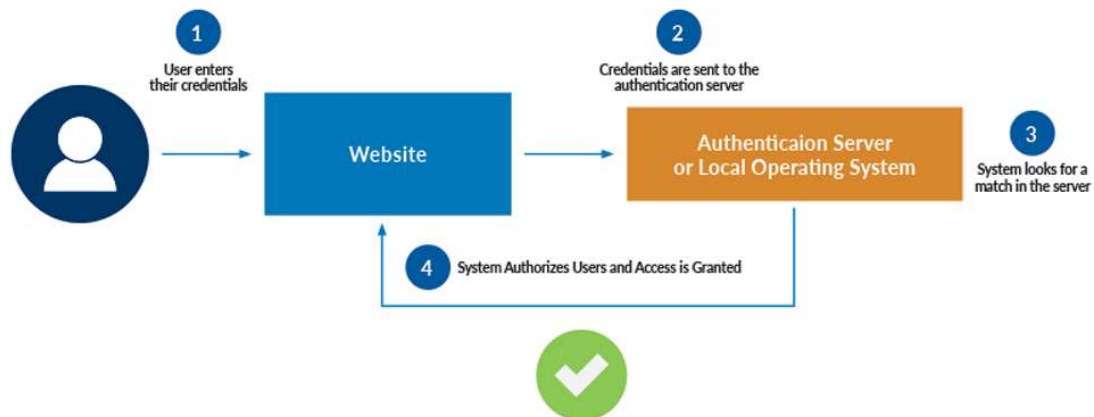


Multi factor authentication



8

Access Control



9

Authentication & Integrity Digital Signatures



- Key property: Public and private keys can be applied in either order
- Alice has message M
 - She applies her private key to it
 - She sends encrypted message to Bob
- Bob decrypts it with Alice's public key
 - gets back original message
 - infers that Alice is indeed the sender (since only Alice has the private key that corresponds to her public key)
- In that way, encrypting a message with one's private key acts as a digital signature!

10

HIPAA Security: Hye-Chung Kum's Opinion



- | | |
|---|--|
| <ul style="list-style-type: none"> ■ NOT security expert ■ Security vs Compliance ■ Main threat <ul style="list-style-type: none"> ○ Identity theft ○ Medical fraud ? ■ When breach occurs <ul style="list-style-type: none"> ○ Reporting requirements ○ Penalties and noncompliance ○ Extenuating circumstances | <ul style="list-style-type: none"> ■ Due Diligence <ul style="list-style-type: none"> ○ Risk Analysis and Management <ul style="list-style-type: none"> • Security Risk Assessment : Tools ○ Physical Safeguards ○ Technical Safeguards ○ Administrative Safeguards <ul style="list-style-type: none"> • Training • Reasonable documentation of policies & procedures |
|---|--|

11

HIPAA Security: Hye-Chung Kum's Opinion Summary

- The art of balancing
 - Security is costly BUT very important
 - Security costs can take away from services
 - Each health system MUST have someone who knows enough about security to do the balancing act
 - Management have to know enough to recognize them, keep them, and listen to their advice
 - Dynamic: Stay just above the curve
 - At least now - lots of systems have lots of holes
 - So relatively easy to stay ahead of the curve

12

Take Away I: What is Computer Security ?

- Securing communications
 - Three steps:
 - Secrecy = prevent understanding of intercepted communication
 - Authentication = establish identity of sender
 - Integrity = establish that communication has not been tampered with
- Securing access to resources
 - Two steps:
 - Authenticate = establish identity of the requestor
 - Authorize = grant or deny access

13

Take Away II: Encryption

- Secret key cryptography: Based on a secret key
 - Same secret key used for encryption and decryption
 - Problem: How to transmit key securely on the Internet???
- Public key cryptography: Two keys used
 - Public key known to everybody. Used for encryption.
 - Private key known only to owner. Used for decryption.
 - Reliable public key distributed
 - This is the most difficult problem!
 - Public Key Infrastructure (PKI): certification services (trusted site)

14

Take Away III: Defensive Measures

- | | |
|--|---|
| <ul style="list-style-type: none"> ■ Install and maintain antivirus software ■ Firewalls <ul style="list-style-type: none"> ○ Put up around a network for more security ○ Hide structure of network ○ Only allow traffic from "legitimate users" ○ Screens data packets for checks ■ Intrusion Detection Systems <ul style="list-style-type: none"> ○ Data mining techniques to detect and report suspicious activities ○ Main strategies <ul style="list-style-type: none"> • Pattern recognition • Anomaly detection ■ Other Preventive Measures <ul style="list-style-type: none"> ○ Stay Current on patches <ul style="list-style-type: none"> • Zero day attack: Never seen before | <ul style="list-style-type: none"> ■ Protect mobile devices ■ Maintain good computer habits ■ Plan for the unexpected (i.e., create backups) ■ Control access to PHI ■ Use strong passwords ■ Limit network access ■ Control physical access |
|--|---|

15

Information Privacy in the Digital Era

Hye-Chung Kum (kum@tamu.edu)

Associate Professor

Population Informatics Lab (<https://pinformatics.org/>)

Course URL: <http://pinformatics.org/phpm631>

Health Information Technology by Hye-Chung Kum is licensed under a
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

License:



16

16

Privacy, etc.

Slides Adapted from

Cason Schmit, J.D.

Research Assistant Professor

HIPAA Liason

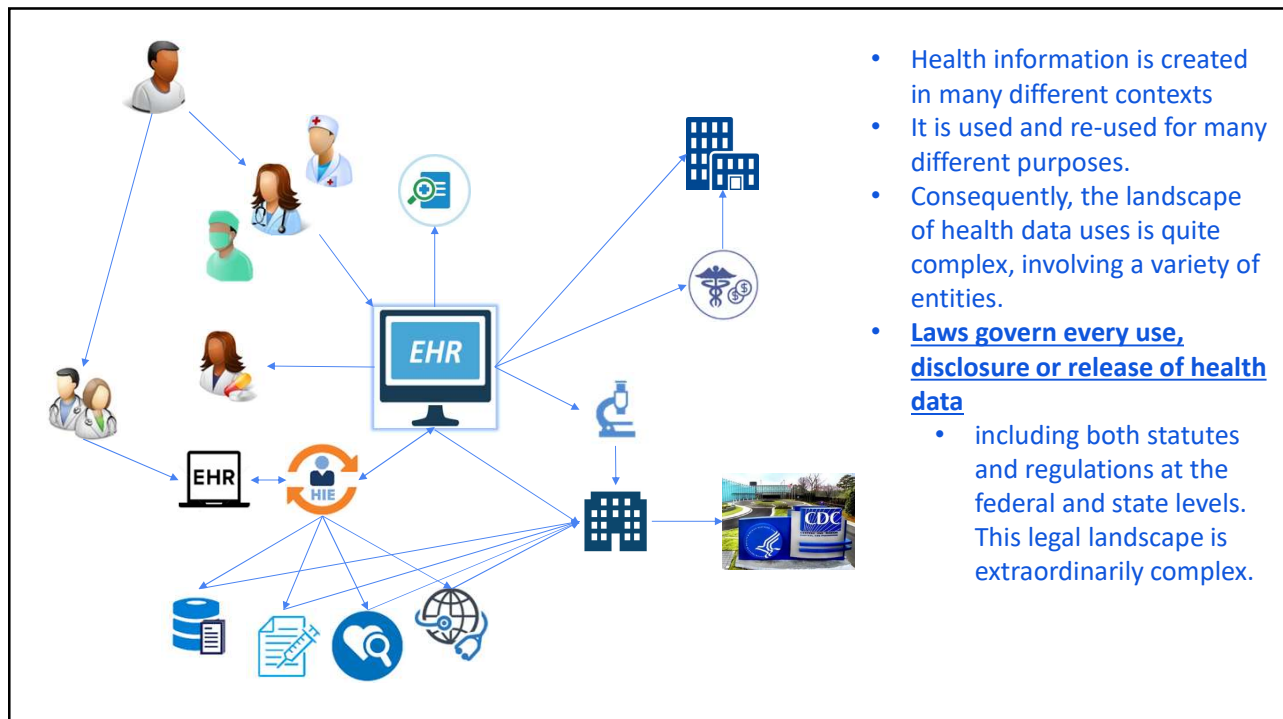
Texas A&M School of Public Health

17

THE HEALTH DATA LANDSCAPE

How is health data used?

18



19

Objectives of This Lecture

- We want to give you a **basic understanding** of a few legal issues that you **will likely come across** in your career.
- We want you to **be more comfortable engaging** in your legal counsel to **identify legal tools** that will help you accomplish your objectives
- We want to **empower you to work with legal counsel** to think creatively about **technological solutions** to legal barriers

20

Actual and Perceived Legal Barriers to Data Use and Release

- There are many “perceived” legal barriers to data use and release
 - Not all are actual legal prohibitions
 - Three approaches to perceived barriers
 - Identify conservative data use policies that may need to be addressed
 - Identify legal solutions
 - Identify technological solutions
- } Require an understanding of
underlying legal framework.
Your attorney is your friend!

21

Example of Conservative Data Use Policies

- Conservative HIPAA policies in organizations
 - Total data lockdown
 - Assume all data is identifiable/HIPAA-protected
 - Share nothing
 - No secondary data uses permitted
 - Restricts legal uses of data



22

Examples of Legal Solutions to Perceived Barriers

- EHR Access difficulties during a fungal meningitis outbreak investigation
 - Educate healthcare providers of legal protections and exceptions
 - Create data use and confidentiality agreements with healthcare providers
 - Share governance documents and policies and procedures
 - Enact new laws
 - “Access shall be given in the most efficient and expedient means possible, including remote electronic access, to facilitate investigations and inquiries while responding to an immediate threat to the public health, welfare, or general good.”
 - TENN. CODE ANN. § 63-1-117 (West)

Improving Your Access to Electronic Health Records During Outbreaks of Healthcare-associated Infections,
<http://www.astho.org/Toolkit/Improving-Access-to-EHRs-During-Outbreaks/>

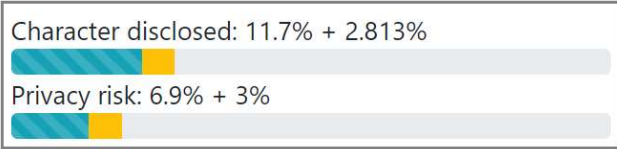
23

Examples of Technological Solutions to Perceived Barriers

- Distributed database querying
 - Allows custodians to maintain custody of health data
 - Allows researchers to query distributed database network for aggregated results
 - No personally identifiable data is obtained
- Differential privacy
 - Adds random “noise” to datasets to limit re-identification of individuals
 - Maintains some aggregate query functionality
- Controlled Selective Partial Disclosure with Accountability

24

Controlled Selective Disclosure with Accountability in Patient Matching



Pair	ID	FFreq	First name	Last name	LFreq	DoB (M/D/Y)	Sex	Race
1	*****00**	①	✓	*****	①	**/**/**00	✓	@
	*****48**	①	✓	***** JR	①	**/**/**48	✓	&
1	*****27**	①	✓	*****	①	**/**/**06	M	@
	*****35**	①	✓	***** JR	①	**/**/**60	M	&
1	8000002767	①	JUDE	WILLIAM	①	09/09/1906	M	W
	8000003567	①	JUDE	WILLIAM JR	①	09/09/1960	M	B

Nothing Opened
 click
 Partially Opened
 click
 Full Opened

25

Privacy, Confidentiality, Security, and Authorization

Untangling the Legal Issues

26

Untangling the legal issues

- Four interrelated legal issues
 - Privacy
 - Confidentiality
 - Security
 - Authorization
 - AKA Consent in some circumstances (e.g., HIPAA)
- These are often incorrectly used interchangeably
 - They are not the same!

27

Privacy, Confidentiality, Security, & Authorization

- Each is very different in the eyes of the law
 - Different laws shape the issues for each concept
 - Examples:
 - HIPAA Privacy Rule
 - Doctor-Patient Privilege
 - HIPAA Security Rule
 - The Common Rule regulations on informed consent

28

Privacy

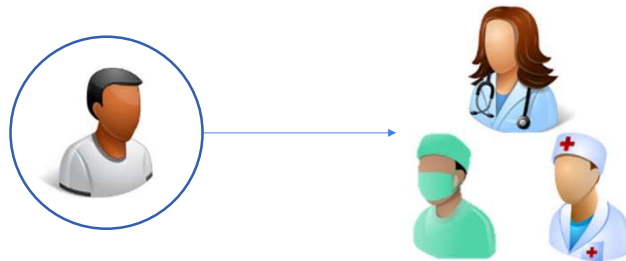
- “[A] set of protections against a related cluster of problems.”
 - Daniel Solove, *Understanding Privacy*
- What sort of problems?
 - Surveillance
 - Insecurity
 - Identification
 - Secondary use
 - Exclusion
 - Aggregation
 - Disclosure



29

Privacy, Cont.

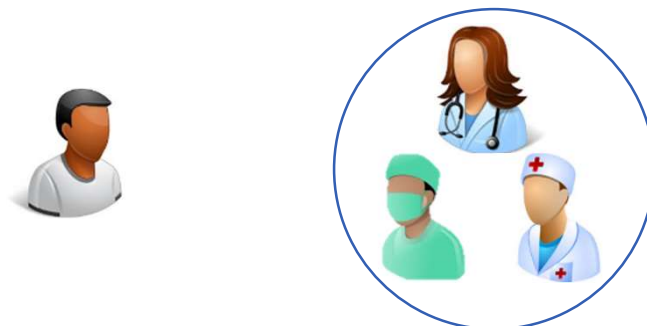
- Privacy protections are held by the patient or customer
- Privacy protections find their origins and parameters in various legal sources, such as:
 - Constitutions
 - Statutes
 - Regulations



30

Confidentiality

- A duty or responsibility that is held by a person that receives information
- Like privacy, the origins and parameters of duties of Confidentiality are found in various legal sources, such as:
 - Constitutions
 - Statutes
 - Regulations



31

Confidentiality, Cont.

- A duty of confidentiality can apply to various entities, including:
 - Doctors
 - Nurses
 - Healthcare facility employees
 - Health department officials
 - Researchers
- A duty may not be explicit in the law
 - Ex: A statute that says information shall be held confidentially might attach a duty of confidentiality to custodians of the information.



32

Security

- Different from Privacy and Confidentiality
 - Privacy = A right conferred by law
 - Confidentiality = a duty of a person or entity
 - Security = a TOOL

33

Security, Cont.

- Two different perspectives:
 - A way to protect the right to privacy of the person giving information
 - A way to maintain the duty of confidentiality of the person receiving information
- Security is increasingly being mandated by law
 - This is especially tricky in the context of rapidly evolving information technology
 - It is difficult to regulate something that is constantly changing

34

Authorization and Consent

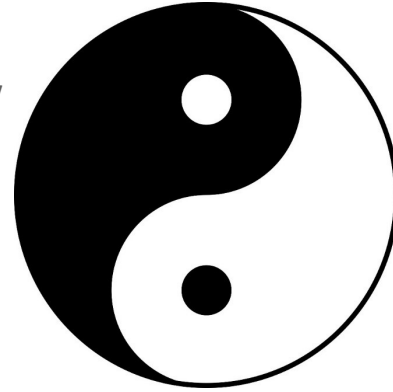
- Authorization and Consent are TOOLS like security
- Tools of
 - Use
 - Disclosure



35

Authorization and Security

- Security is a tool to
 - Possess, store, and maintain
- Authorization and Consent are tools to allow
 - Use
 - Disclosure
 - Sharing



36

Authorization and Consent, Cont.

- Increasingly nuanced
- Contemporary authorizations often have very specific legal origins
 - May be time limited or revocable
- Important relationship with rules of privacy and confidentiality
- “Informed” consent on complicated concepts
 - Communication, language
 - Use more modern technology to better communication of dynamic information
 - Paper form vs live document via tablet
 - Avatar, simulations

37

Knowledge Check - Mix and Match!

- Privacy — A right held by a patient
- Confidentiality — A duty held by a provider
- Security — A tool to protect rights and duties
- Authorization — A tool for use and disclosure

38

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Privacy Rule Primer

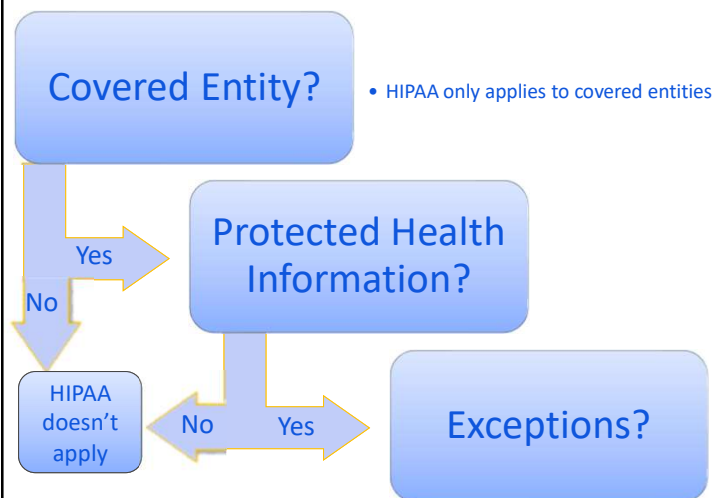
39

HIPAA Privacy Rule: The General Rule

- A covered entity can only use or disclose protected health information for limited purposes unless the individual authorizes the use or disclosure
 - 45 C.F.R. § 164.502 et al.
 - What limited purposes?
 - Disclosure to the individual
 - Disclosures for treatment, payment, or health care operations

40

Basic HIPAA Privacy Rule Flow Chart



41

Knowledge Check

- True or False?
 - HIPAA does not apply to public health authorities unless they perform covered functions (e.g., provide healthcare services).

- TRUE!
 - Public health activities are not covered functions under HIPAA
 - However, a public health authority that performs covered functions can choose to be a hybrid entity or a covered entity

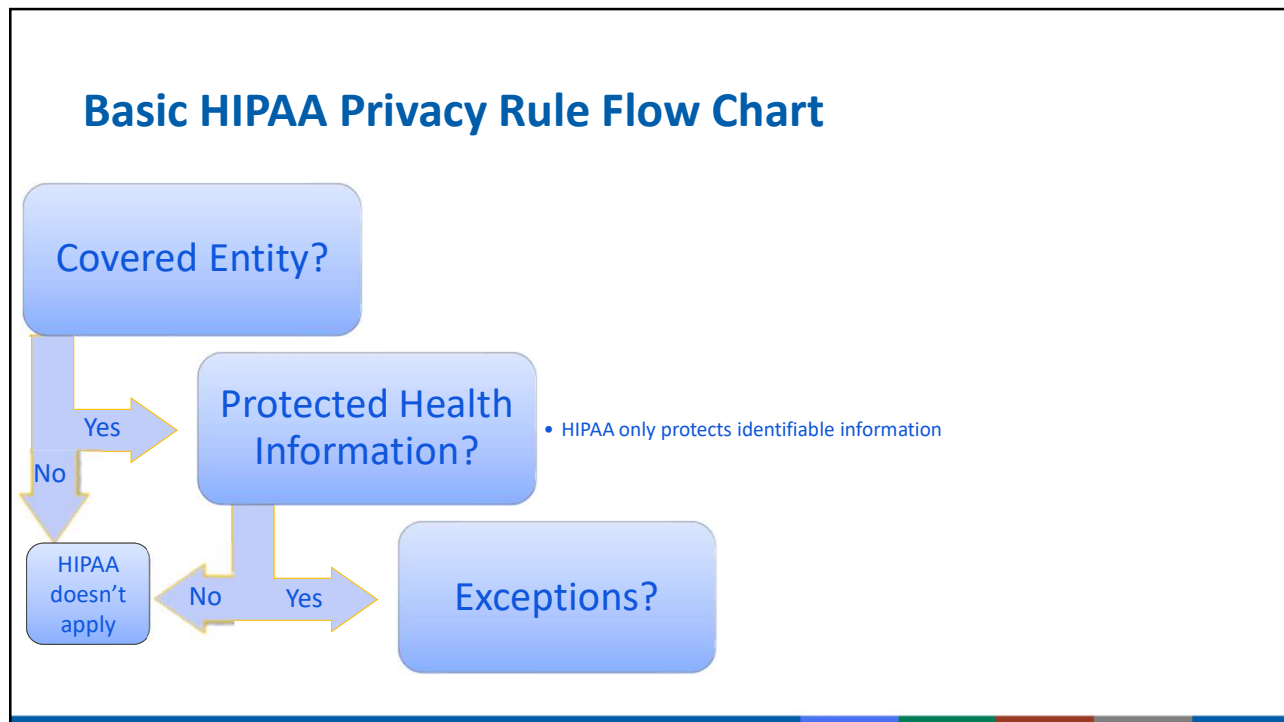
42

State Health Department HIPAA Status (2005)

State	HIPAA Status	State	HIPAA Status	State	HIPAA Status
Alabama	Hybrid	Louisiana	Covered	Ohio	Hybrid
Alaska	Covered	Maine	Other	Oklahoma	Covered
Arizona	Hybrid	Maryland	Hybrid	Oregon	Covered
Arkansas	Covered	Massachusetts	Hybrid	Pennsylvania	Hybrid
California	Covered	Michigan	Hybrid	Rhode Island	Hybrid
Colorado	Other	Minnesota	Other	South Carolina	Hybrid
Connecticut	Hybrid	Mississippi	Covered	South Dakota	Hybrid
Delaware	Hybrid	Missouri	Hybrid	Tennessee	Covered
Florida	Hybrid	Montana	Covered	Texas	Hybrid
Georgia	Covered	Nebraska	Covered	Utah	Hybrid
Hawaii	Hybrid	Nevada	Hybrid	Vermont	Hybrid
Idaho	Hybrid	New Hampshire	Covered	Virginia	Hybrid
Illinois	Hybrid	New Jersey	Hybrid	Washington	Hybrid
Indiana	Hybrid	New Mexico	Covered	Wisconsin	Hybrid
Iowa	Other	New York	Hybrid	West Virginia	Hybrid
Kansas	Hybrid	North Carolina	Hybrid	Wyoming	Covered
Kentucky	Hybrid	North Dakota	Hybrid		

▪ Adapted from: American Public Health Association. (2005). *Public Health Agency Rule Implementation in State Public Health Agencies: Successes, Challenges, and Future Needs* (2005), astho.org (accessed 1/7/2016).

43



44

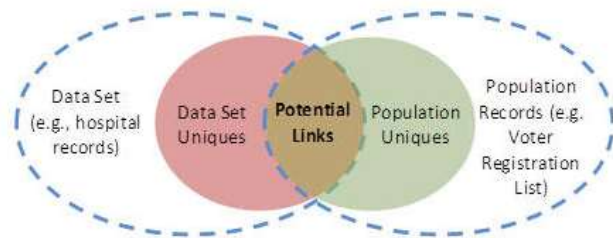
What does HIPAA protect?

- Individually identifiable health information
 - Is created or received by a covered entity; and
 - Relates to the health of an individual; and
 - Identifies the individual; or
 - Reasonable to believe information can be used to identify the individual.
- Protected health information
 - Individually identifiable health information that is transmitted or maintained in any form or medium
 - Some exclusions apply

45

De-identification Methods

- Why de-identify?
 - Information that is not identifiable is not HIPAA protected
- Methods
 - Statistical De-identification (Expert Opinion)
 - Re-identification risk is “very small”
 - Might depend on anticipated recipient
 - “Safe Harbor” De-identification
 - Exclude list of 18 identifiers
 - No actual knowledge
- Aggregate data
 - Not individually identifiable



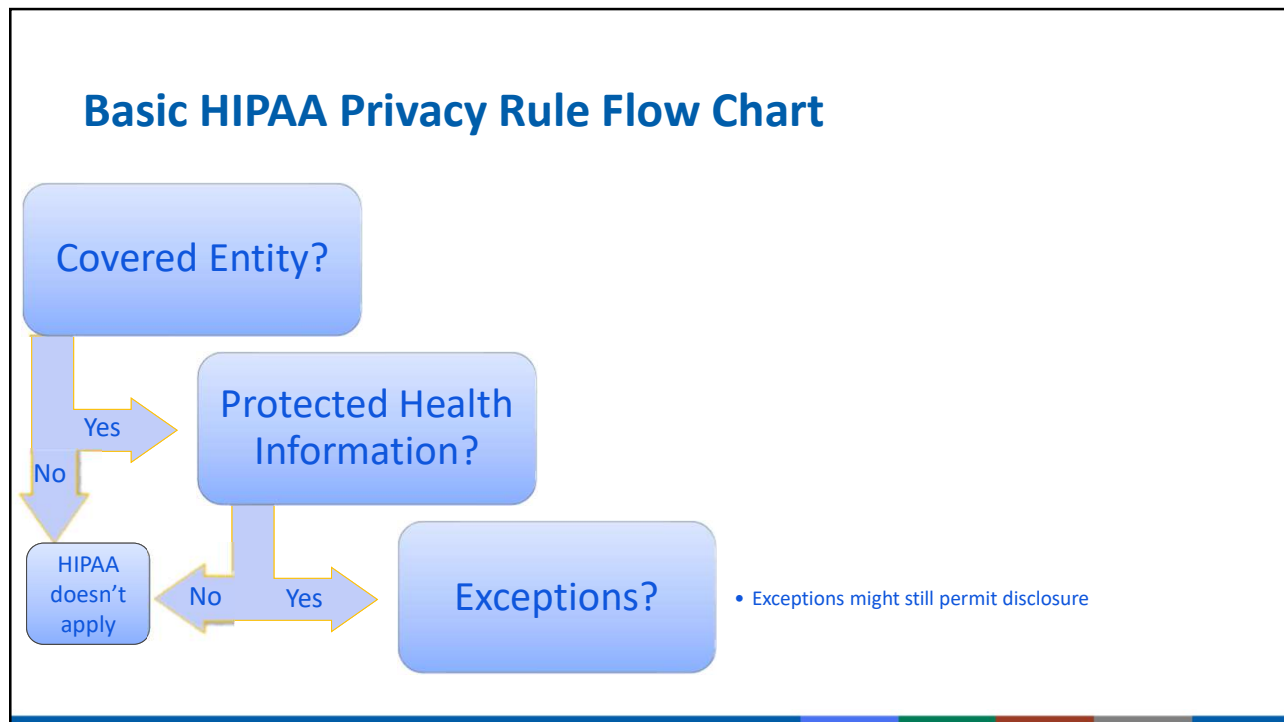
▪ Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, <http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard>

46

Knowledge Check

- True or False?
 - De-identified health information can be disclosed under HIPAA even if no disclosure exceptions apply.
- TRUE!
 - HIPAA does not protect de-identified health information.
 - No exceptions needed!

47



48

Important!

- Many HIPAA provisions allow the use and release of protected health information!!!

49

Important HIPAA Disclosure Exceptions

- No requirement for authorization or opportunity to object for:
 - Public health activities
 - PH authority authorized to collect information
 - i.e., state and local legal authorities
 - Other entities
 - Research
 - IRB or Privacy Board approval for Waiver
 - IRB must follow Common Rule
 - Others
 - E.g., uses and disclosures required by law, for law enforcement activities, health oversight activities



50

Scope of HIPAA Disclosures

- Minimum Necessary
- Limited Data Set

51

Limited Dataset v. Minimum Necessary

- **Limited Data set Disclosure**
 - A specific type of disclosure
 - Specific data elements are excluded
 - Permitted uses:
 - Research
 - Public health
 - Health care operations
 - Requires a Data Use Agreement
- **Minimum Necessary Standard**
 - Standard for many permitted HIPAA disclosures
 - Get what you need
 - *Including data elements that would be excluded from a Limited Dataset disclosure*
 - Reasonable effort
 - Covered entity may rely (if reasonable) on PH official's representations

52

Knowledge Check

- HIPAA permits the following disclosures for public health purposes without patient authorization:
 - A) A disclosure of the minimum data necessary for the public health use
 - B) A disclosure of a limited data set for the public health use
 - C) All of the above

Answer: C

Remember!

- The minimum necessary and limited data set standards are different.
- Either standard might allow disclosure of information the other does not!

53

Limited Dataset v. "Safe Harbor" De-identification

Prohibited Data for "Safe-harbor" De-identification	Prohibited Data in Limited Dataset
Names	Names
Telephone #	Telephone #
Fax #	Fax #
Email	Email
SSN	SSN
Medical record #	Medical record #
Health plan beneficiary #	Health plan beneficiary #
Account #	Account #
Certificate/license #	Certificate/license #
Vehicle identifiers	Vehicle identifiers
Device identifiers and serial #	Device identifiers and serial #
Web URLs	Web URLs
IP address #	IP address #
Biometric identifiers, including finger and voice prints	Biometric identifiers, including finger and voice prints
Full face photographic images	Full face photographic images
All geographic subdivisions < State	Postal Address (other than city, state, and zip)
Dates (except year)	
Other unique identifying #, characteristic, or code	
No <u>actual</u> knowledge information is re-identifiable	

54

Data Use Agreements

Legal Tool for Disclosing Health Data

55

Data Use Agreements (DUA)

- Formal written agreements between two or more parties
- Tools to
 - Constrain use of data after it has been disclosed
 - Constrain additional disclosure
 - Ensure rights and obligations are maintained
 - Parties (e.g., CDC, Health Departments, Healthcare providers)
 - Stakeholders (e.g., patients)

56

When should you consider a DUA?

- Whenever you want to disclose data, and
 - You are concerned about the future use and disclosure of your data
 - You are required by law to enter a DUA to disclose the data
 - E.g., A limited data set disclosure under HIPAA
- DUA's are not required for every disclosure
 - E.g., Public health disclosures for outbreak response
 - Unnecessary DUA negotiations may delay necessary response

57

Contents of a Limited Data Set DUA

- Establish
 - Permitted uses and disclosures of the data
 - Who is permitted to use or receive the data
- Provide that data recipient will
 - Not use or disclose data other than permitted by DUA or required by law
 - Use appropriate safeguards
 - Report unauthorized disclosures
 - Ensure any agents to whom the recipient provides the data agree to the same restrictions and conditions
 - Not identify the information or contact the individuals

45 C.F.R. § 164.514(e)(4)(ii)

58

Knowledge Check

- True or false?
 - Covered entities need DUAs for all PHI disclosures under HIPAA

- FALSE
 - Many HIPAA disclosures do not require a DUA. However, disclosures of a limited data set require parties enter into a DUA.

59

Limited Data Set DUA Activity

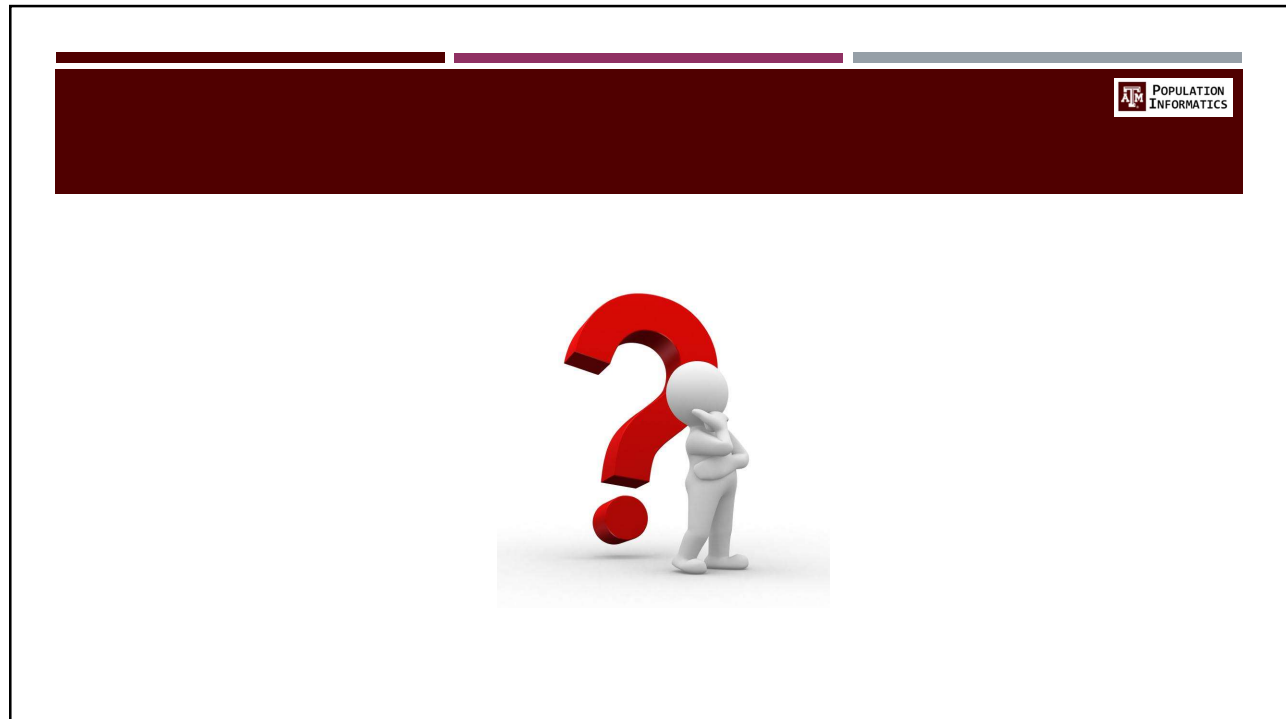
- Task: Identify the following terms of the example DUA
 - A. Permitted uses and disclosures of the data
 - B. Who is permitted to use or receive the data
 - C. No use or disclosure other than permitted by DUA or required by law
 - D. Use of appropriate safeguards
 - E. Reporting of unauthorized disclosures
 - F. Application of DUA to other entities whom the recipient provides the data
 - G. No identification of the individuals or contact of the individuals

60

Definitions

- Privacy
- Confidentiality
- Security
- Accountability
- Authorization/Consent
- PHI
- Limited Data
- DUA
- Etc...

61



62



The logo for ATM Population Informatics, featuring the letters 'ATM' in a stylized font next to the words 'POPULATION INFORMATICS'.

Remaining Agenda

- Grades & feedback: upto assignment 4
 - Assignment 5: tomorrow
 - Assignment 6: by wed
- Break: Read assignment 7
- Midterm Q&A
- Privacy lecture

63

63





Midterm

- A cumulative mid-term exam
- covering lecture (ppt on website), reading, and assignments & labs
- In class (2h): 70 ~ 90 questions
 - Part 1: e-campus
 - Multiple choice
 - T/F
 - Short answer
 - Part 2: Matching - download and upload from e-campus
- Open textbook & notes (from assignment 7)
- What you need
 - Camera & sound, on zoom
 - Quite room
 - Get on E-campus

64

64



Next week

- Assignment 7: Review notes
- In class midterm

66

66