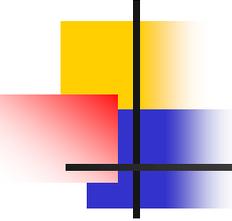


Health Insurance Portability and Accountability Act of 1996

The HITECH Impact

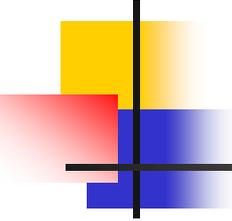
Socrates H. Tuch, MA, JD
Senior Counsel, Privacy Officer
Ohio Department of Health

2013



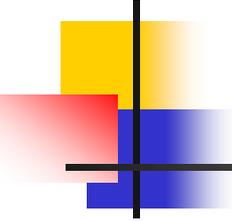
Goals

- To better understand HIPAA.
- To better understand how the “Health Information Technology for Economic and Clinical Health Act” (HITECH Act) impacts HIPAA.



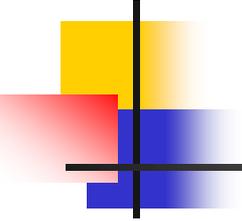
What is Privacy?

- Privacy is an expectation of information being held in some confidence.
- Privacy is not a complete blackout of information.



What is HIPAA?

- HIPAA is a federal act addressing health insurance and health care practices in the United States.
 - Establishes the minimum or “floor.”
- It empowers the US Department of Health and Human Services to create necessary regulations.
 - Preempts less stringent state laws.

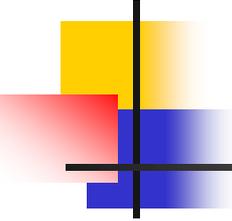


HIPAA is an attempt to empower information with its own privacy regardless of the context in which the information is found.

What is the purpose of HIPAA?

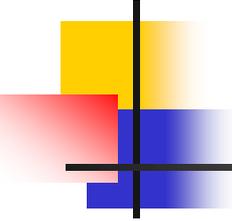
- HIPAA was created in order to regulate the private health care industry.
- Intended as a cost-saving measure.
- A good idea gone complicated.
- Ensure privacy.





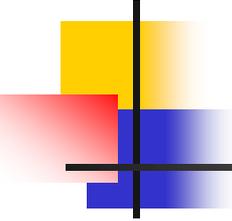
Distinctions

- Ownership of documents v. Ownership of information
- Possession of information v. Control of information



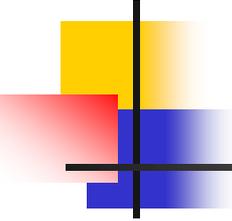
General Rule

- An entity cannot use or disclose Protected Health Information without:
 - Authorization,
 - From the individual who is the subject of the information.



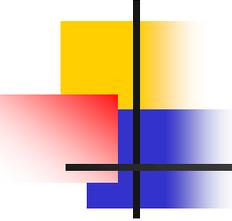
Protected Health Information

- "PHI"
- Individually identifiable information relating to:
 - the past, present, or future physical or mental health or condition of an individual, or
 - provision of health care to an individual, or
 - the past, present, or future payment for health care provided to an individual.



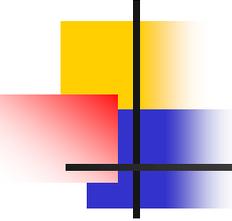
Covered Entity (CE)

- Health care provider
- Health plan
- Health care clearinghouse



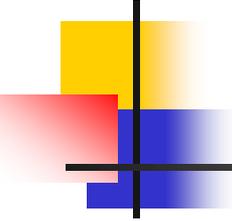
Health Care Provider

- Provider of medical or health services or any other person or entity who furnishes, bills, or is paid for health care in the normal course of business.
- Transmits any individually identifiable health information in electronic form relating to any covered transaction.



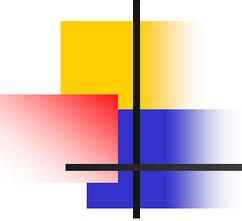
Health Plan

- An individual or group plan that provides, or pays the cost of, medical care, including:
 - Diagnosis, cure, mitigation, treatment, or prevention of disease or for the purpose of affecting any structure of the body.
 - Transportation for and essential to medical care.
 - Insurance covering medical care.



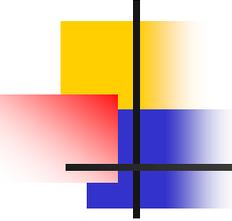
Health Care Clearinghouse

- An entity that processes health information from one format into another format.
 - Think “billing service” or “third-party administrator.”



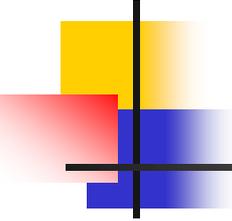
Duck Test

- Looks like...
- Walks like...
- Sounds like...



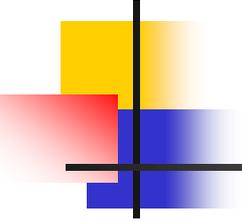
ODH - a “Hybrid Entity”

- A single legal entity that has covered functions that are not its primary mission.
 - A mixed entity.

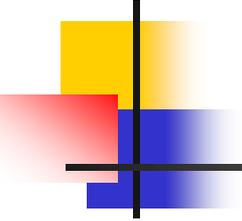


ODH as a hybrid entity

- The entity has parts that function as a health plan, health care provider, or health care clearinghouse.
- Other parts function as business associates of the covered functions or “covered programs.”



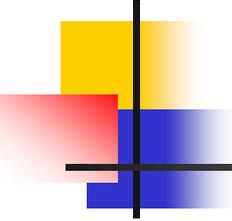
Persons in “associated non-covered programs” are expected to observe the policies, procedures, and confidentiality required by HIPAA.



Exceptions

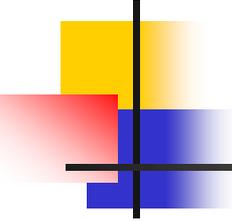
45 C.F.R. 164.512:

- Public Health
- Health Care Oversight
- Prisons – Custody
- Missing Persons
- National Security



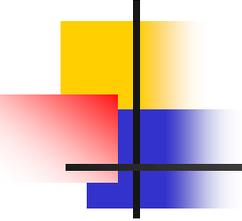
Health oversight agency

- A government agency or authority, or an employee, contractor, or agent thereof and those to whom the agency or authority has granted authority, that is responsible for:
 - overseeing the public or private health care system, or
 - government programs in which health information is necessary to determine eligibility or compliance, or
 - enforcing civil rights for which health information is relevant.



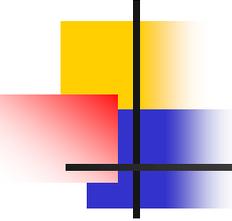
Required by law

- A mandate contained in law that compels an entity to use or disclose PHI and is enforceable in a court of law. Examples:
 - Court orders.
 - Disease reporting.
 - Legally required information for payment from government-funded program.



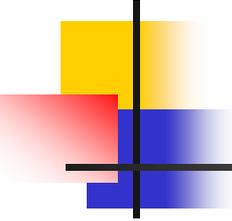
The Big Three: TPO

- Treatment
- Payment
- Health care Operations



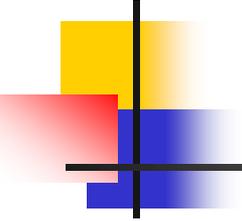
Treatment

- The provision, coordination or management of health care and related services,
- Consultation between providers relating to an individual,
- Referral of an individual to another provider for health care.



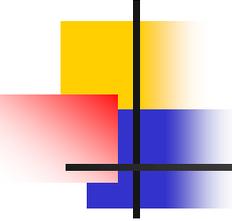
Payment

- Activities undertaken to obtain or provide reimbursement for health care, including:
 - Eligibility or coverage determinations.
 - Billing or collection activities.
 - Medical necessity determinations.
 - Utilization review.



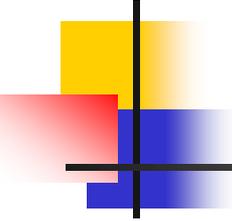
Funding of an Entity

- If an entity receives money from a government agency and the entity transmits information to the agency:
 - Entity is not necessarily a Business Associate
- Have to go through analysis.



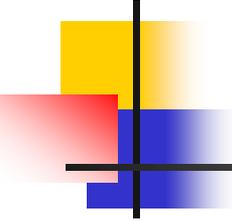
Health care operations

- Includes activities related to covered functions such as:
 - Quality assessment, assurance, or improvement.
 - Conducting or arranging medical review.
 - Legal or auditing services.
 - General business and administrative activities.



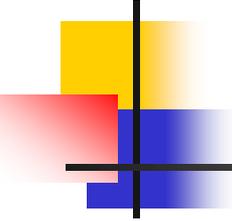
Safeguards

- A CE must make reasonable efforts to protect PHI from improper disclosures or uses by implementing safeguards:
 - Administrative
 - Technical
 - Physical



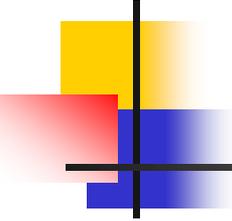
Minimum Necessary Standard

CE must make reasonable efforts to request or provide only the minimum PHI necessary to accomplish the purpose of the use, disclosure, or request.



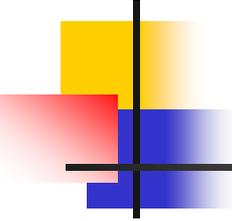
CE Minimum Necessary Duties

- CE must identify the persons who need access to PHI for their duties.
- CE must make reasonable efforts to limit the access to those persons.
- The CE should set out policies as to how access is determined and by whom.



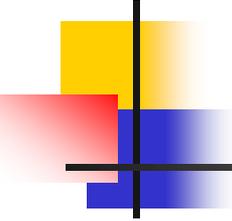
Minimum Necessary does not apply to:

- Requests from provider for treatment purposes.
- Uses or Disclosures made by or to the individual who is the subject of info.
- Uses or disclosures according to an authorization.
- Disclosures to Secretary of US HHS.
- Uses or disclosures required by law.



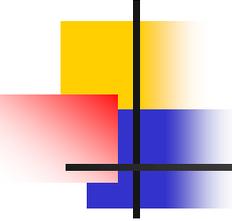
Mitigation:

- A CE has a duty to make reasonable efforts to mitigate harm from improper disclosures or uses of PHI.



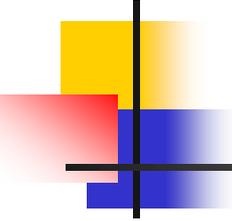
A CE must maintain for 6 years,
paper or electronic copies of:

- Polices & Procedures
- Any communication required
by HIPAA



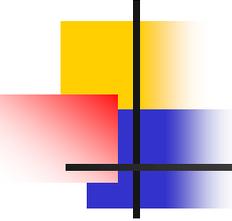
Right of Access

- Person has right to access his/her PHI
- Access can be denied if exception applies – examples:
 - Psychotherapy notes.
 - Material compiled in anticipation of litigation.
 - Access reasonably likely to endanger or harm person or others.



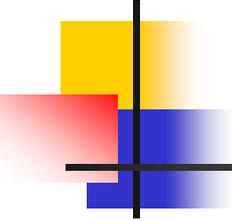
Accounting

- Every person has right to an accounting of the uses and disclosures of the person's PHI.
 - With certain exceptions.
- Must provide accounting within 60 days of request.
 - Can extend by 30 days.
- Six year time frame.



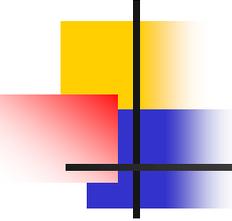
Content of Accounting

- Date of disclosure.
- Name of entity or person receiving the PHI.
- Brief description of PHI disclosed.
- Brief description of the purpose of disclosure.
- If multiple disclosures to same person or entity, list frequency.



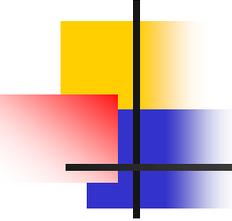
Right to Amend PHI

- Individuals have right to request amendment to PHI.
 - Request should be in writing;
 - Must provide reason and support for amendment.
- CE must act upon request within 60 days.
 - CE can have one 30-day extension.



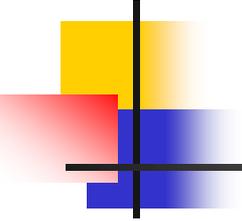
Accepting amendment

- If CE agrees to amend the PHI, in whole or in part, then the CE must:
 - Identify all the affected records and make the amendment.
 - Timely notify the individual who is the subject of the PHI.
 - Obtain authorization to notify previous recipients of the PHI of the amendment.

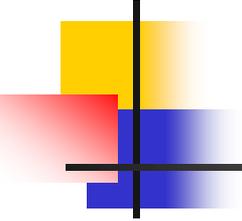


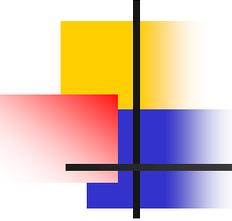
Conditional Communications

- Persons have a right to request restrictions of uses and disclosures.
- Persons have a right to request communication through alternative means or locations.
- CE is not required to agree.
 - If agreeable, then contract-like obligation.



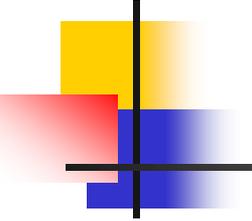
A CE cannot intimidate or retaliate against anyone who exercises her or his rights or complains.

- 
-
- The deceased have the same rights as the living.
 - Exercised by the Estate as a “personal representative.”
 - Rights terminate 50 years after death.



Notice of Privacy Practices must be:

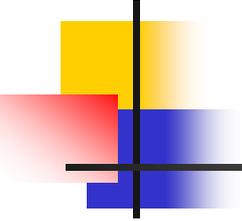
- Readily available to all patients/clients.
- Posted in a prominent location.
- Provided at the time of service and upon request.
- Posted on your web site.
- Explain all rights and obligations.



HITECH Act

The American Recovery and Reinvestment Act of 2009 (ARRA) contained parts intended to promote the use of electronic health records (EHR).

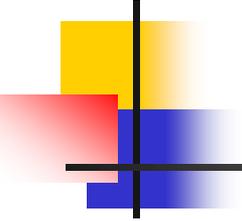
- Title XIII of ARRA is titled the “Health Information Technology for Economic and Clinical Health Act” (HITECH Act) and makes significant changes to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Most changes were effective February 17, 2010.



Changes

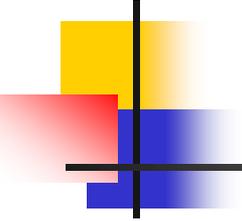
Most of the changes are assist the development of a nationwide health information technology infrastructure by:

- Adding some definitions
- Extending the reach of HIPAA



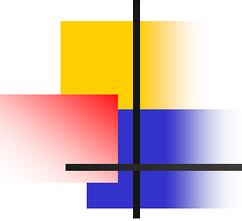
Key Points

- Extends the reach of HIPAA
- Covered Entities (CEs) and BAs are now required to notify clients/patients of nearly all Privacy or Security Breaches
- All entities that touch the data must be covered by HIPAA either directly or by contract.



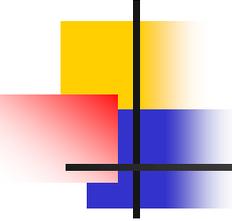
Key Points

- Limit certain uses of and disclosures of PHI
- Increases certain individual rights
- Significantly increases enforcement and penalties



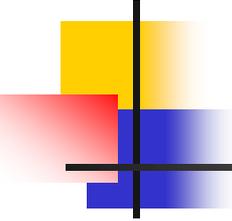
Definitions

“Breach” means the unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) which compromises the security or privacy of the information, EXCEPT where disclosure is to an unauthorized person who “would not reasonably have been able to retain such information.”



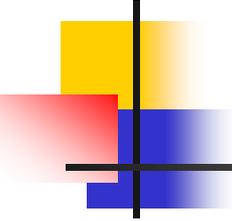
Definitions

“Unsecured Protected Health Information” (UPHI) is Protected Health Information (PHI) that is not secured by a technology standard developed or endorsed by an ANSI-accredited standards developing organization. The Secretary of the United States Department of Health and Human Services (HHS) can specify the technology or methodology to be used in guidance.



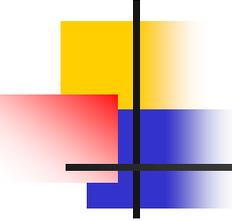
Other definitions

- Electronic media
- Reasonable diligence
- Willful neglect
- PHI now includes “genetic information” per GINA (Genetic Information Nondiscrimination Act of 2008)
- Administrative safeguards
- Physical safeguards



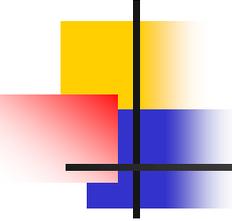
Breach Risk Assessment

- Entities must do an assessment of the risk to determine whether notification is required.
- It is a 4 step analysis.
- “Harm” is no longer part of the risk analysis.
 - Harm is now only part of mitigation
 - Now includes reputational harm.



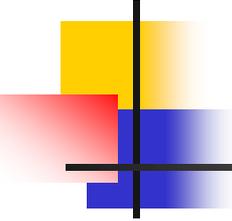
Assessment Factors

- Decision to Notify of Breach is based on:
 - Nature & extent of PHI (including likelihood of re-identification).
 - Identity of unauthorized person(s).
 - Whether PHI was actually acquired or viewed.
 - Extent to which risk has been mitigated.



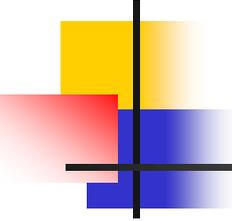
Mitigation Factors

- Nature/extent of violation.
 - Includes number of people affected and
 - Time duration of violation.
- Nature/extent of resulting harm.
- Compliance history.
- Financial condition of violator.
- Overall Justice.



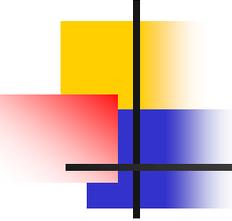
Penalties Will Apply

- It is not a question of whether, but of how much.
- Now more like “strict liability.”
 - Lack of knowledge is no defense.
 - 30 day cure period from date entity knew or should have known.
 - Cannot contract away liability/responsibility.



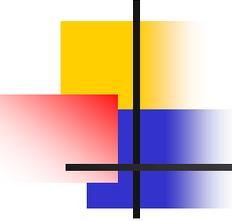
Agency

- CEs are responsible for the actions of their BAs through agency.
- “Federal Common Law” determination of agency.
- “Totality of the circumstances” analysis.
- “Willful Neglect” is now a key aggravator.



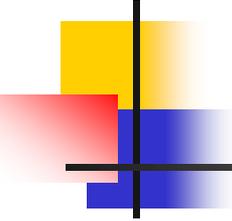
Agency Factors

- Time, place, and purpose of a BA's conduct.
- Whether CE can/could control the BA's actions.
- Whether the BA's conduct is usual or necessary to perform service for CE.
- Whether CE reasonably anticipated BA's conduct.



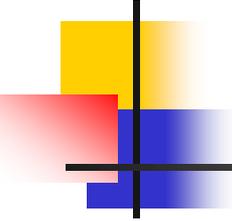
Other note-worthy items

- Immunizations
 - CEs may now disclose immunization records directly to schools as part of the “public health” exception.
- Marketing/Fundraising
 - Patients must now be given the option of “opting out” of any marketing or fundraising.



Other note-worthy items

- Access
 - CE must provide an individual with his or her PHI in the format requested if reasonable.
 - Access must be timely and reasonable – 30 days is the standard.
- Sale of PHI
 - CE must obtain prior authorization.



Thank you

Questions?

Socrates H. Tuch

Senior Legal Counsel/Privacy Officer

PH: 614-466-4882

socrates.tuch@odh.ohio.gov