LATHAM & WATKINS LLP

SAHF Privacy Working Group:

Privacy Impact Assessments

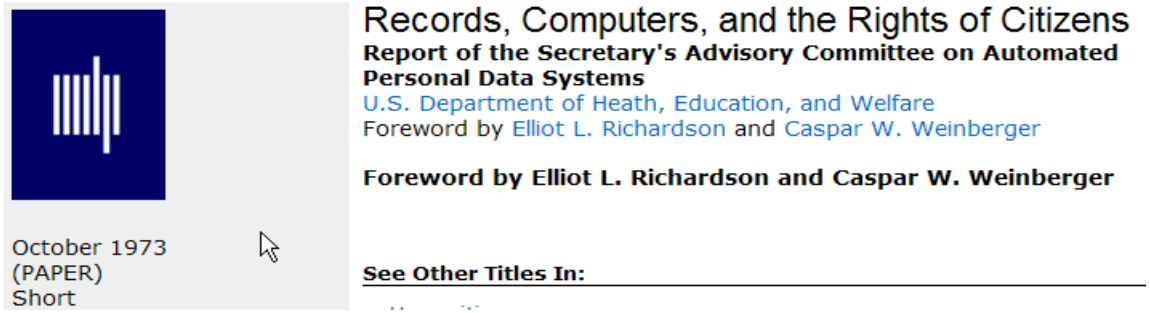
HIPAA

Susan A. Ebersole
Latham & Watkins LLP
February 18, 2016

Fair Information Practice Principles (FIPPS)

- ***Transparency***: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of Personal Data.

- ***Individual Participation***: Organizations should involve the individual in the process of using Personal Data and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of Personal Data. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of Personal Data.



FIPPS, continued

- ***Purpose Specification***: Organizations should specifically articulate the authority that permits the collection of Personal Data and specifically articulate the purpose or purposes for which the Personal Data is intended to be used.
- ***Data Minimization***: Organizations should only collect Personal Data that is directly relevant and necessary to accomplish the specified purpose(s) and only retain Personal Data for as long as is necessary to fulfill the specified purpose(s).
- ***Use Limitation***: Organizations should use Personal Data solely for the purpose(s) specified in the notice. Sharing Personal Data should be for a purpose compatible with the purpose for which the Personal Data was collected.

FIPPS, continued

- ***Data Quality and Integrity***: Organizations should, to the extent practicable, ensure that Personal Data is accurate, relevant, timely, and complete.
- ***Security***: Organizations should protect Personal Data (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- ***Accountability and Auditing***: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use Personal Data, and auditing the actual use of Personal Data to demonstrate compliance with these principles and all applicable privacy protection requirements.

What is Personal Data?

Typical Federal Trade Commission Definition from consent decree:

(a) a first and last name;

(b) a home or other physical address, including street name and name of city or town;

(c) an email address or other online contact information, such as an instant messaging user identifier or a screen name;

(d) a telephone number;

(e) a Social Security number;

(f) a driver's license or other state-issued identification number;

(g) a financial institution account number;

(h) credit or debit card information, including card number, expiration date, and security code;

(i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or

(j) any information that is combined with any of (a) through (i) above.

Privacy By Design

- Proactive/preventative
- Organizational priority
- Part of design process
- Embedded into everything
- End to end life cycle
- Privacy as default (regulator preference)
- Safeguarding
- Collection limited to legitimate business use
- Accuracy
- Visibility/transparency
- Retention periods customized by data set

LATHAM & WATKINS LLP

Privacy Impact Assessments (PIAs)

Privacy Impact Assessments

- Used by government (Privacy Act requirement) but also many private actors to assess and govern systems that handle Personal Data
- Identifies the type of Personal Data in the system (including any ability to combine multiple identifying elements on an individual);
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to defined purpose/mission is included.

Privacy Impact Assessment Approach

- List fields of data (Name, etc.)
- How will it be collected (directly from individual or indirectly about an individual?)
- Purpose of collection (use specification)
- Disclosures to others (employees or affiliates, government, service providers?)
- Resident choices? (opt in or out)
- Security/confidentiality safeguards (administrative, technical)
- Who can access, who administers those controls so that security and use limitations are achieved?
- Oversight, monitoring, training, accountability
- Breach readiness

6 Main Elements of a PIA

- Identify the need for a PIA
  - Scope the inquiry with threshold factual questions
- Describe the information flows
  - What/Who/Where/Why
- Identify privacy and related risks
  - Data minimization is a key to reducing risk
- Identify and evaluate solutions (remediation)
  - Driven by overall business tolerance for risk
- Sign-off and record PIA outcomes
  - Document
- Integrate PIA outcomes back into business plan
  - Learn for next project

SAHF Outcomes Initiative

- Outcomes Initiative aims to establish common outcome measures that show the impact and cost implications of the affordable housing and services SAHF members provide or could provide
- Goals:
  - Improve consistency and integrity of data
  - Improve variety and nature of services provided
  - Position members to take advantage of incentives
- Five Fields of Focus:
  - Health & wellness
  - Work, income, & assets
  - Housing stability
  - Youth & education
  - Community engagement

SAHF Outcomes Initiative PIA

- Purpose of data collection
  - Articulate clearly and in detail
  - Align with values and goals of project and organization
- What Personal Data is being collected?
  - Specify at “data field” level
  - Data sources
  - Keep in mind FIPPs principles of data minimization, transparency, and individual participation
- What is the intended use of the Personal Data?
  - Keep closely tailored to purpose specification
  - Consider whether Data Subjects adequately and clearly notified of intended use
  - Who within organization will use? Data minimization at use level.

SAHF Outcomes Initiative PIA, cont'd

- Data Governance Controls
  - How is data stored within the organization?
  - Who has access and is responsible for data quality and integrity?
  - Data from which data subjects is stored?
- System Ownership, Data Maintenance & Retention, Data Security
  - Data quality and integrity
  - Security
  - Accountability and Auditing
- Data Sharing Outside of Organization
  - Consider controls on service providers

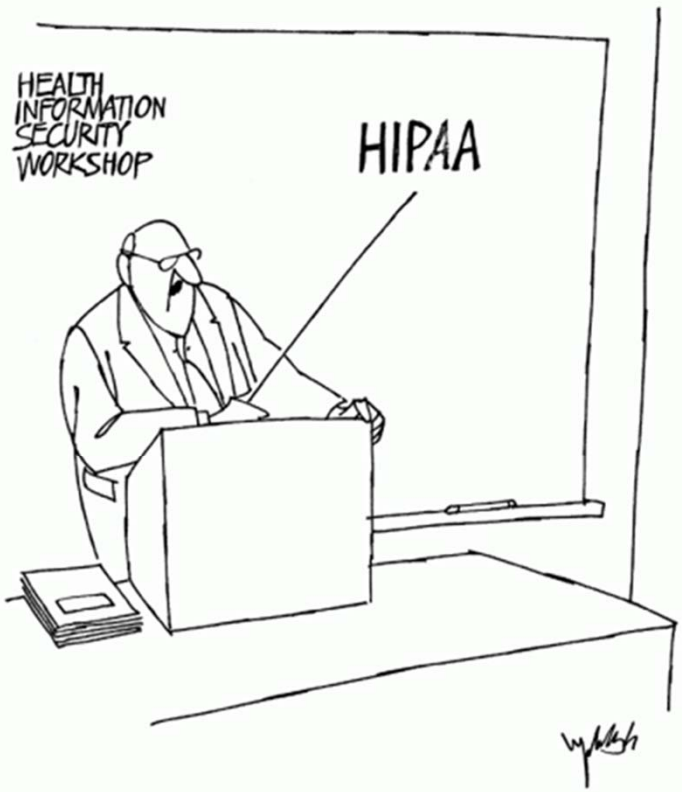
SAHF Outcomes Initiative PIA, cont'd

- Security Incident Reporting and Management
  - What is the organization's plan?
- Security Incident Related Liability
  - What are the risks to the organization of collecting, storing, and using the data for this project?
  - How can those risks be minimized?

LATHAM & WATKINS LLP

HIPAA in the Residential Services Context

What is HIPAA?



"No, it's not a female Hippopotamus, anyone else know?"

What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is the federal medical privacy law
- Sets a baseline for medical privacy laws – may be preempted by more stringent state laws
- HIPAA was enacted to:
  - Increase *efficiency* and *effectiveness* of the health care system
  - Protect the ***privacy*** and provide for the ***security*** of protected health information ("PHI")
  - Establish ***standards*** for accessing, storing and transmitting medical data and ensuring the privacy and security of PHI

HIPAA Rules
(Health Insurance Portability and Accountability Act of 1996)

- Secretary of HHS was required to issue regulations for medical data privacy & security
- "Covered entities" compliance with Privacy Rule effective April 2003
- Compliance with HIPAA Security Rule for electronic systems containing Protected Health Information (PHI) required April 2005 (directly applicable to Business Associates)

The HIPAA Legal Timeline

HIPAA
(Aug. 21, 1996): The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established "baseline" federal medical privacy and security standards.

HIPAA Privacy Rule
(Final Rule Dec. 2000, modified Aug. 2002): established rules to regulate the use or disclosure of PHI and provide individuals with certain rights with respect to such PHI.

HIPAA Security Rule
(Feb. 2003): established a system of reasonable and appropriate administrative, physical and technical safeguards for protecting PHI.

The HITECH Act
(Feb. 17, 2009): among other things, (i) extended the reach of the HIPAA Privacy and Security Rules to business associates (BAs); (ii) imposed breach notification requirements on covered entities (CEs) and BAs; and (iii) created enhanced penalties.

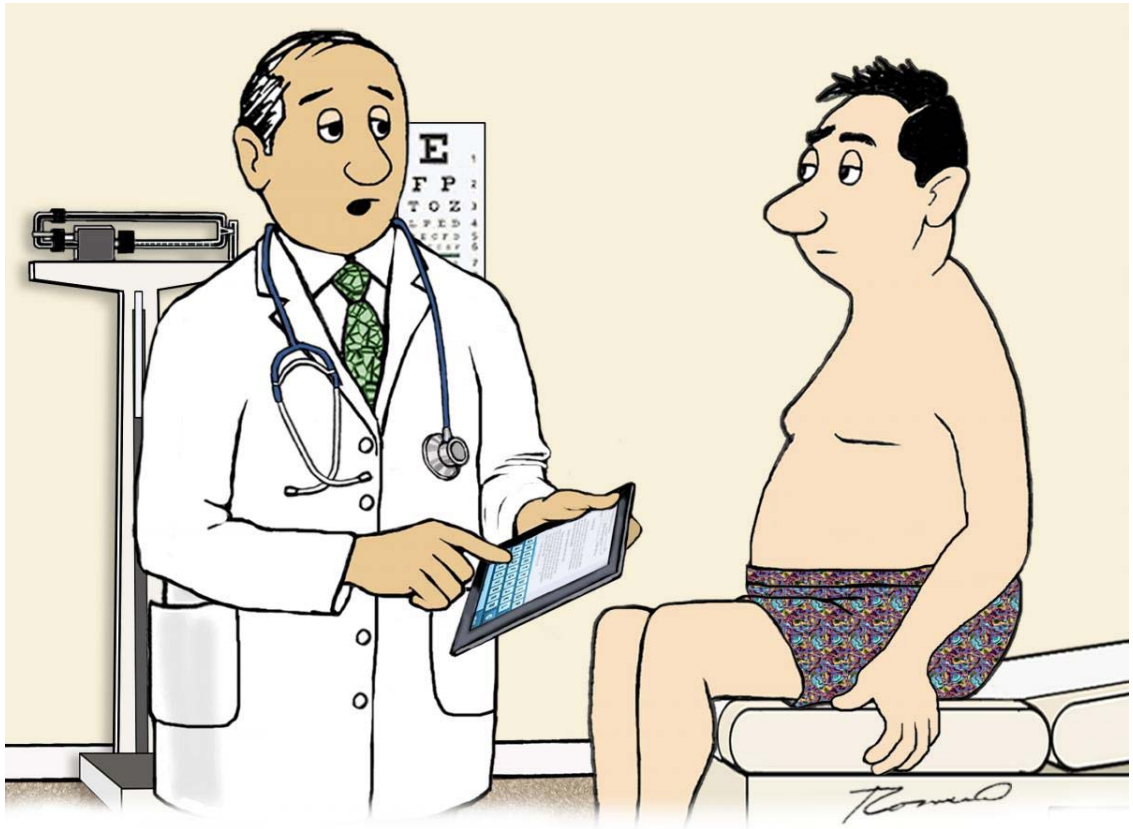
HIPAA Omnibus Final Rule (Omnibus Rule)
(Jan. 25, 2013): amended the HIPAA Privacy and Security Rules and implemented requirements of the HITECH Act, extending certain HIPAA obligations to BAs and their subcontractors.

The HIPAA Privacy and Security Rules

- **Privacy:** refers to WHAT is protected – health information about an individual, and restrictions placed on WHO may use, disclose or access the information.
  - 45 C.F.R. Part 160 and Subparts A and E of Part 164

- **Security:** refers to HOW information is safeguarded – system of administrative, physical and technical safeguards for ***electronic*** PHI.
  - 45 C.F.R. Part 160 and Subparts A and C of Part 164

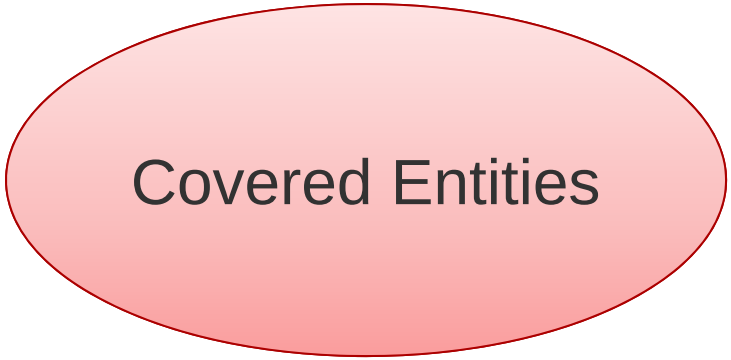
What Information is Protected by HIPAA?



What Information is Protected by HIPAA?

- **Protected health information** ("**PHI**") is:
  - Individually identifiable health information
  - Held or transmitted by a Covered Entity or Business Associate
  - In any form or media – whether electronic, paper or oral
  - That relates to:
    - Individual's **past, present, or future physical or mental health or condition**;
    - **Provision of health care** to the individual; or
    - **Past, present, or future payment** for the provision of health care to the individual
  - *AND that identifies an individual, or there is a reasonable basis to believe it can be used to identify an individual*
    - Includes common identifiers such as name, address, birthdate and SSN
  - But not de-identified information

Who is Regulated by HIPAA?



What is a Covered Entity?

- **Health plans** (HMOs, employer group health plans)
- **Health care clearinghouses**
  - E.g., billing service, repricing company, community health information system that provides data processing services regarding standardizing data formats
- **Health care providers** that engage in *standard electronic transactions* (hospitals, medical groups)
  - Transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule

Who is a Business Associate?

- A person or entity, other than a member of a covered entity's workforce, that creates, receives, maintains or transmits PHI ***on behalf of*** a covered entity for a function or activity regulated by HIPAA

- Under the Omnibus Rule, the definition of business associate **includes subcontractors** of business associates

- May also be a **covered entity**

- Must execute a **business associate agreement**

Does HIPAA Apply?

1. How did you receive patient health information?

2. Are you a covered entity?
   - Health care providers (furnish, bill, or are paid for health care in the normal course of business)
   - Sending covered transactions electronically
   - Plans/Clearinghouses

3. Are you a business associate?

Does HIPAA Apply?

- Do you handle patient health care information?
- Did you receive it from the End User directly, and you are a Covered Entity? (then YES)
- If information was received from a Covered Entity, you may have signed a Business Associate Agreement effectively agreeing that HIPAA does apply, or you will meet its standards as if it did.
- De-identification (per HIPAA requirements) as common way forward.

Overview of effects of HIPAA Privacy Rule

- Requires covered entities to:
  - Make a good faith effort to get signed acknowledgement of information practices related to PHI used in treatment, payment and operations
  - Obtain authorization for special additional uses of PHI
  - Designate a privacy official
  - Develop policies and procedures (including receiving complaints)
  - Provide a privacy training to their workforce
  - Develop a system of sanctions for employees who violate an entity's policies
  - Meet documentation requirements
  - Implement appropriate administrative, technical, & physical safeguards to protect privacy

Security Rule: Electronic Protected Health Information

- Security Rule applies only to electronic protected health information (ePHI):
  - PHI that is created, received, maintained or transmitted in electronic format
  - Does not include paper-to-paper faxes or video teleconferencing or messages left on voice mail
    - Information being exchanged did not exist in electronic form before the transmission.

HIPAA/HITECH Key Steps/Changes

- Thorough risk assessments including identifying locations with protected health information (PHI)
- Update policies and procedures
- Adopting a cross-functional approach to compliance
- The necessity of encryption
- Mitigating top risks and
- Updated business associate (BA) contracts
- Breach notification rules (unsecured PHI that is not encrypted)
- BAs required to implement applicable privacy provisions and all of the security provisions
- Same penalties for BAs