Are You Ready? Analyzing the Ramp-Up in HIPAA Audits and Enforcement

Adam Robison, Partner
Juliet M. McBride, Senior Associate
King & Spalding LLP
Houston, Texas
“99% of computer users are vulnerable to exploit kits (software vulnerabilities).”
Source: Heimdal Security

“Four out of five victims [of a breach] don’t realize they’ve been attacked for a week or longer.”
Source: 2016 Data Breach Investigations Report from Verizon

“80% of analyzed breaches had a financial motive.”
Source: 2016 Data Breach Investigations Report from Verizon
Agenda

- HIPAA Overview
- HIPAA Rules
  - Privacy Rule
  - Security Rule
  - Breach Notification Rule
  - Enforcement Rule
- HIPAA Audits
- HIPAA Enforcement
HIPAA Overview
Federal and State HIPAA

The Statutes and Regulations

• Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  — Privacy Rule (April 2003)
  — Security Rule (April 2005)

• Genetic Information Nondiscrimination Act of 2008 (GINA)

• Health Information Technology for Economic and Clinical Act of 2009 (HITECH)
  — Breach Notification (February 2010)
  — Omnibus Rule (September 2013)
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (“HIPAA”)


Established, for the first time, a set of national standards for the protection of certain health information
HIPAA Rules

• The Unique Identifiers Rule (NPIs)
• The Transactions and Code Sets Rule
• The Privacy Rule
• The Security Rule
• The Enforcement Rule
• The Breach Notification Rule
HIPAA Objectives

• **Portability**
  - Provide ability for individuals to maintain health insurance between jobs

• **Accountability**
  - Combat fraud & abuse
  - Establish uniform *privacy and security protections* for PHI
  - Mandate uniform standards for electronic transmission of PHI related administrative and financial information
Key HIPAA Dates

**Privacy Rule**
- Compliance Date: April 14, 2003

**Security Rule**
- Compliance Date: April 21, 2005

**Enforcement Rule**
- Compliance Date: March 16, 2006

**Breach Notification Rule**
- Compliance Date: February 2010
Final Omnibus Rule

• **Subtitle D:**
  - Addresses privacy and security concerns with electronic transmission of PHI
  - Strengthened HIPAA’s Enforcement & Privacy Rules
  - Added Breach Notification requirements (Breach Rule)
  - Did not change Security Rule but increased penalties

• **Key Dates:**
  - Published in Federal Register – January 25, 2013
  - Effective Date – March 26, 2013
  - Compliance Date – September 23, 2013
  - Transition Period – Up to September 22, 2014 for certain Business Associate Agreements
  - No new regulations since March 26, 2013
HIPAA Overview

Key Definitions *(Who isCoveredby HIPAA)*

- **Covered Entity (CE):**
  - Health care provider who bills using electronic medium
  - Health Plan (public or private, self-insured or insured)
  - Clearinghouse (billing service, re-pricing company, etc.)
  - Medicare Prescription Drug Plan Sponsors

- **Business Associate (BA):**
  - Entity that creates, receives, maintains, or transmits PHI on behalf of a CE
  - Service providers (e.g., lawyers, actuaries & consultants)
  - Subcontractors
Business Associates

Covered Entity

Lawyers
Consultants
Auditors
Billing
TPA
Clearinghouses
Data Processing
Accountants
JC
HIPAA Overview

Key Definitions (What is Covered by HIPAA)

- **Protected Health Information (“PHI”)**
  - Individually Identifiable Health Information
    - Health information, including demographic info
    - Relates to health condition, provision of healthcare, or payment for healthcare; and
    - Identifies or could be used to identify the individual
    - Any form (oral, written or electronic)
  - In the possession of a CE or BA

- **Unsecured PHI** – PHI not rendered unusable, unreadable, or indecipherable through encryption or destruction
HIPAA Rules
Privacy Rule
Privacy Rule

- **Purpose**: Safeguard PHI from inappropriate access, use, or disclosure.

- **Applicability**: CEs and BAs (for certain purposes).

- **General Rule**: Prohibits a CE or BA from using or disclosing PHI, except as permitted or required under the HIPAA regulations.
The Privacy Rule: General Overview

The Privacy Rule in one really long sentence:

CEs may only use PHI as set forth in the Privacy Rule, which:

(1) limits use and disclosure of PHI (absent authorization) to treatment, payment, health care operations, and other enumerated public purpose disclosures;

(2) requires CEs to give individuals certain rights (e.g., to access and amend their PHI); and

(3) requires CEs to implement various administrative policies and procedures to protect the confidentiality of PHI.
Key Concept: *Use* vs. *Disclosure*

**Use**: Sharing, Employing, Applying, Utilizing, Examining, Analyzing

Used when it moves **within** an organization

**Disclosure**: Releasing, Transferring, Providing access to, Divulging in any manner

Disclosed when it is transmitted **outside** an organization
How the Privacy Rule Works

• The Privacy Rule’s standards protect the confidentiality of PHI by:
  — Regulating use and disclosure by CEs and BAs; and
  — Requiring CEs and BAs to enter into BAAs and provide “satisfactory assurances” regarding use, disclosure, and safeguarding PHI.
Permitted Uses, Required Disclosures, and Minimum Necessary Requirement

- **Permitted Uses and Disclosures of PHI by CE:**
  - De-identified PHI
  - Treatment, payment, and health care operations
  - Pursuant to a valid authorization (except health plans may not use genetic information for underwriting purposes)
  - Other authorized uses and disclosures (e.g., public health, law enforcement, required by law, etc.)
  - BAs (with contractual assurances)

- **Required Disclosures:** To the individual and HHS per request.

- **Minimum Necessary Standard:** Uses and disclosures limited to minimum required.
De-identified Data

Health information can be de-identified

*De-identified data is not subject to HIPAA*

- Two Methods:
  1. “Safe Harbor” method
     - Remove 18 identifiers AND have no knowledge remaining information can be used to identify an individual
  2. Statistical method
     - Expert determines risk of re-identification is very small
De-Identified Information

- De-Identified information is not PHI

Remove 18 identifiers
- Name, age, address
- Telephone, fax, e-mail
- Social security number, account number, license number
- Others
Health Care Operations

- Quality Assessment
- Population-based Activities
  - Reviewing competence, credentialing
  - Training
- Accreditation, certification, licensing
- Underwriting
  - Medical review, legal services, auditing, compliance
  - Business planning and development
Multi-Tiered Approach to Obtaining Patient Permission to Use or Disclose PHI

- **Oral Opportunity** (for Individual to Agree or Object to use of certain types of PHI)
- **Written Consent** (for uses and disclosures relating to treatment, payment, or health care operations)
- **Written Authorization** (other uses and disclosures not relating to treatment, payment, or health care operations)
Oral Opportunity

• Directory information

• Uses and disclosures to persons involved in the individual’s care (e.g., family member)
Written Consent for Treatment, Payment, or Health Care Operations

- **General Rule:** With some exception (psychotherapy notes, marketing, sale of PHI), a CE may use or disclose PHI for treatment, payment, or health care operations.
  - Applies to:
    - CE’s own treatment, payment or healthcare operations
    - Treatment activities of a direct healthcare provider
    - Another CE or healthcare provider for payment or healthcare operations
    - Other participants to a organized healthcare arrangement

- A CE **may** (but is not required to) obtain consent to carry out treatment, payment or health care operations.
  - Consent is not an effective substitute for an authorization where required.
  - Consent form is general in nature
Conditioning Treatment or Enrollment on Completion of Consent Form

- Health care providers may condition treatment on the individual signing a consent form.
- Health plans may condition enrollment on the individual signing a consent form.
- Compare: Health care providers and health plans may not condition *treatment or enrollment* on the individual signing an *authorization form*.
Written Authorization for Purposes Unrelated to Treatment, Payment, or Health Care Operations

- More specific than the Consent Form
- Must contain specific information including:
  - Core Elements (e.g., description of info to be used, name of person to whom disclosure will be made, etc.)
  - Required Statements (e.g., right to revoke, prohibition against conditioning treatment, payment, enrollment, or eligibility on signing the authorization)
- Additional and different content requirements depending on whether:
  - For psychotherapy notes
  - For marketing
  - For sale of PHI
  - For a covered entity’s own uses or disclosures;
  - For disclosures by others; or
  - For PHI created for research including treatment
When No Patient Permission is Required …

- Payment, treatment, or healthcare operations
- When use or disclosure is required by law
- Public health activities
- Disclosures about victims of abuse, neglect, or domestic violence
- Health oversight activities (e.g., Gov’t investigations)
When No Patient Permission is Required …

• Judicial and administrative proceedings
• Disclosures to coroners, medical examiners, and funeral directors
• Uses and disclosures for organ, tissue, and eye donation
• Uses and disclosures for research
• And others …
Minimum Necessary Standard

- Minimum Necessary Use
- Minimum Necessary Disclosures
- Minimum Necessary Requests
Business Associates

• General Rule: Disclosure of PHI to a BA requires a written contract that meets the HIPAA requirements

• Exceptions:
  — Disclosure to a health care provider for treatment of an individual
  — Disclosure from group health plan to plan sponsor under certain circumstances
  — Disclosure to government program under certain circumstances
Individual Rights

Individuals have six “individual rights”:

1. **Notice:** Right to receive a notice of privacy practices of PHI

2. **Restriction:** Right to request a restriction of uses and disclosures of PHI

3. **Confidential Communication:** Right to request confidential communications of PHI

4. **Access:** Right to access and copy PHI

5. **Amendment:** Right to amend PHI

6. **Accounting:** Right to receive an accounting of non-routine disclosures of PHI
The Ten
“Administrative Requirements”

1. Personnel Designations (including privacy official)
2. Training
3. Safeguards
4. Complaint Process
5. Sanctions
6. Mitigation
The Ten
“Administrative Requirements”

7. Refraining from “intimidating or retaliatory acts”
8. Cannot require individuals to waive right to complain to Secretary of HHS
9. Privacy policies and procedures
10. Documentation and retention of records
The Security Rule
The Security Rule

- Applies to electronic PHI ("EPHI"), which is PHI transmitted by or maintained in an electronic media
  - Hard drive, CD, internet, etc.
  - Does not include paper faxes
- Must ensure confidentiality of EPHI and protect against reasonable anticipated threats
- 36 Implementation Specifications: Some are mandatory and others are "addressable"
Categories of Security Standards

- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security Mechanisms
Security Rule – Administrative Safeguards

- Policies and Procedures
- Personnel Designations
- Risk Analysis & Management Plan
- Access Control & Management
- Training
Security Rule – Physical Safeguards

- Workstation Use and Security
- Control Access to Facility
- Device and Medical Controls
Security Rule – Technical Safeguards

- Access Authorization; Screensavers; Encryption
- Audit Controls
- Integrity Measures; Virus Scans; Firewalls
- Authentication Through Password Management
- Transmission Security
Security Rule – Risk Analysis

• Review Data
  — Type of data
  — Storage location
  — Persons with access
  — Access procedures
  — Audit logs
  — Encryption

• Gap Analysis

• Implement Appropriate Security Measures
Enforcement Rule
HIPAA Enforcement Rule

- Enforcement of the Privacy Rule began April 14, 2003 for most HIPAA covered entities.

- CEs were required to comply with the Security Rule beginning on April 20, 2005. OCR became responsible for enforcing the Security Rule on July 27, 2009.

- HITECH Act strengthened civil and criminal enforcement of HIPAA.
Enforcement Agencies

Civil Actions

• By:
  – Office for Civil Rights (OCR)
  – State Attorney’s General Offices

• Types:
  – Settlements
  – Resolution Agreements w/Corrective Action Plan

Criminal Actions

• Referred by OCR to DOJ
HIPAA Enforcement– Key Terms

• **Reasonable Diligence** - the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances

• **Reasonable Cause** - an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect

• **Willful Neglect** - conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.
Civil Enforcement Penalties

- Enforcement by Office of Civil Rights
- $1.5 annual cap applies for violation of identical requirements

<table>
<thead>
<tr>
<th>Nature of Violation</th>
<th>Penalty Amount (Per Violation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Cause</td>
<td>$100 - $50,000</td>
</tr>
<tr>
<td>Reasonable Cause and Not Willful Neglect</td>
<td>$1,000 - $50,000</td>
</tr>
<tr>
<td>Willful Neglect</td>
<td>$10,000 - $50,000</td>
</tr>
<tr>
<td>Willful Neglect (Not Corrected Within 30 Days)</td>
<td>At least $50,000</td>
</tr>
</tbody>
</table>
Criminal Enforcement Actions

• Generally:
  — $50,000 fine
  — 1 year in prison
  — or both

• False Pretenses:
  — $100,000 fine
  — 5 years in prison
  — or both

• Really Bad Intent (e.g., commercial gain, malicious harm):
  — $250,000 fine
  — 10 years in prison
  — or both
Breach Notification Rule
Breach Notification Rule

Overview

• **General Rule.** Notification to certain parties is required following discovery of a breach of “unsecured” PHI

• **Unsecured:** Not rendered unusable, unreadable, or indecipherable to unauthorized persons per HHS guidance

  — Encryption
  — Destruction
Breach Notification Rule

Who Must be Notified?

- **CE:**
  - Individuals
  - HHS Secretary
    - At same time as individuals if >500 individuals involved
    - Annual log if <500 individuals involved
    - Media notice if >500 residents in a jurisdiction

- **BA:**
  - CE
  - May notify individuals if arranged with the CE
Breach Notification Rule

What Constitutes a Breach?

- Acquisition, access, use or disclosure of PHI
  - Not permitted by HIPAA Privacy Rule; and
  - Compromises security or privacy of PHI
- If HIPAA Privacy Rule is violated, breach is presumed unless the CE or BA demonstrates low probability of compromise based on risk assessment of:
  - Nature and extent of PHI
  - Unauthorized person involved
  - Whether PHI was actually acquired or viewed
  - Extent of risk mitigation
Breach Notification Rule

What Does Not Constitute a Breach?

- Unintentional acquisition, access or use by workforce member, if in good faith and within scope of authority, and no further use or disclosure

- Inadvertent disclosure to a colleague who is also authorized to access PHI, and no further use or disclosure

- Disclosure where there is a good faith belief that the unauthorized person was not reasonably able to retain the information
Breach Notification Rule

Notice to Individuals

• To individuals (or their representatives) whose information is reasonably believed to have been accessed, acquired, used or disclosed without authorization

• Use plain language

• Include certain required information (e.g. description of breach, dates, types of information involved)
Breach Notification Rule

When is Notice Required?

- “Without unreasonable delay” and no later than 60 days after “discovery of breach” (even if investigation is ongoing)

- Clock starts for a business associate breach depending on relationship:
  - For independent contractor, 60 days from notification to covered entity
  - For agent, 60 days from business associate’s own discovery

- Law enforcement delay is possible
Breach Notification Rule

When is a Breach “Discovered”?

• “Discovery” means first day on which breach is known or by exercising reasonable diligence would have been known to any employee, officer, or agent

• Company should have in place:
  — System for detecting breach
  — Training and policies to ensure that breaches are reported to management by employees
Office of Civil Rights Audits
OCR Audit Program: Origin and Objectives

• HITECH requires OCR to conduct periodic audits of CEs’ and BAAs’ compliance with HIPAA.

• Audit Objectives:
  – Examine mechanisms for compliance
  – Identify best practices
  – Discover risks and vulnerabilities that may not have otherwise been discovered
  – Renew attention to health information privacy and security compliance activities
OCR Audit Program: Pilot / Phase 1

- OCR conducted a pilot audit program in 2011-12.

- 115 entities were audited:
  - 61 providers, 47 health plans, 7 clearinghouses.
  - In selecting the entities, OCR categorized them into 4 “levels”, by extent to which entities used HIT.

- Total 979 audit findings and observations:
  - 293 privacy, 592 security, 94 breach notification.

- Observations were most numerous for providers.
OCR Audit Program: Phase 2

• Phase 2 is currently underway.

• OCR’s goals:
  — Understand compliance efforts by entities
  — Guide development of OCR technical assistance
  — Develop tools to assist in compliance

• Audit will include both covered entities and business associates, selected based on size, affiliations, location, public/private.

• Audit will comprise over 200 desk audits and a “smaller number” of onsite audits.

• On July 11, 2016, OCR notified 167 covered entities of selection for desk audits.
OCR Audit Program: Phase 2

- Desk audit scope is limited to 7 controls. Entities will be audited on:
  - Security Rule controls or
  - Privacy Rule and Breach Notification Rule compliance.

<table>
<thead>
<tr>
<th>Privacy Rule Controls</th>
<th>Notice of Privacy Practices &amp; Content Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provision of Notice – Electronic Notice</td>
</tr>
<tr>
<td></td>
<td>Right to Access</td>
</tr>
<tr>
<td>Breach Notification Rule Controls</td>
<td>Timeliness of Notification</td>
</tr>
<tr>
<td></td>
<td>Content of Notification</td>
</tr>
</tbody>
</table>
OCR Audit Program: Phase 2

• For desk audits, auditees will have 10 business days to provide information to OCR:
  — Applicable policies, procedures, evidence of implementation; and
  — A list of the entity’s business associates.

• Desk audits of BAs will commence in late September, and will focus on BAs identified by CEs.

• Onsite audits will begin in early 2017 and will use a comprehensive set of HIPAA controls.
OCR Audit Program: Phase 2

• Entity-specific audit results will not be published, but may be subject to disclosure under the Freedom of Information Act.

• Based on audit findings, OCR may open a separate compliance review “in a circumstance where significant threats to the privacy and security of PHI are revealed through the audit.”
Enforcement Activity
HIPAA / Privacy Enforcement

Most common types of covered entities required to take corrective action by HHS OCR to achieve voluntary compliance are:

1. Private Practices;
2. General Hospitals;
3. Outpatient Facilities;
4. Pharmacies; and
5. Health Plans

www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html
HIPAA / Privacy Enforcement

Most frequent compliance issues investigated from the compliance date in April 2003 to present:

1. Impermissible uses and disclosures of PHI;
2. Lack of safeguards of PHI;
3. Lack of patient access to their PHI;
4. Use or disclosure of more than the minimum necessary PHI; and
5. Lack of administrative safeguards of electronic PHI

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html
OCR Enforcement Activity: Increase In Complaints

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html#
OCR Enforcement Activity: Complaints Intake & Review

During Intake & Review of a Complaint, OCR Considers the following:

- Alleged conduct is after the Rules went into effect (2003 or 2005)
- Complaint is filed against an entity required to comply with Privacy and Security rules (i.e., not against life insurers, employers, workers compensation carriers, schools, state agencies, law enforcement agencies, municipal offices)
- Alleges an activity, that if proven true, would violate the Privacy or Security rule (i.e., does not make allegations for permitted disclosures)
- Must be filed within 180 days of when the person submitting the complaint knew or should have known of the alleged violation.

OCR Enforcement Activity: Complaints Investigation

If OCR Accepts a Complaint for Investigation:

— Notify the person who filed the complaint and covered entity.
— Both parties are asked to submit information about the alleged incident.
— If complaint describes a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), OCR may refer the complaint to DOJ for investigation.
— OCR will investigate and determine whether there is no violation of Privacy or Security Rule, or if there is noncompliance, proceed with one of following:
  — Voluntary compliance;
  — Corrective action; and/or
  — Resolution agreement.

HIPAA / Privacy Enforcement
Status of Complaints as of April 2016

<table>
<thead>
<tr>
<th>Status of All Privacy Rule Complaints – April 2016</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Complaints Remaining Open</td>
<td>5,639 (4%)</td>
</tr>
<tr>
<td>Complaints Resolved</td>
<td>126,920 (96%)</td>
</tr>
<tr>
<td>Total Complaints Received</td>
<td>132,559</td>
</tr>
</tbody>
</table>

HIPAA / Privacy Enforcement

OCR Enforcement Activity: Investigations

Investigated Resolutions
April 14, 2003 through December 31, 2014

Enforcement Results

OCR Enforcement Activity: Non-Breach Compliance Reviews

CR Non-Breach Cases Closed
Year: 2014

Total Resolutions: 30

- Corrective Action Obtained: 27 (90%)
- No Violation: 2 (7%)
- Other: 1 (3%)

Significant HHS Settlements of 2016
Through August 4, 2016, HHS has settled 10 cases through Resolution Agreements totaling more than $20 million.
Lincare (Feb. 3, 2016)

- PHI of 278 patients removed from company office, left exposed and then abandoned altogether
- Inadequate policies and procedures to safeguard PHI taken offsite even through frequent practice; unwritten policy for storing PHI in vehicles
- ALJ ruled in favor of OCR enforcement and requires Lincare to pay $239,800 civil money penalty
Complete P.T. (Feb. 16, 2016)

- Physical therapy provider
- Alleged violations that it impermissibly disclosed PHI when it posted patient testimonials, including full names and full face photo images to its website without valid HIPAA-compliant authorizations
- Settlement includes payment of $25,000, adoption and implementation of corrective action plan, and annual reporting of compliance efforts for a one year period.
North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities.

Health system allegedly failed to (1) implement a business associate agreement with a major contractor and (2) institute an organization-wide risk analysis to address risks and vulnerabilities to its patient information.

Settlement includes $1.55 Million payment and robust corrective action plan.
Feinstein Inst. for Med. Res. (March 17, 2016)

• Investigation of research institution after it filed a breach report indicating that a computer containing ePHI of 13,000 patients and research participants was stolen from employee’s car

• Improper disclosure of research participants’ PHI, computer contained ePHI of names of research participants, DOB, addresses, SSN, diagnosis, lab results, medications, and medical info for participation in study

• Agreed to pay $3.9 million to settle and will undertake a substantial corrective action plan
Raleigh Orthopaedic (April 2016)

• Provider group practice that operates clinics and orthopaedic surgery center in the Raleigh, North Carolina area

• Failed to execute a business associate agreement prior to turning over PHI of 17,300 to a potential business partner prior to turning over x-rays

• OCR initiated investigation following a breach report

• $750,000 settlement
New York Presbyterian Hospital (Apr. 21, 2016)

• Disclosed two patients’ PHI to media for filming of a tv show (NY Med) and lacked appropriate safeguards for PHI
• Media crew filmed one patient near death and another in extreme distress
• OCR determined the hospital allowed the crew to unfettered access to its facility creating an environment where PHI could not be protected
• $2.2 Million Settlement and comprehensive corrective action plan with 2 years of monitoring
Catholic Health Care Svs. (June 29, 2016)

- Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) victim of theft of mobile device which compromised the PHI of hundreds of nursing home residents, impacting 412 combined breaches
- CHCS provided management and IT services as a business associate to six skilled nursing facilities
- $650,000 settlement, amount factored in that CHCS provides unique services in Philadelphia region to the elderly, developmentally disabled, young adults aging out of foster care, and individuals living with HIV/AIDS
Oregon Health & Science Univ. (July 18, 2016)

• Oregon Health & Science Univ. (OHSU) submitted multiple breach reports affecting thousands of individuals, including two reports of unencrypted laptops and another larger breach of an unencrypted thumb drive

• OCR investigation revealed issues with HIPAA compliance program, including storage of ePHI on cloud-based server without a business associate agreement, and although OHSU conducted risk analysis for multiple years, did not cover all ePHI

• $2.7 Million settlement and three-year comprehensive corrective action plan
Univ. of Miss. Med. Ctr. (July 21, 2016)

• OCR investigation triggered by a breach of unsecured ePHI impacting nearly 10,000 individuals – password protected laptop likely stolen from ICU

• OCR investigation determined that organization was aware of risks to systems dating back to April 2005 but failed to conduct risk management until after the breach

• $2.75 Million settlement and adoption of corrective action plan
Advocate Health Care

• One of the largest health systems in the country
• OCR investigation in 2013 after Advocate submitted 3 breach notification reports, combined breaches affected ePHI of nearly 4 million individuals
• $5.55 Million settlement and adoption of a corrective action plan
• Largest settlement to date against a single entity due to the extent and duration of the alleged non-compliance, dating back to the inception of the security rule in certain instances
And That’s NOT All Folks

That’s NOT all, folks!

“TASMANIAN DEVIL”

“PORKY PIG”

“BUGS BUNNY”

“TWEETY”
Other Notable Cases Involving Privacy/Security Issues

<table>
<thead>
<tr>
<th>Date</th>
<th>Institution(s)</th>
<th>Potential Privacy/Security Violation(s) and Type of Action</th>
<th>Case Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2016</td>
<td>Millennium Laboratories/Allied World Assurance Co.</td>
<td>Millennium sought coverage from its insurer for $5 million in HIPAA coverage for a DOJ probe under directors liability policy. Insurer’s defense is that it did not owe coverage due to an exclusion for costs that related to actions the policyholder knew before it gained coverage.</td>
<td>Federal district court ruled for insurer and Millennium appealed to 9th Circuit last month</td>
</tr>
<tr>
<td>August 2016</td>
<td>Practice Fusion Inc. (cloud-based EHR company)</td>
<td>FTC finalized administrative settlement over allegations that it failed to disclose that it would post online its doctor reviews that sometimes contained sensitive personal and medical information.</td>
<td>Settled with FTC</td>
</tr>
</tbody>
</table>
Continued – Other Notable Cases

<table>
<thead>
<tr>
<th>Date</th>
<th>Institution(s)</th>
<th>Potential Privacy/Security Violation(s) and Type of Action</th>
<th>Case Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filed Dec. 2014 dismissed Feb. 2016</td>
<td>Miami Beach Healthcare Group</td>
<td>Class action stemming from unauthorized breach of hospital data involving 85,000 patient records. Judge recused self from case since her own records were a part of the breach.</td>
<td>Dismissed for failure to allege that the individual plaintiff’s PHI had actually been misused</td>
</tr>
<tr>
<td>Oct. 2015</td>
<td>Warner Chilcott</td>
<td>DOJ brought criminal charges against individuals for HIPAA violations. Three company district managers pleaded guilty to directing their sales reps. to access pt. records in MD offices to fill out prior authorizations. A physician was indicted for allowing sales reps to access pt. medical files in order to submit prior authorizations. Also had fraud and kickback charges.</td>
<td>Guilty Pleas</td>
</tr>
</tbody>
</table>
Implementation of Internal Controls and Key Takeaways
Implementation of Internal Controls & Key Takeaways

- Ensure company has conducted a complete and accurate risk analysis:
  - Must analyze potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by organization
  - Identify all of the ePHI created, maintained, received or transmitted by the company
  - Update risk analysis as necessary based on scope of practices and potential changes since last analysis
  - Understand process of contracting with third party for purposes of mitigation plan following breach
Implementation of Internal Controls & Key Takeaways

• Risk Analysis continued:
  — When identifying ePHI, consider:
    — Applications (EHR, PM, billing systems, documents/spreadsheets, database systems, web servers, fax servers, backup servers, etc.)
    — Computers (servers, workstations, laptops, virtual and cloud based systems, etc.)
    — Medical Devices (tomography, radiology, DXA, EKG, ultrasounds, spirometry, etc.)
    — Messaging Apps (email, texting, ftp, etc.)
    — Mobile and Other Devices (tablets, smartphones, copiers, digital cameras, etc.)
    — Media (tapes, CDs/DVDs, USB drives, memory cards, etc.)
Implementation of Internal Controls & Key Takeaways

• Understand company policy for recognizing and reporting HIPAA concerns to the HIPAA Privacy Officer

• Avoid storing PHI or ePHI, but if necessary:
  — Store in secure form (i.e., encrypted)
  — If there is back-up, immediately delete after use
  — Do not leave unencrypted/unsecured devices unattended (i.e., do not leave blackberry, iPhone, laptops, iPads, etc. in car or elsewhere unattended)
  — Caution with use of shared networks, storage of information on desktops, email, Box, paper files
Implementation of Internal Controls & Key Takeaways

• Avoid transmitting PHI or ePHI, but if necessary:
  — If don’t have to email, don’t. But if email is required, send in an encrypted/secure manner
  — Caution with printing, faxing, walking through open areas with PHI
  — Caution with working remotely via VPN or otherwise and not to store information on personal files

• Carefully review BAAs
  — Confirm they contain required provisions
  — Provide sufficient protections for your company
  — Understand allocation of duties
Implementation of Internal Controls & Key Takeaways

- Any legal notices related to PHI (i.e., subpoenas, court orders, etc.) should immediately be forwarded to the HIPAA Privacy Officer.
- Contact the HIPAA Privacy Officer with questions—Don’t guess, assume, or attempt to investigate issues.
- Understand scope of state law implications and how institution separately addresses.
- Understand company policies on HIPAA-compliant policies and practices including breach notification practices.
- Consider company policies related to clinical research and other sensitive areas such as securing data related to patients with HIV/AIDS.
- Be aware of company policies related to media communications (i.e., Zika and Ebola instances).
Questions?