Privacy of Electronic Health Information

IEEE Madison Section
March 17, 2011

Kenneth G. Hartman, CISSP, CPHIMS

Biography

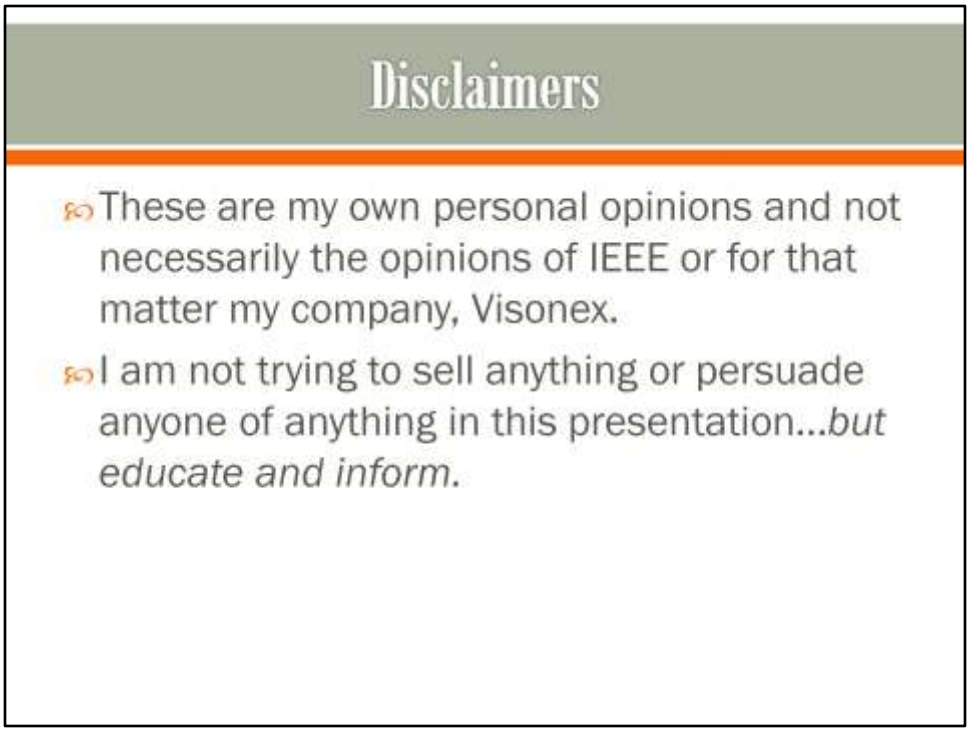
Since 2002, Kenneth Hartman has served as the Chief Security & Privacy Officer for Visonex, LLC a healthcare informatics company based in Green Bay, WI. In this capacity, Ken is responsible for all aspects of assuring the security and privacy of both the company's internal IT systems and the company's SaaS offerings.

Prior to coming to Visonex, Ken worked as a corporate Electrical Systems Manager for Kraft Foods where he helped to secure the plant floor automation systems. Ken holds a BS Electrical Engineering from Michigan Technological University and holds the Certified Information Systems Security Professional (CISSP), and the Certified Professional in Healthcare Information Management Systems (CPHMIS) credentials.

Recently, Ken became a mentor for the *SANS® +S™ Training Program for the CISSP® Certification Exam*. This course helps Madison area security professionals achieve their CISSP certifications.

www.KennethGHartman.com

www.linkedin.com/in/kennethghartman



I am not a privacy advocate, per se…but I am thankful for those that are.

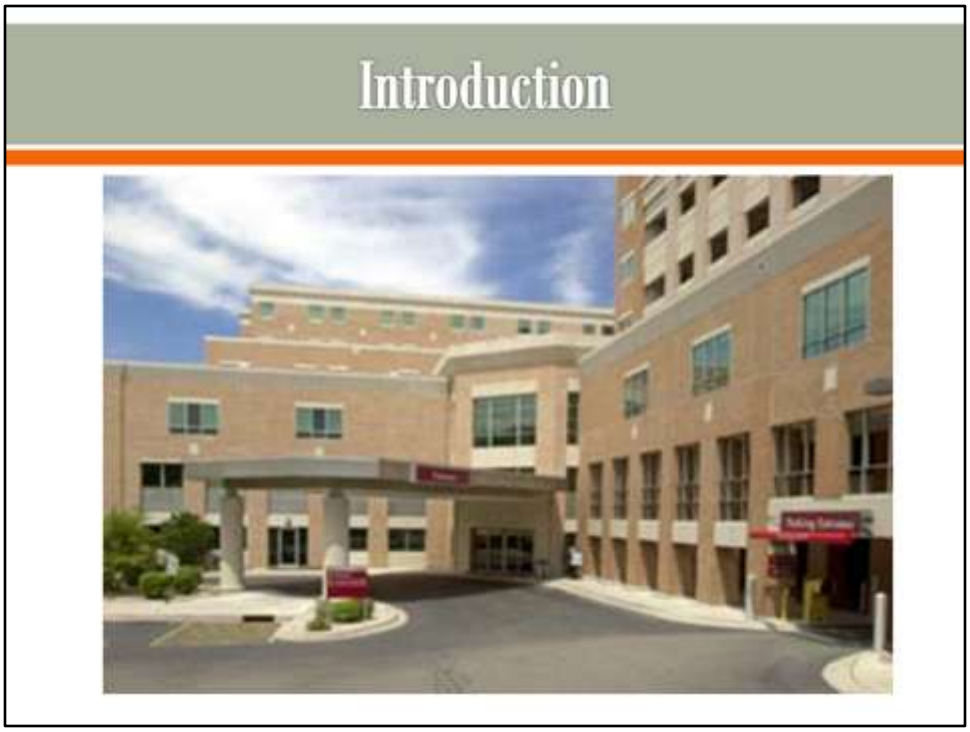
After all…I am not only a privacy and security officer…I am also a patient

There is lots of work going on right now in the area of privacy and my goal with this presentation is to provide you with various perspectives, insights, resources and information about where to learn more information

I am well aware that this is a very controversial topic, and while some of the material may be provocative, if you listen with an open mind, I think that privacy concerns CAN be addressed to the satisfaction of those concerned.

Agenda

- Privacy Concerns
- Attitudes About Privacy
- Understanding "Trust"
- HIPAA Privacy Rule
- HITECH Act
- Disclosure Accounting
- Breach Notification
- Health Information Exchange
- ONC Tiger Team
- Consent Framework



In preparation for this talk, I contemplated what makes people so concerned about the privacy of **their** medical records?

Then I asked myself…"what makes **me** so concerned about the privacy of **my** medical records?"

Next, I wondered…are my concerns the same as everyone else's concerns?...after all, I am a professional in the field of Healthcare Informatics

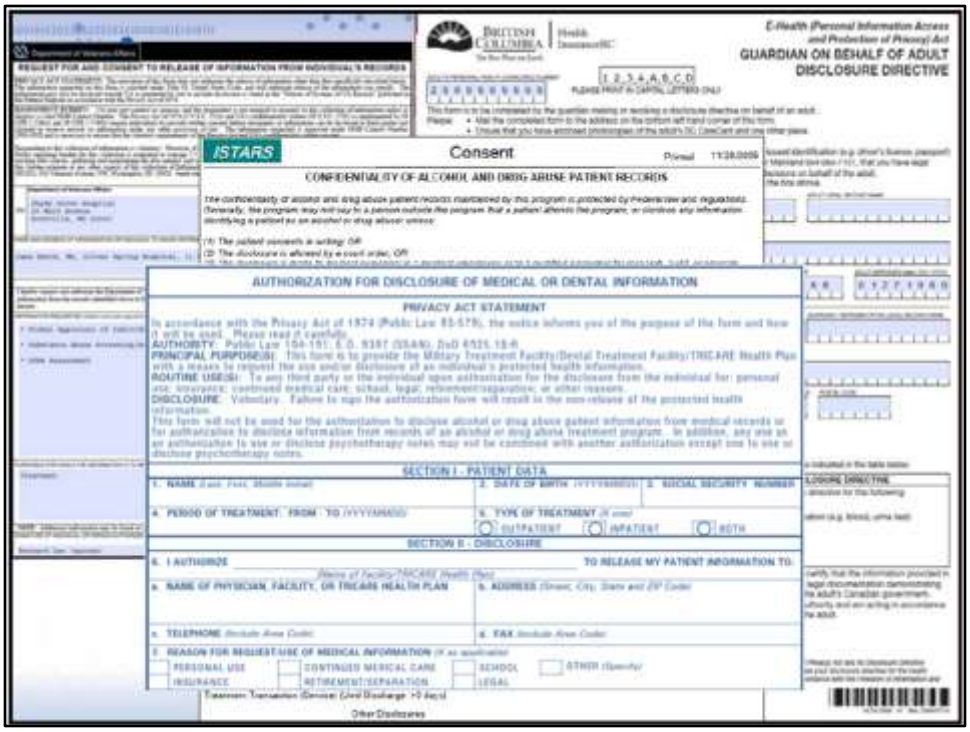
---

SCENARIO

The typical visit to the Doctor's office

You are given a "Notice of Privacy Practices" and typically asked to sign a form

And then you go sit in the waiting room, and flip through magazines…



REQUEST FOR AND CONSENT TO RELEASE OF INFORMATION FROM INDIVIDUAL'S RECORDS

E-Health (Personal Information Access and Protection of Privacy) Act

GUARDIAN ON BEHALF OF ADULT DISCLOSURE DIRECTIVE

ISTARS

Consent

CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE PATIENT RECORDS

AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION

PRIVACY ACT STATEMENT

SECTION I - PATIENT DATA

SECTION II - DISCLOSURE

So is the March 21st issue (2011) of Time Magazine supposed to make you feel better?

Hmm….Maybe I will read the paper

University of Iowa formally reports breach of football players' privacy

Associated Press
Updated: 03/01/2011 10:54:25 AM CST

IOWA CITY, Iowa — The U.S. Department of Health and Human Services says it will be up to the agency's Kansas City office to decide whether to investigate a breach of medical records involving hospitalized members of the University of Iowa football team.

The university on Monday formally reported the breach to the department, which is in charge of enforcing medical privacy laws. The university announced last month three employees were fired and two were suspended for accessing the records of players who were getting treatment for an unusual muscle disorder.

Rachel Seeger, spokeswoman for the agency's Office of Civil Rights, confirmed the university reported the incident. She said its regional offices determine whether to open an investigation.

UI spokesman Tom Moore says he is not expecting the hospital to face any additional consequences.

Snooping Tucson Hospital Workers Fired In Records Breach

by SCOTT HENSLEY

Just about everyone we know is fascinated by the remarkable medical saga unfolding at University Medical Center in Tucson, Ariz.

Chris Morrison/AP

The flag of the state of Arizona flies at half-staff outside University Medical Center in Tucson, Ariz., on Jan. 8.

Since last Saturday's tragic shooting, we've been hanging on every detail about Rep. Gabrielle Giffords' condition and the status of the dozen other people injured. At a Friday media briefing, neurosurgeon G. Michael Lemole Jr. said of Giffords, "We're very encouraged she's making all the right moves."

But some workers at the hospital have let their curiosity get the best of them. Earlier this week, management at University Medical Center fired three employees and let go a nurse working for a contractor because they'd snooped on confidential computerized medical records of patients injured in the shooting.

The hospital released a statement late Wednesday, saying the people violated a "zero tolerance policy on patient privacy violations." The hospital notified the patients' families about the breach and said nothing from the records appears to have been made public.

Zero Tolerance – Healthcare systems make a public statement when they fire employees for medical records snooping to emphasize that they DO TRACK and MONITOR Health records access

Furthermore, it is a well known technique to create fake records that will only be accessed by those who are snooping

Remember these users are <u>trusted staff</u> who have who are abusing their access level because they are accessing patients that they are not assigned to

Source: http://www.npr.org/blogs/health/2011/01/14/132928883/snooping-tucson-hospital-workers-fired-in-records-breach

Besides Medical Records Snooping there is also a well known epidemic of Identity theft…

The World Privacy Forum has a 56 page whitepaper called "*MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You"* at the URL listed on this page.

It is a very interesting discussion of the problem as well as how to detect and prevent Medical Identity Theft

This report cites some specific examples of Medical Identity Theft:

- A Boston area psychiatrist made false entries in charts of individuals who were not his patients. He gave individuals diagnoses of drug addiction and abuse, severe depression and numerous psychiatric sessions which they did not actually have, then used their personal information to submit false bills to insurance. The victims, after learning of the crime, had difficulties getting the false information removed from their medical files. One woman told an investigator that she "is concerned about obtaining future health insurance coverage … because her husband is self-employed."
- Another non-patient of the same Boston psychiatrist discovered that his medical record had been falsified to include numerous psychiatric sessions that did not occur and false diagnoses of severe depression. He discovered the false diagnoses after he had applied for employment.
- A Pennsylvania man discovered that an imposter used his identity at five different hospitals to receive more than $100,000 worth of medical treatment. At each

hospital, the imposter created medical histories in the victim's name.

***Make sure that you review your medical record AND ask for an accounting of the disclosures

Next, I will discuss two recent research studies about patient's attitudes about privacy and then after that I will unpack some important concepts regarding trust that have an important relationship to our individual attitudes about privacy.

Before I present information about the two research, I want to take a minute to share a concept that I recently read:

"Take note when something occurs that bothers you and ask yourself why you are upset. Chances are one of your values is being violated."
---from the book "Career Distinction" by William Aruda & Kirsten Dixon

Journal of Medical Internet Research

Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study

Journal of Medical Internet Research - 6-8-2009
www.jmir.org/2009/3/e30/

Study Results

Three dominant themes emerged:

1. concerns about privacy and security,
2. the potential benefit to a person's health, and
3. the desire for more information about the consent process.

On the pre-discussion questionnaire, 55 out of 62 participants (88%) **indicated that they would provide consent** for their information to be shared electronically among their health care providers, given the materials they had reviewed.

http://www.jmir.org/2009/3/e30/

Conclusions

- Patients are enthusiastic about electronic health information exchange, recognizing its capacity to improve the quality and safety of health care;
- **However, they are also concerned about its potential to result in breached privacy and misuse of health data.**
- As the exchange of electronic health information becomes more widespread, policy makers will need to ensure that patients have access to concise educational materials and opportunities to engage in conversations about the risks and benefits of participation.

http://www.jmir.org/2009/3/e30/

NORC at University of Chicago Research

"New Study: Seventy-Eight Percent of Americans Favor Electronic Medical Records; Sixty-Four Percent Say Benefits Outweigh Privacy Concerns"

January 31, 2011 Press Release

www.norc.uchicago.edu/News/HIT+Release+2011Jan31.htm

Reading from the press release….

Moreover, individuals with lower income and those who have less familiarity with electronic technology have less favorable attitudes towards health IT. This implies that some of the populations that are most likely to benefit from health IT may be least open-minded about it.

"Our core finding is that a large majority of Americans support use of health IT to improve health care and safety, and reduce costs**, which suggests that government and industry efforts to increase the effectiveness and use of health IT are generally consistent with the public's wishes**" said Dan Gaylin, NORC's Executive Vice President for Research, and the lead author of the study. "But there is still room for efforts to demonstrate the advantages of health IT among some important demographic groups."

Next, I want to discuss the concept of "Trust"

Trust involves risk –the risk that the people that we trust will pull through for us. If it were absolutely certain, there would be no risk…and no reason to trust.
When we trust others, we risk losing the things that we entrust to others…which can be shattered by the betrayal of our trust.

Trust is required for most human interactions, but especially the purchase of a service, because you trust that the service that you are buying will be worth the value that you have paid.

ChangingMinds.org says this about trust:

- "Trust is both an emotional and a logical act.
- Emotionally, it is where you expose your vulnerabilities to people, but believe they will not take advantage of your openness.
- Logically, it is where you have assessed the probabilities of gain and loss…and concluded that the person in question will behave in a predictable manner"

The thoughts on this slide come from the website "Changing Minds.org" in an article called "What is Trust?"

Predictability

- We are constantly forecasting and creating internal models of the world based on our experiences and social programming
- We need to make plans and take actions to achieve our longer term goals
- We are also doing risk assessments based on threats that we identify

Value Exchange

- Exchange is the basis for all human relationships
- I'll swap you $2 a Grande cup of Starbuck's Coffee
- Trust in value exchange is required because we do not know fully whether what we are receiving is what we expect
- If I buy a used car, I do not want to buy a car that the seller know is a lemon

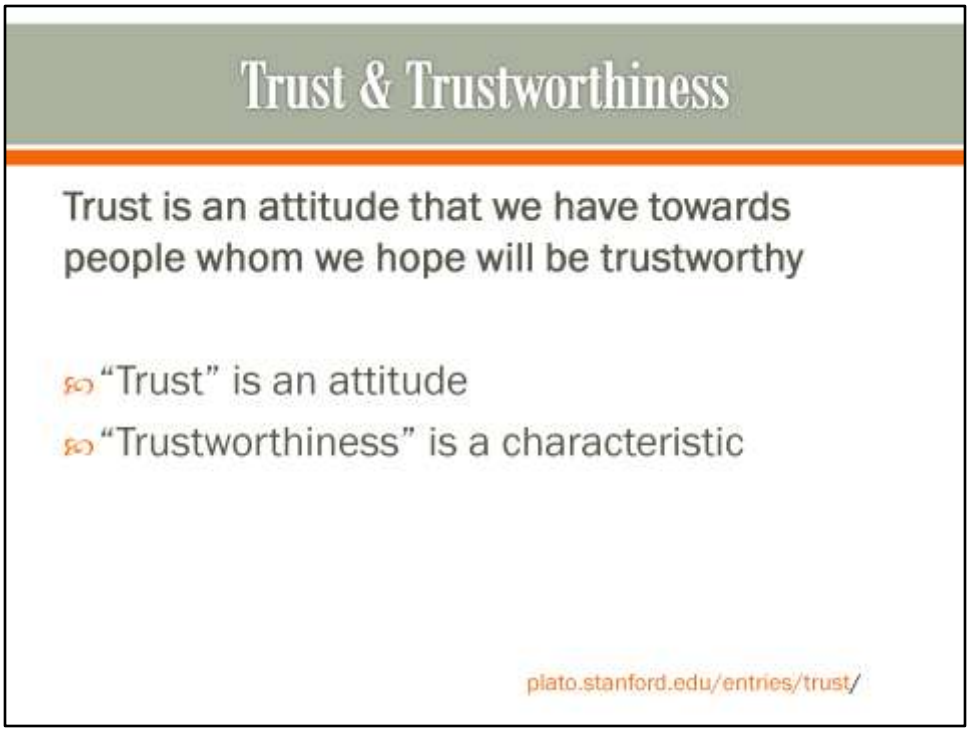
Delayed Reciprocity

- Something given now, but the return is paid back in the future
- The delay in the value exchange creates additional uncertainty

Exposed Vulnerabilities

- We may also expose ourselves in a way that they can take advantage of our

vulnerabilities



Trust is an attitude – the parties to a relationship must have attitudes toward each other that permit trust

Trustworthiness is a characteristic – both parties to a relationship must be trustworthy

Therefore the "risk assessment" we make when deciding to trust someone is based on determinations of their trustworthiness and their attitudes about trust

***These thoughts are from the **Stanford Encyclopedia of Philosophy**

Vulnerability to Betrayal

- people who monitor and constrain other people's behavior and do not allow them to prove their own trustworthiness may rely on others, they do not trust them.
- For, while their reliance could be disappointed, it could not be betrayed.
- Consider that one can rely on inanimate objects, such as alarm clocks; but when they break, one is not betrayed, although one may be disappointed.
- Reliance without the possibility of betrayal is not trust.
- Thus, people who rely on one another in a way that makes betrayal impossible do not trust one another.

Think Well of Others

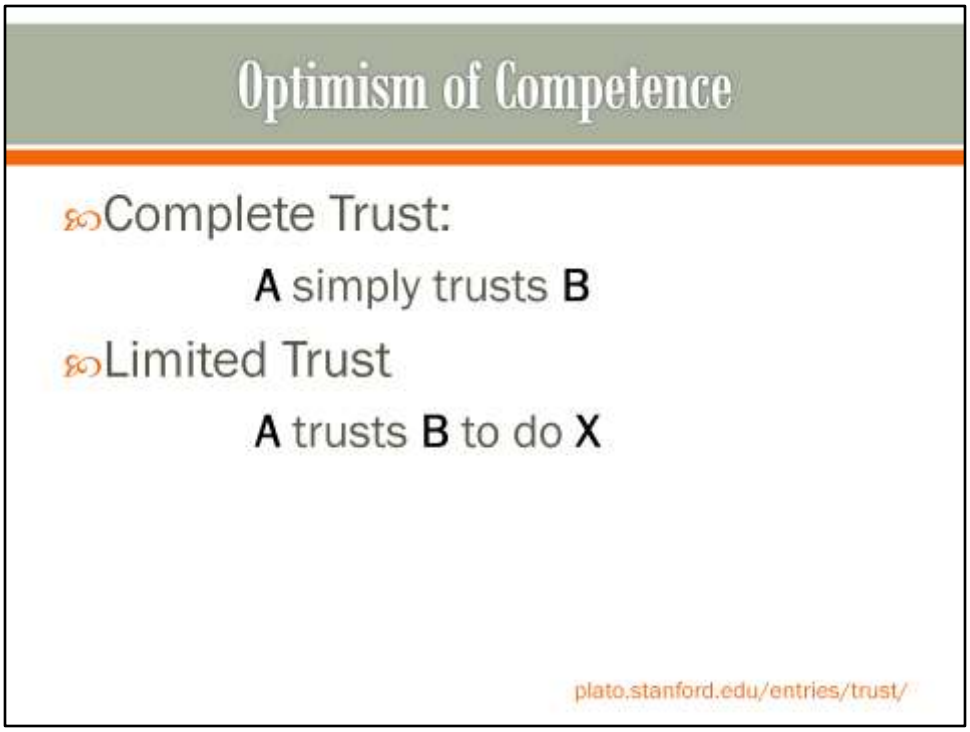
- People also do not, or cannot, trust one another if they are easily suspicious of one another
- **If one assumes the worst about someone--then one distrusts, rather than trusts the person**
- trust involves being optimistic, rather than pessimistic, that the trustee will do something for us (or for others perhaps), which is in part what makes us vulnerable by trusting

Optimistic that they are competent

- Failing to be optimistic about people's competence also makes trust impossible.
- Without being confident that people will display some competence, we cannot

trust them.

- **We usually trust people *to do* certain things—for example, to look after our children, to give us advice, or to be honest with us**
- **but we would not do so if we thought they had none of the relevant skills (including moral skills of knowing what it means to be honest or caring.)**



Rarely, if ever, do we trust people completely (i.e. A simply trusts B).

Instead, "trust is generally a three-part relation: A trusts B to do X"

To have trust in a relationship, therefore, **we do not have to assume that the other person will be competent in *every* way**.
Optimism about the person's competence in at least one area is essential, however.

- I trust my pediatrician to treat my sick child but not to manage my retirement account, and
- I trust my financial planner to manage my retirement account but not to treat my sick child

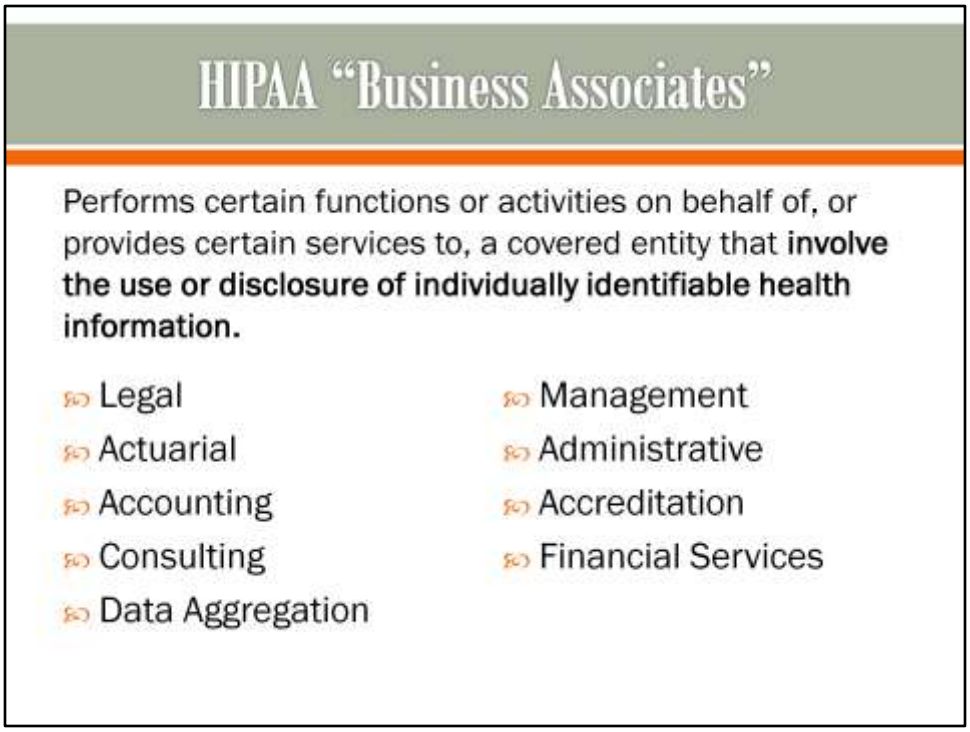
Keep this concept of "Limited Trust" in mind…as we will come back to it. But first, we need to shift gears and discuss some legislation

HIPAA Privacy Rule

HIPAA Privacy Rule

- The Privacy Rule standards address the use and disclosure of *Individually Identifiable Health Information*
  - "protected health information" or "PHI"
- *"Assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."*
- Published: December 28, 2000
- Final Modifications: August 14, 2002.

Health care clearinghouses include billing services, repricing companies, community health management information systems, and other entities that perform clearinghouse functions.



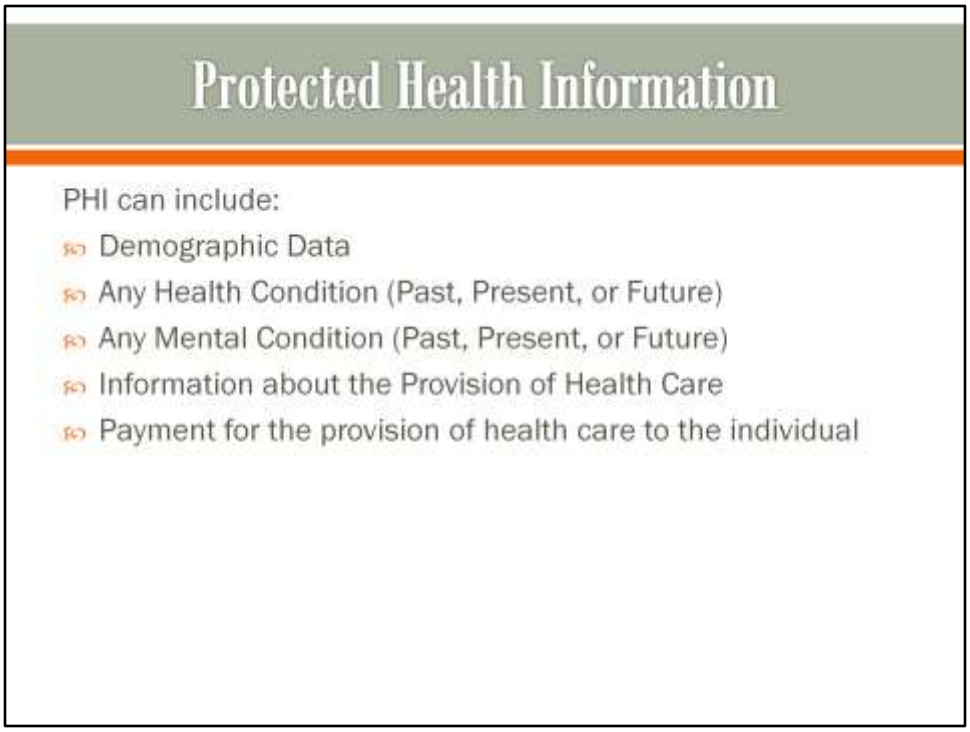
Business Associates, by definition handle PHI

A "Business associate" functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.

A covered entity can be the business associate of another covered entity.

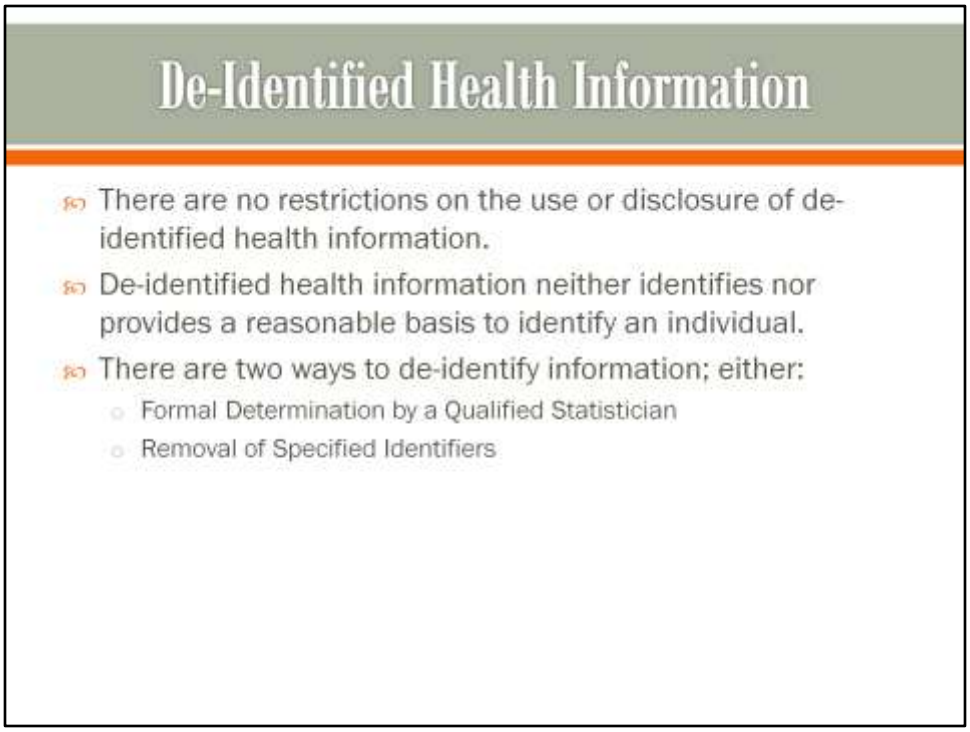
In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.

Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the HIPAA Privacy Rule.



Individually identifiable health information => Protected Health Information

Any medical or demographic data that identifies the individual or for which "**there is reasonable basis could be used to identify the individual"**



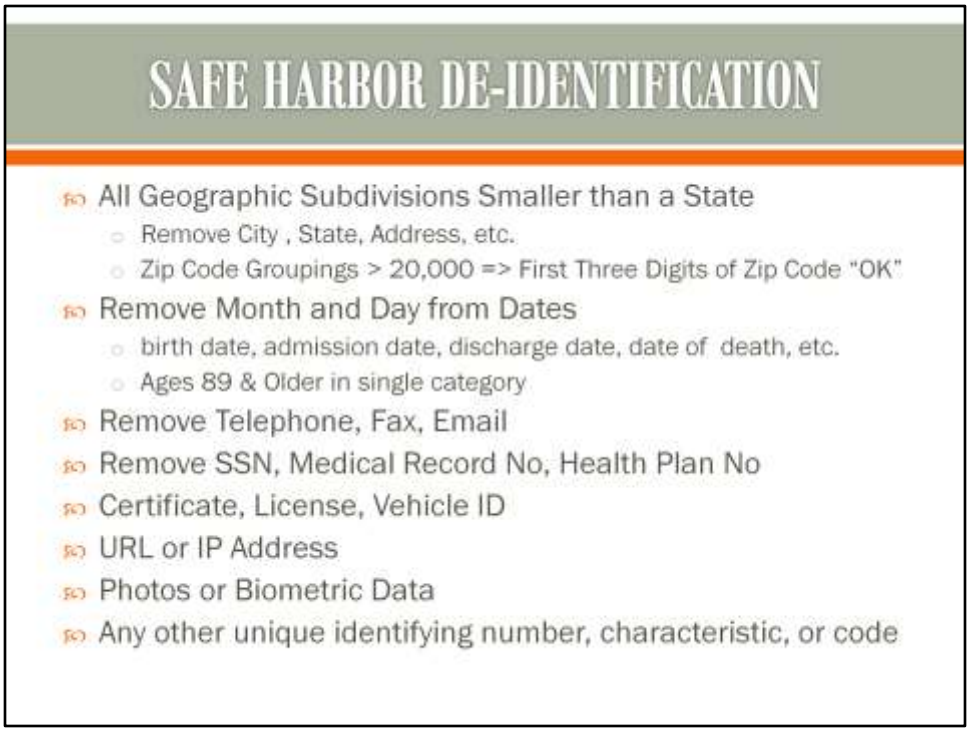
The formal determination by a qualified Statitician is a

"A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable"

- 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;
- Documents the methods and results of the analysis that justify such determination"

SAFE HARBOR RULE
the removal of specified identifiers of

- the individual
- the individual's relatives
- household members
- and employers



The information could be used alone or in combination with other information must not allow identification of an individual who is a subject of the information.

For example, a patient who is 104 on dialysis in a specific county can be re-identified to medical records from that county if the age was left in the record set

Written Consent is not Needed For:

1. The Individual

2. Treatment, Payment, and Operations is discussed in the next slide

3. Uses and Disclosures with Opportunity to Agree or Object
- i.e. Facility Directory
- A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends. ←Well wishers calling during a hospital stay
- or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care. ← i.e. Spouse
- This allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient.
- Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death.

4. Incident to an Otherwise Permitted Use & Disclosure

5. Public Interest & Benefit
- Judicial & Administrative Proceedings
- **Required by Law – Statute, Regulation, and Court Orders**
- **Victims of Abuse, Neglect, or Domestic Violence**
- Health Oversight Activities ← For Example a Hospital Accreditation Board (JAHCO)
- Organ Donations
- **Serious Threat to Health or Safety**
- Essential Government Functions
- Workers' Compensation.

A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.

Obtaining "consent" for TPO is optional under the HIPAA Privacy Rule ←But MOST providers do

The content of a [WRITTEN] consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

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

NOTE: De-Identified Data is no longer PHI, so no limitations on it (YET!)

privacyruleandresearch.nih.gov/healthservicesprivacy.asp
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/research.html

Written Authorization Required

- Anything Other than TPO & Other Permitted Disclosures
- Examples:
  - Disclosures to a Life Insurer for Coverage Purposes
  - Disclosures to an Employer for Pre-Employment Drug Test
- Must be in Plain English
- Patient Has Right to Revoke

Minimum Necessary Use

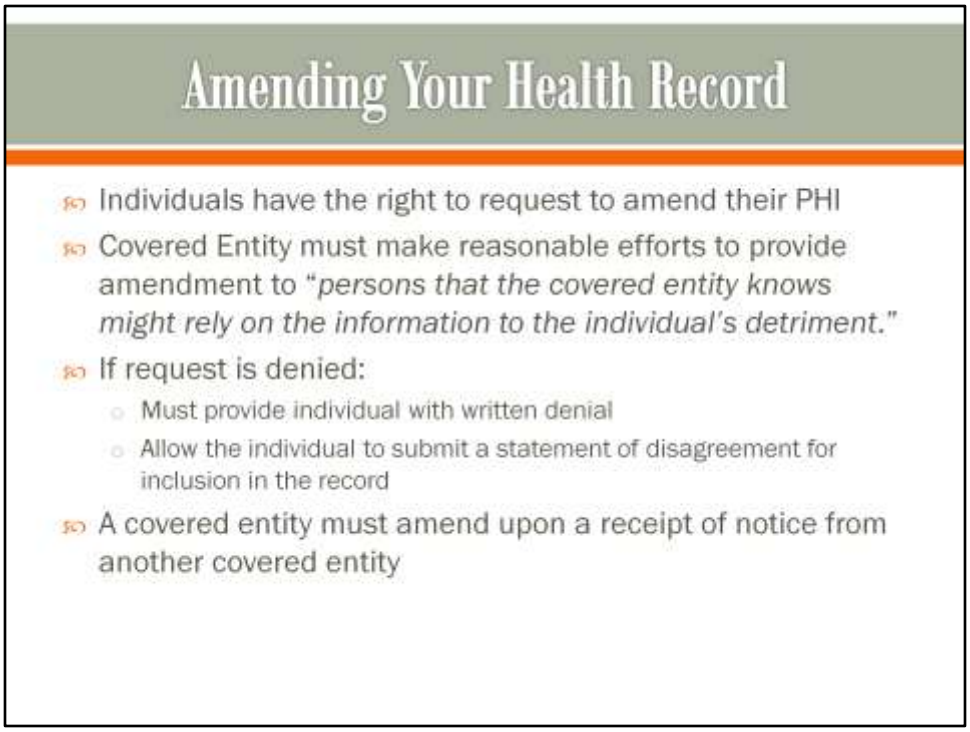
- A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.
- A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary.

Access to Your Health Record

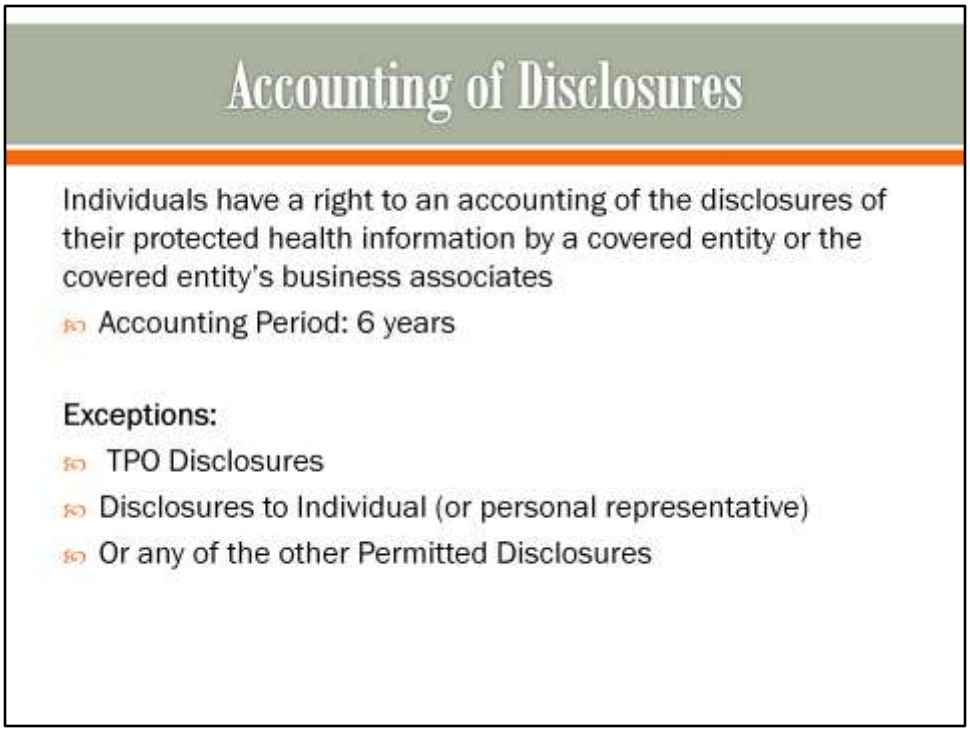
- Except in certain circumstances, individuals have the right to review and obtain a copy of their PHI in a covered entity's **designated record set.**
- Response within 30 Days
- Covered entities may impose reasonable, cost-based fees for the cost of copying and postage

Designated Record Set

- The group of records maintained by a covered entity to make decisions about individuals,
- A provider's medical and billing records about individuals
- A health plan's enrollment, payment, claims adjudication, and case or medical management record systems.



Amendment. The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete.



The maximum disclosure accounting period is the six years immediately preceding the accounting request

There are exceptions that do not need to be accounted for. These were discussed a few slides back as "Permitted Disclosures"

1. To the Individual;
2. Treatment, Payment, and Health Care Operations;
3. Uses and Disclosures with Opportunity to Agree or Object; (Facility Directories, etc)
4. Public Interest and Benefit Activities; and
5. Limited Data Set for the purposes of research, public health or health care operations.

Privacy Policies and Procedures. A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.

Privacy Personnel. A covered entity must designate a privacy official responsible for
- developing and implementing its privacy policies and procedures
- receiving complaints and
- providing individuals with information on the covered entity's privacy practices

A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.

Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or ***its business associates*** in violation of its privacy policies and procedures or the Privacy Rule.

Data Safeguards. A covered entity must maintain reasonable and appropriate ***administrative, technical, and physical safeguards*** to *prevent intentional or unintentional* use or disclosure of protected health information in violation of the Privacy Rule

All Records must be maintained for SIX years:

- its privacy policies and procedures,
- its privacy practices notices,
- disposition of complaints,
- And anything else that the Privacy Rule requires to be documented.

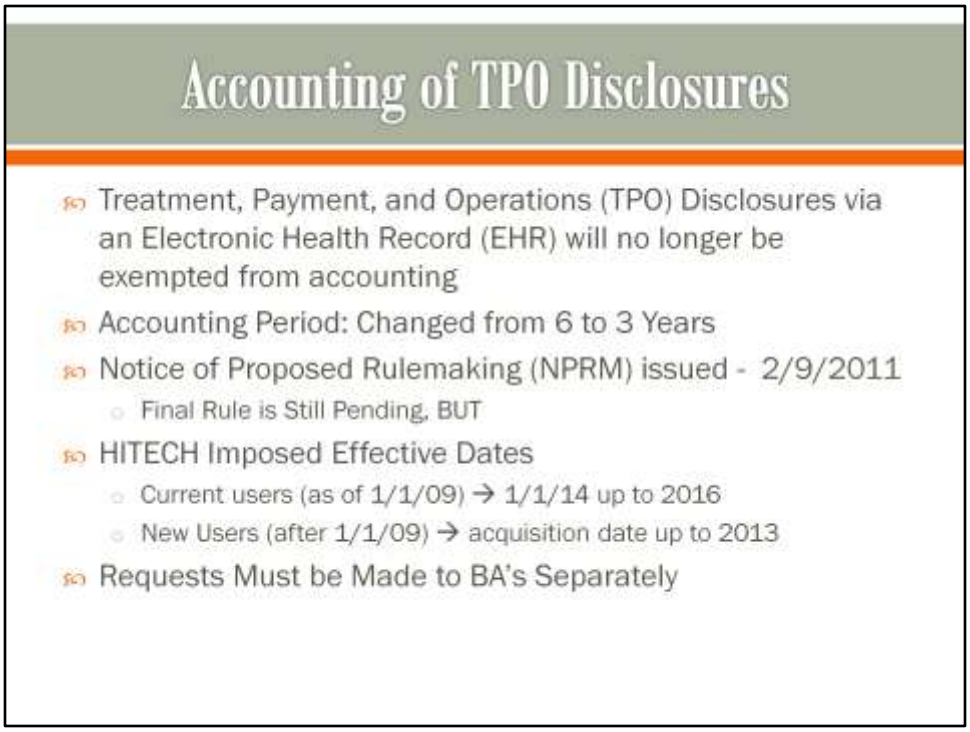
Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of ARRA included many important changes in Privacy of Health Information

Date of Enactment: February 17, 2009

Previously, if a Business Associate breached privacy, all a Covered Entity could do was terminate the contract

Now, the Business Associate has Direct Liability & Responsibility for a Breach

Source:
http://www.hipaa.com/2009/02/arras-hitech-privacy-provisions-apply-hipaa-security-rule-to-business-associates/



Also Note that the HIPAA Security Rule already requires logs to be generated and reviewed as to who access what PHI in a Electronic Health Record

http://blogs.hcpro.com/hipaa/2011/02/ehr-accounting-of-disclosures-rule-close-to-publication/
http://www.hipaasurvivalguide.com/hitech-act-13405.php

Other Provisions

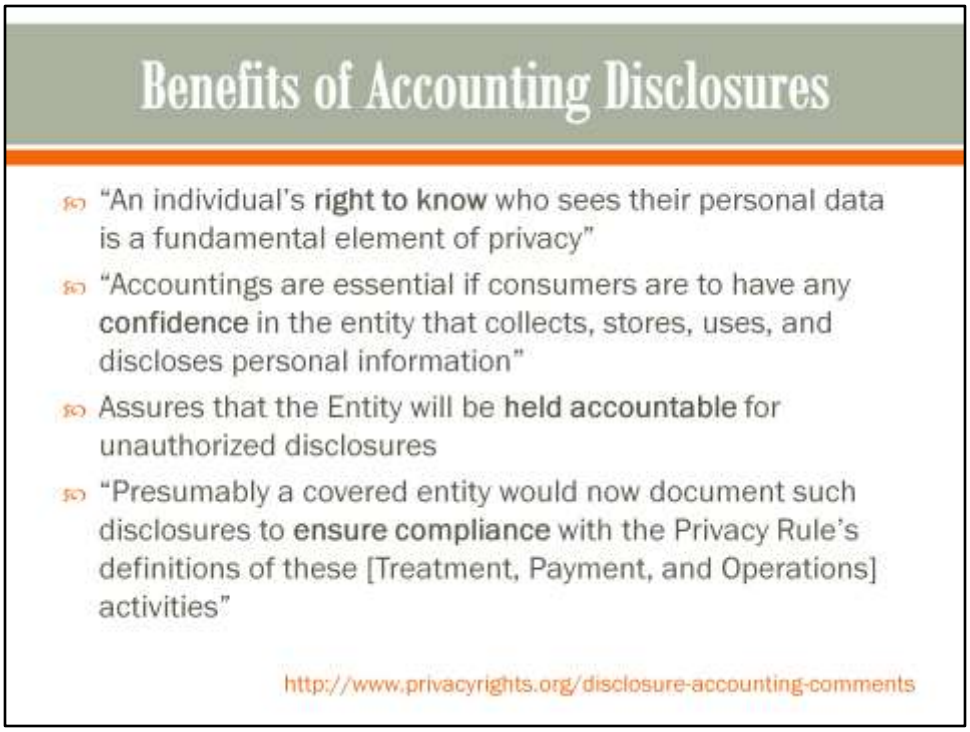
- Clarifications on the Limited Data Set (Research)
- Prohibition on the Sale of Health Records or PHI
- Breach Notification
- Clarifications on use of PHI for Marketing & Fundraising
- Wrongful Disclosures Criminal Penalties
- Clarifies Enforcement

Health Information Privacy Education

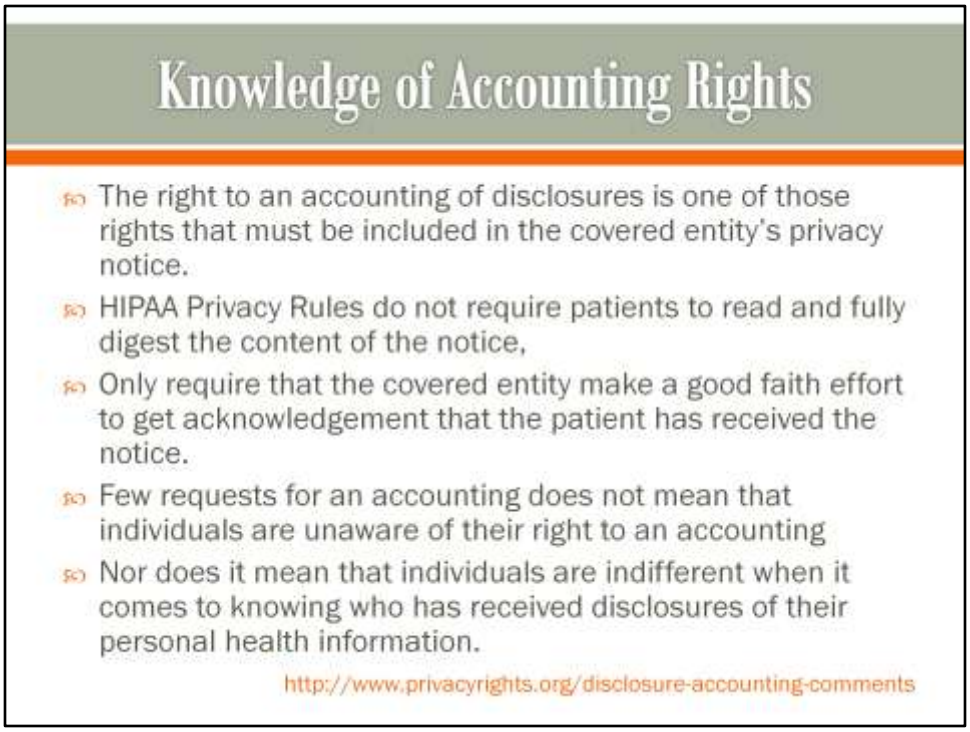
The Office for Civil Rights within the Department of Health and Human Services shall develop and maintain a multi-faceted national education initiative to **enhance public transparency** regarding the uses of protected health information, including programs to *educate individuals about the* ***potential uses*** *of their protected health information, the* ***effects*** *of such uses, and the* ***rights of individuals*** *with respect to such uses.*

– CFR 13403(b)

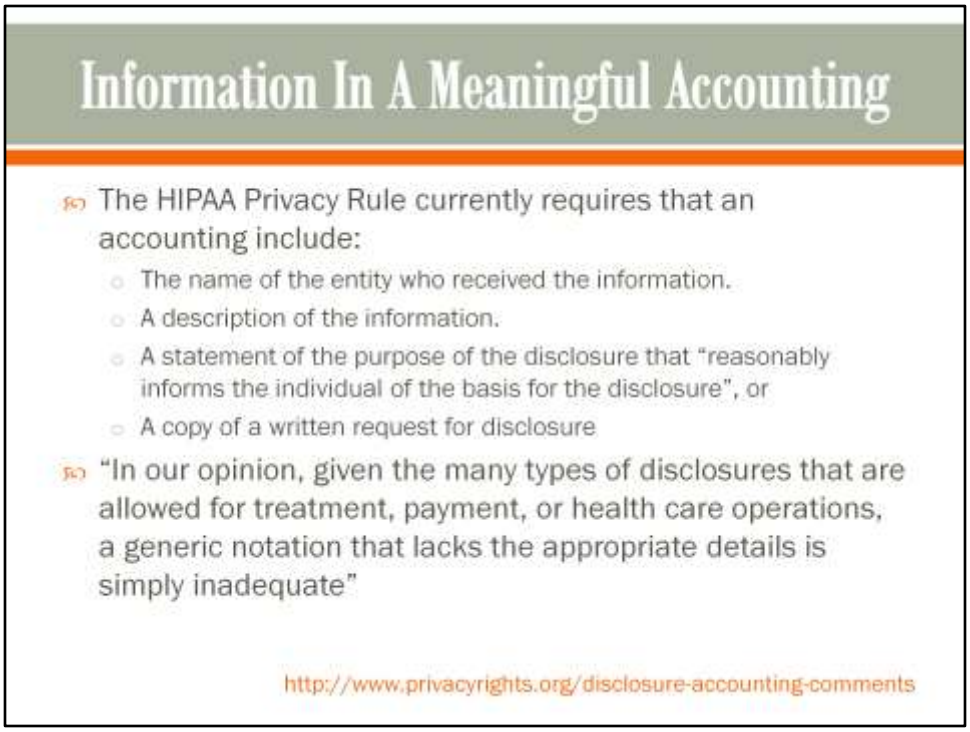
You can be sure that responses such as from the Privacy Rights Clearinghouse will be reflected in the Rule Making on the Accounting of TPO Disclosures



OCR's Question Number 1 asks: "What are the benefits to the individual of an accounting of disclosures, particularly of disclosures made for treatment, payment, and health care operations purposes?"



OCR's Question Number 2 asks: "Are individuals aware of their current right to receive an accounting of disclosures?"



OCR's Question 5 explores various data elements that should be included in an accounting in addition to

- date,
- time,
- patient identification number,
- user identification,
- and a description of the disclosure.

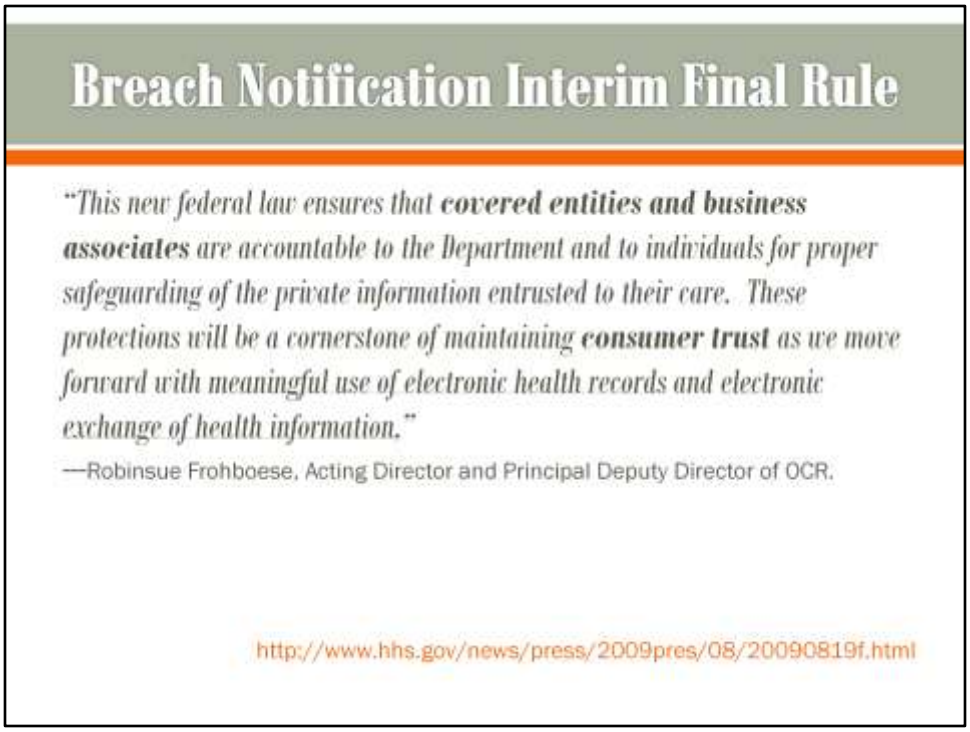
OCR asks whether other data elements such as recipient and purpose of the disclosure should be included or, in the alternative, whether a simple notation that the disclosure is for treatment, payment or health care operations is sufficient.

HHS Compliance Audits

- Authorized under CFR Sec 13411
- Covered Entities ***and now*** Business Associates
- Performed by the Office for Civil Rights
- Reported Breaches can Trigger Audits

Cignet Fined $4.3MM for Privacy Violations

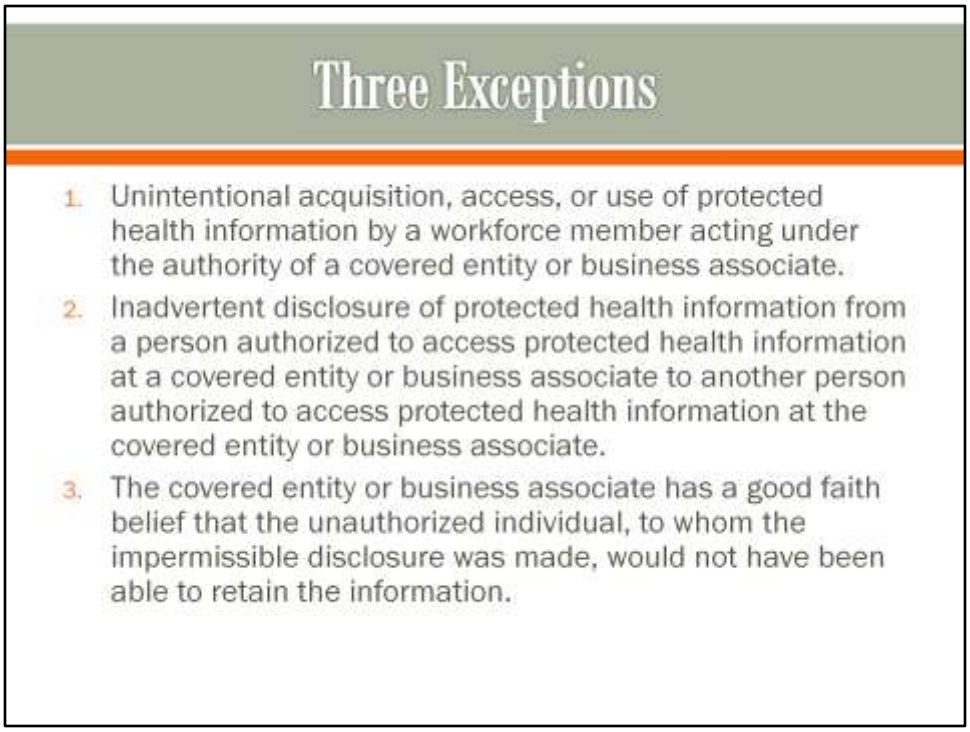
- February 23, 2011
- HHS Determined that Cignet Health violated The HIPAA Privacy Rule.
- Cignet fined $4.3 Million "Civil Money Penalty"
- Denying patients access to their medical records and failing to cooperate with the investigation.
- First time that the agency has used its legal authority to penalize a company for privacy violations.



"This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care. These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information,"
---Robinsue Frohboese, Acting Director and Principal Deputy Director of OCR.

Definition of Breach

- *"An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a **significant risk** of financial, reputational, or other harm to the affected individual."*



These 3 exceptions are still considered “Disclosures” but not a “Reportable Breach”

Situation #1 covers accidentally encountering PHI that you do not have a “need to Know” while working at a covered entity or business associate

Situation #2 covers a situation where email might be misdirected between two employees at a covered entity that are both under the authority of the covered entity

In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule

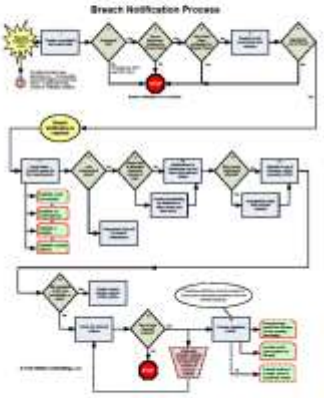
An example of Situation #3 would be if, for example a Nurse gave a patient the wrong discharge papers but retrieved them before the patient read and understood them.

Breach Flowchart

This Breach Notification Flowchart Presented is Courtesy of:

Tom Walsh, CISSP
President
Tom Walsh Consulting, LLC
www.TomWalshConsulting.com

Used by permission



NOTE: Click on the flowchart embedded in slide to open the Adobe Acrobat Document

Breaches Affecting 500 or More Individuals

- As required by the HITECH Act, the HHS Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals.
- Access this list here:
  - www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
- 249 Records as of 3/16/2011
- 8,289,821 Patients Affected

St Mary's Hospital Incident

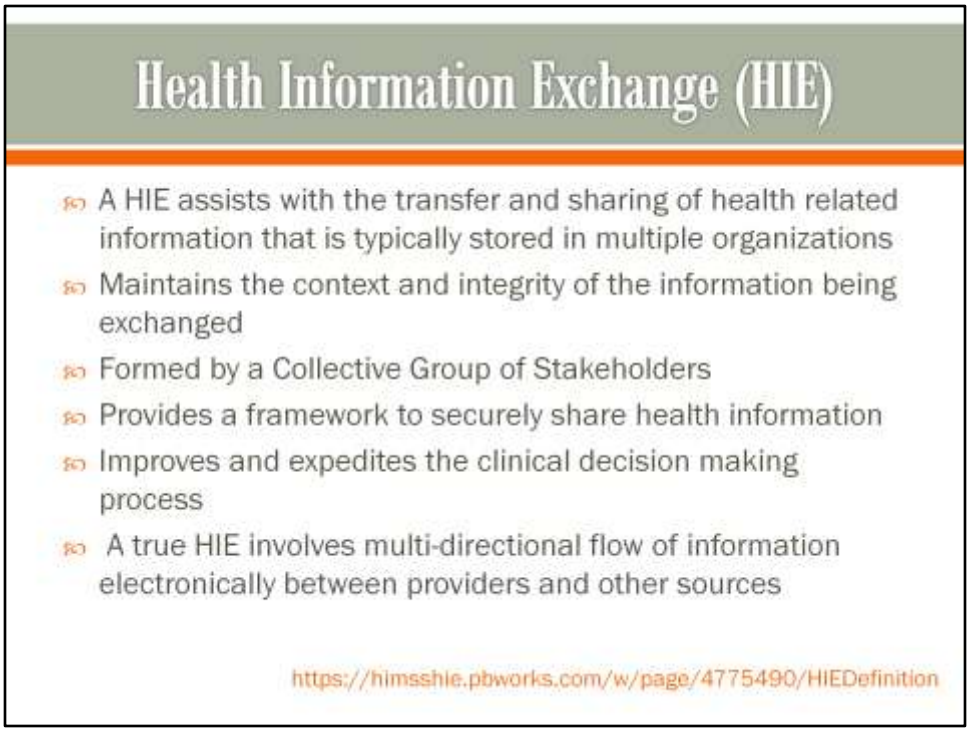
"Stolen laptop contained medical data on thousands of patients" Wisc .State Journal 12/20/2010

http://host.madison.com/wsj/news/local/crime_and_courts/article_24f20b7c-0ca0-11e0-b14e-001cc4c03286.html?mode=more

"Dean and St. Mary's Hospital handle data breach with elegance" Examiner.com 12/23/2011

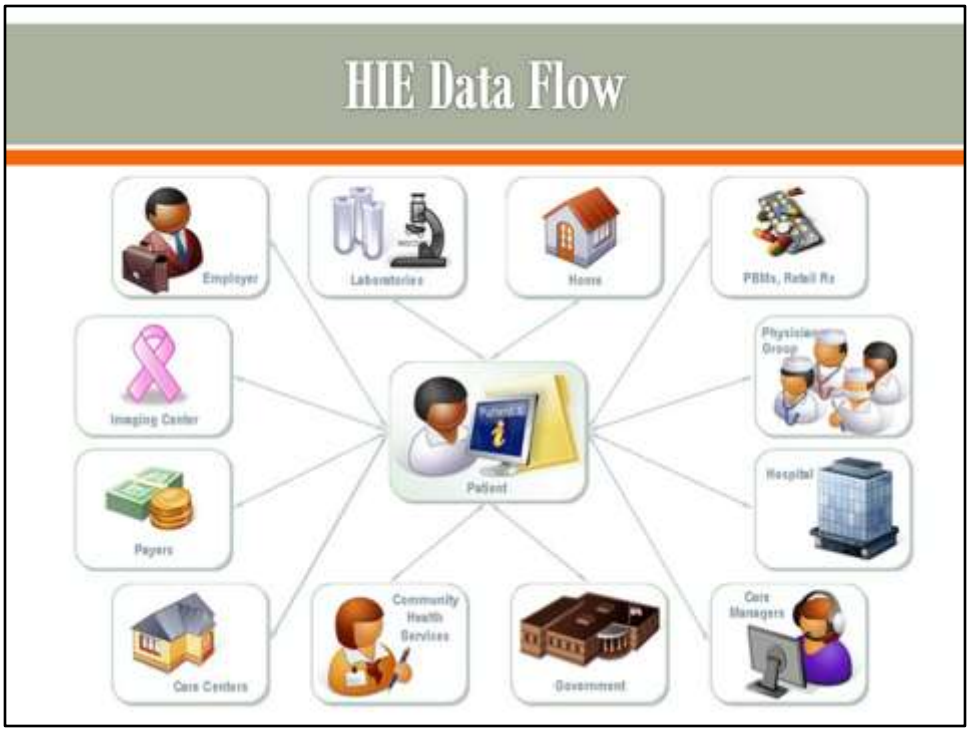
http://www.examiner.com/headlines-in-madison/dean-and-st-mary-s-hospital-handle-data-breach-with-elegance

- Bad Things can Happen to Good Companies
- 3288 Patients impacted by Stolen Personal Laptop from a Physician's Home
- Full Hard Disk Encryption Would have Prevented
- St Mary's Has Set an Excellent Example of Proper Response



Health Information Exchange – a "noun" and a "verb"

Formal organizations have been created in a number of states and regions that provide technology, governance, and support for HIE efforts.
Those formal organizations are termed **Health Information Organizations** (HIO) or Regional Health Information Organizations (RHIO).



physician web portals,
personal health records,
clinical messaging,
clinical interoperability and
Exchange of data from electronic medical records

Source:
https://himsshie.pbworks.com/w/page/4775490/HIEDefinition

Common Features of a HIE

- Patient Portal
- Clinical Messaging
- Clinical Interoperability
- Electronic Health Record (HER)
- Personal Health Record
- Record Locating
- Administrative Services
- Chronic Disease Management
- Community & Public Health

https://himsshie.pbworks.com/w/page/4777206/Features

Office of the National Coordinator for Health Information Technology (ONC)

ONC's mission includes:

- Promoting development of a nationwide Health IT infrastructure that allows for electronic use and exchange of information that:
  - Ensures secure and protected patient health information
  - Improves health care quality
  - Reduces health care costs
- Health IT policy coordination;
- Strategic planning for Health IT adoption and health information exchange
- *And much more...*

http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__onc/1200

ONC Tiger Team

- Launched June 10, 2010
- Workgroup of the Health IT Policy Committee
- A quick-response work group to provide ONC "with policy and technical advice on health IT privacy and security issues"
- *The "tiger team" created to resolve thorny privacy and security issues associated with sharing patients' health records* – GovHealthIT.com
- Open Meetings via Teleconference
- Website Contains Transcripts & MP3's of Meetings
  - http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19421

Tiger Team Recommendations

- ONC will determine whether to use the recommendations in proposed federal policies
- HHS ultimately would have to approve the policies

Scope

- Fair Information Practices
- Consent Requirements
- Meaningful Consent
- Granular Consent

Not Covered

- Exchange with Patients
- Data for Research

Fair Information Practices

Individual Access – Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

Correction – Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

Openness and Transparency – There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf

Fair Information Practices (2)

- *Individual Choice* – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.
- *Collection, Use, and Disclosure Limitation* – Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
- *Data Quality and Integrity* – Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.

http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf

Fair Information Practices (3)

- *Safeguards* – Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- *Accountability* – These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

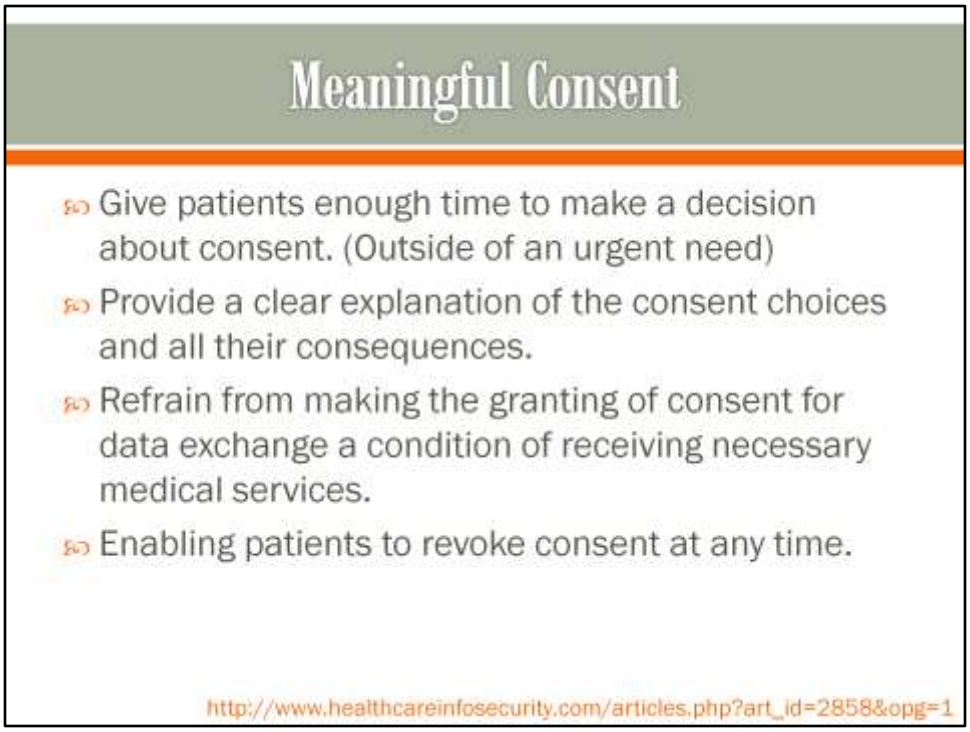
http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf

Tiger Team: Core Values

- The relationship between the patient and his or her health care provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information.
- As key agents of trust for patients, providers are responsible for maintaining the privacy and security of their patients' records.
- We must consider patient needs and expectations. Patients should not be surprised about or harmed by collections, uses, or disclosures of their information.
- Ultimately, to be successful in the use of health information exchange to improve health and health care, we need to earn the trust of both consumers and physicians.

http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_947491_0_0_18/TigerTeamRecommendationLetter8-17_2.pdf

Patient consent for the direct exchange of information between two provider organizations, such as when ordering a radiology exam, because that is handled under existing rules



When the decision to disclose or exchange the patient's identifiable health information
from the provider's record **is not in the control of the provider**
patients should be able to exercise *meaningful consent* to their participation.

Came to the conclusion that both opt-in and opt-out can be implemented in ways that fail to permit the patient to give meaningful consent.

“Based on our core values, the person who has the direct, treating relationship with the individual, in most cases the patient's provider, holds the trust relationship and is responsible for educating and discussing with patients about how information is shared and with whom”

Granular Consent

- All health information is sensitive, and what patients deem to be sensitive is likely to be dependent on their own circumstances.
- However, the law recognizes some categories of data as being more sensitive than others.
- Recommendations on consent do not make any assumptions about the capacity for an individual to exercise granular control over their information.
- Still Investigating Technology & Policy Considerations

Granular Consent (2)

- The technology for supporting more granular patient consent is promising but is still in the early stages of development and adoption.
- ONC should explore possible approaches to providing patients more granular control over the exchange and use of their identifiable health information
- Consider implications for quality of care and patient safety, patient educational needs, and operational implications.
- Find evidence (such as through pilots) for models that have been implemented successfully and in ways that can be demonstrated to be used by patients and fulfill their expectations.

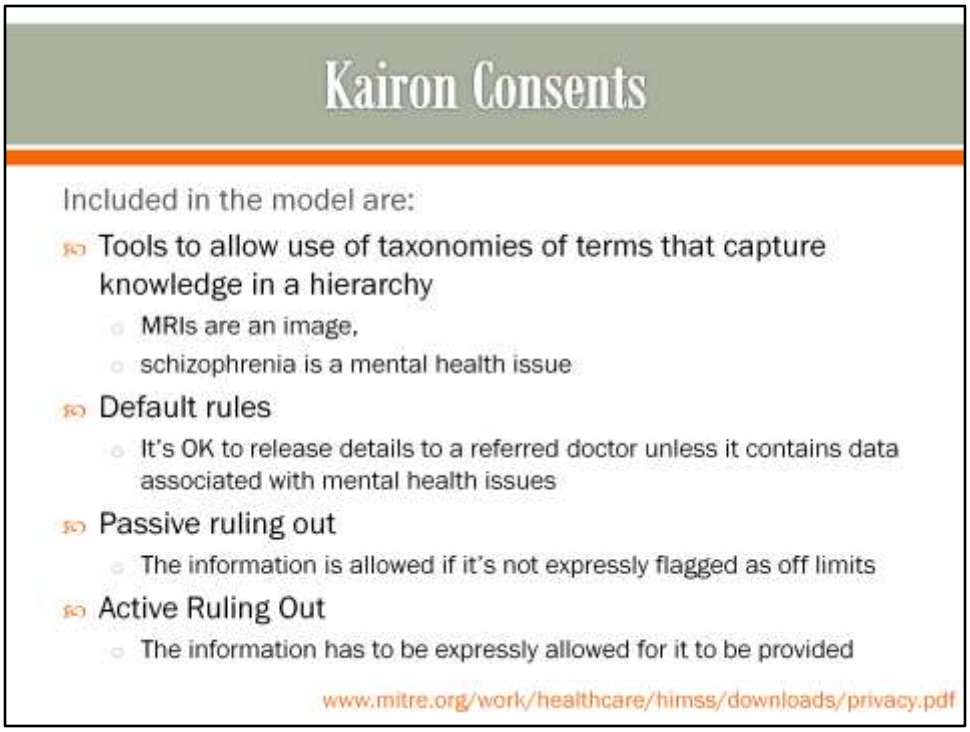
Granular Consent (3)

In the interim, and in situations where these technical capabilities are being developed and not uniformly applied, **patient education is paramount**: Patients must understand the implications of their decisions and the extent to which their requests can be honored, and we encourage setting realistic expectations.

The MITRE Kairon Consents Project

- Open Source Project by The MITRE Corporation
  - *http://sourceforge.net/projects/kaironconsents/*
- Response to Tiger Team Recommendation to Develop a practical, working prototype.
- Kairon has developed a UI and model that allows them to research how patients can express privacy preferences
- The rule language for expressing consents supports several important features that help discern and organize scenarios under which information should be provided or suppressed
- All constraints are compiled and published using the Extensible Access Control Markup Language (XACML).

www.mitre.org/work/healthcare/himss/downloads/privacy.pdf



To visualize this process, assume the patient registered the following preferences, after being guided through menus that go from general to increasingly specific:

- The primary care provider can receive any information for any purpose.
- Doctors referred by the primary care provider can receive information for treatment on allergies and medications but not mental health.
- A doctor with no established relationship with the patient cannot receive any information.
- Any requester doing research can receive information as long as it's not in the form of images and does not include personally identifiable information – but no mental health records even if de-identified.
- Any requester engaged in emergency care can receive any information – except about mental health.

When access to the patient's record is requested for any reason—and wherever the record resides—the globally available preference enforcer may be consulted by any record holder to determine the patient's current preferences for data sharing.

Resourcers & More Info

Privacy Advocacy Groups

- Center for Digital Democracy
- Consumer Action
- Consumer Federation of America
- Consumer Watchdog
- Electronic Frontier Foundation
- Privacy Lives
- Privacy Rights Clearinghouse
- Privacy Times
- World Privacy Forum
- U.S. Public Interest Research Group
- Electronic Privacy Information Center
- Health Policy Project - Center for Democracy & Technology

Websites

- Electronic Privacy Information Center
- The World Privacy Forum Medical Privacy Project
- Privacy & Security Tiger Team
- Uses and Disclosures for Treatment, Payment, and Health Care Operations
- Summary of the HIPAA Privacy Rule
- Summary of the HIPAA Security Rule
- HIMSS Health Information Exchange Toolkit

Download this PowerPoint

www.kennethGhartman.com

(Articles & Presentations Page)