United States Department of Health & Human Services
Office for Civil Rights

Current Trends in Data Privacy and Security Enforcement

HCCA Regional Conference – Kansas City
September 21, 2018

Steven M. Mitchell, Office for Civil Rights (OCR),
U.S. Department of Health and Human Services

Iliana L. Peters, Shareholder, Polsinelli

United States Department of Health & Human Services
Office for Civil Rights

Updates

- Policy Development
- Breach Notification
- Enforcement
- Audit

United States Department of Health & Human Services
Office for Civil Rights

POLICY DEVELOPMENT

United States Department of Health & Human Services
Office for Civil Rights

Title XI: Compassionate Communication on HIPAA

New OCR Guidance on HIPAA and Information Related to Mental and Behavioral Health

- Opioid Overdose Guidance (issued 10/27/2017)
- Updated Guidance on Sharing Information Related to Mental Health (new additions to 2014 guidance)
- 30 Frequently Asked Questions:
  - New tab for mental health in "FAQs for Professionals"
  - 9 new FAQs added (as PDF and in database)
- New Materials for Professionals and Consumers
  - Fact Sheets for Specific Audiences
  - Information-sharing Decision Charts

United States Department of Health & Human Services
Office for Civil Rights

Where to Find OCR's New Materials

OCR Website Navigation

- For professionals: https://www.hhs.gov/hipaa/for-professionals/index.html > Special Topics > Mental Health & Substance Use Disorders
- For consumers: https://www.hhs.gov/hipaa/for-individuals/index.html > Mental Health & Substance Use Disorders
- Mental Health FAQ Database: https://www.hhs.gov/hipaa/for-professionals/faq/mental-health

United States Department of Health & Human Services
Office for Civil Rights

Platform for users to influence guidance
http://hipaaQsportal.hhs.gov

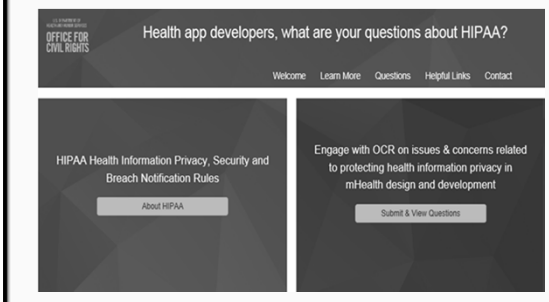
HIT Developer Portal

- OCR launched platform for mobile health developers in October 2015; purpose is to understand concerns of developers new to health care industry and HIPAA standards
- Users can submit questions, comment on other submissions, vote on relevancy of topic
- OCR will consider comments as we develop our priorities for additional guidance and technical assistance
- Guidance issued in February 2016 about how HIPAA might apply to a range of health app use scenarios
- FTC/ONC/OCR/FDA Mobile Health Apps Interactive Tool on Which Laws Apply issued in April 2016

United States Department of Health & Human Services

Office for Civil Rights

Platform for users to influence guidance
http://hipaaQsportal.hhs.gov



October 2015

United States Department of Health & Human Services

Office for Civil Rights

Cloud Guidance

Cloud Computing Guidance

- OCR released guidance clarifying that a CSP is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.
- When a CSP stores and/or processes ePHI for a covered entity or business associate, that CSP is a business associate under HIPAA, even if the CSP stores the ePHI in encrypted form and does not have the key.
- CSPs are not likely to be considered "conduits," because their services typically involve storage of ePHI on more than a temporary basis.
- http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

United States Department of Health & Human Services

Office for Civil Rights

New Cybersecurity Guidance page

Cyber Security Guidance Material

- HHS OCR has launched a Cyber Security Guidance Material webpage, including a Cyber Security Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.
  - Cyber Security Checklist - PDF
  - Cyber Security Infographic [GIF 802 KB]

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Cybersecurity Newsletters

- Began in January 2016
- Recent 2017-2018 Newsletters
  - October 2017 (Mobile Devices and PHI)
  - November 2017 (Insider Threats and Termination Procedures)
  - December 2017 (Cybersecurity While on Holiday)
  - January 2018 (Cyber Extortion)
  - February 2018 (Phishing)
  - March 2018 (Contingency Planning)
  - April 2018 (Risk Analyses vs. Gap Analyses)
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Ransomware Guidance

- OCR guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.
- http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

United States Department of Health & Human Services
Office for Civil Rights

Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted
- OCR posts breaches affecting 500+ individuals on OCR website

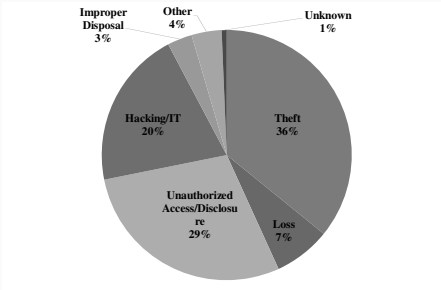
United States Department of Health & Human Services
Office for Civil Rights

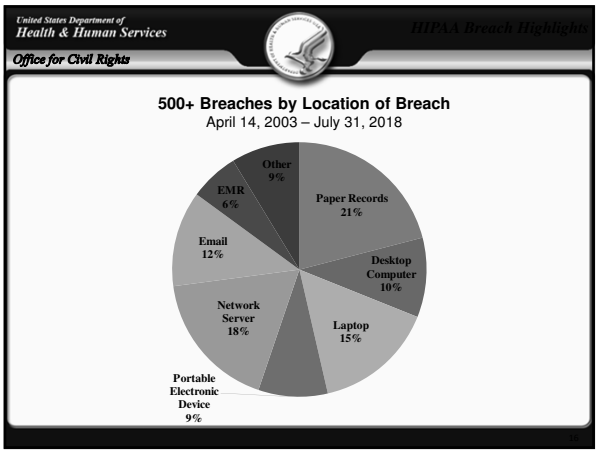
September 2009 through July 31, 2018

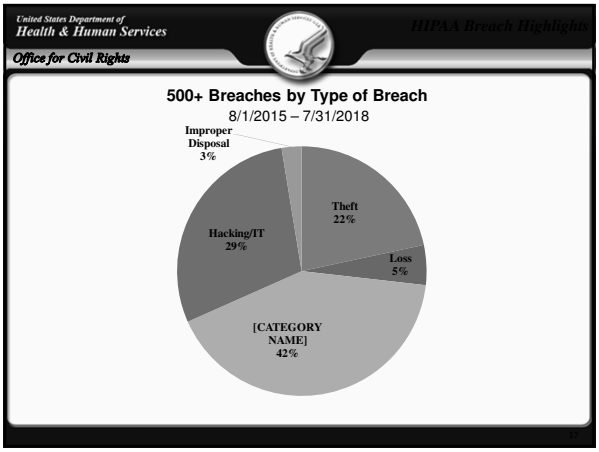
- Approximately 2,393 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 43% of large breaches
  - Hacking/IT now account for 20% of incidents
  - Laptops and other portable storage devices account for 24% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 264,728,418
- Approximately 354,334 reports of breaches of PHI affecting fewer than 500 individuals

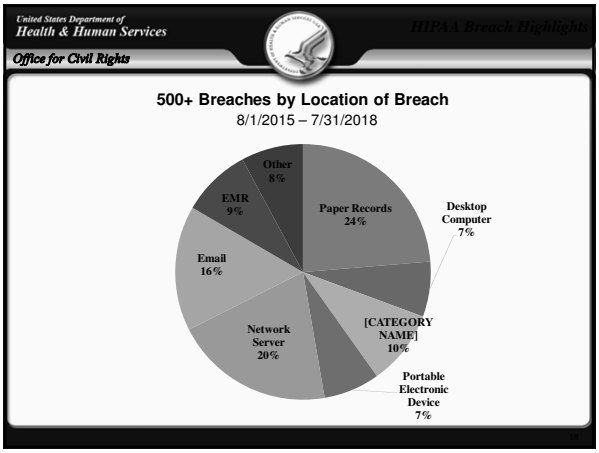
United States Department of Health & Human Services
Office for Civil Rights

500+ Breaches by Type of Breach
April 14, 2003 – July 31, 2018




United States Department of Health & Human Services
Office for Civil Rights
HIPAA Breach Highlights
500+ Breaches by Location of Breach
April 14, 2003 – July 31, 2018
Other 9%
EMR 6%
Paper Records 21%
Email 12%
Desktop Computer 10%
Network Server 18%
Laptop 15%
Portable Electronic Device 9%


United States Department of Health & Human Services
Office for Civil Rights
HIPAA Breach Highlights
500+ Breaches by Type of Breach
8/1/2015 – 7/31/2018
Improper Disposal 3%
Theft 22%
Hacking/IT 29%
Loss 5%
[CATEGORY NAME] 42%


United States Department of Health & Human Services
Office for Civil Rights
HIPAA Breach Highlights
500+ Breaches by Location of Breach
8/1/2015 – 7/31/2018
Other 8%
EMR 9%
Paper Records 24%
Desktop Computer 7%
Email 16%
[CATEGORY NAME] 10%
Network Server 20%
Portable Electronic Device 7%

United States Department of Health & Human Services
Office for Civil Rights

What Happens When HHS/OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity's compliance prior to breach

United States Department of Health & Human Services
Office for Civil Rights

General Enforcement Highlights

General HIPAA Enforcement Highlights as of April 14, 2003 – July 31, 2018

- Over 186,453 complaints received to date
- Over 26,152 cases resolved with corrective action and/or technical assistance
- Expect to receive 24,000 complaints this year

United States Department of Health & Human Services
Office for Civil Rights

General Enforcement Highlights

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 52 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 4 civil money penalties

Recent HHS Enforcement Actions

- April 24, 2017: CardioNet
  - $2,500,000
  - $2.5 million settlement shows that not understanding HIPAA requirements creates risk
- May 10, 2017: Memorial Hermann Health System (MHHS)
  - $2,400,000
  - Texas health system settles potential HIPAA violations for disclosing patient information
- May 23, 2017: St. Luke's Roosevelt Hospital System Inc.
  - $387,200
  - Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k
- December 18, 2017: 21st Century Oncology
  - $2,300,000
  - $2.3 Million Levied for Multiple HIPAA Violations at NY-Based Provider
- February 1, 2018: Fresenius Medical Care North America (FMCNA)
  - $3,500,000
  - Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules
- February 13, 2018: Filefax, Inc.
  - $100,000
  - Consequences for HIPAA violations don't stop when a business closes
- June 18, 2018: MD Anderson
  - $4.3 Million CMP
  - Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations

22

Recent FTC Enforcement Actions

- June 6, 2018
  - U.S. Court of Appeals, 11th Circuit Ruling in LabMD, Inc.
  - http://media.ca11.uscourts.gov/opinions/pub/files/201616270.pdf
- Feb 27, 2018:
  - PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act
- Nov 29, 2017:
  - FTC Gives Final Approval to Settlements with Companies that Falsely Claimed Participation in Privacy Shield
- Nov 8, 2017:
  - FTC Gives Final Approval to Settlement with Online Tax Preparation Service
- Aug 15, 2017:
  - Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

23

United States Department of Health & Human Services
Office for Civil Rights

Recurring Compliance Issues

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

24

Risk Analysis

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization]. See 45 C.F.R. § 164.308(a)(1)(ii)(A).
- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.
- When identifying ePHI, be sure to consider:
  - Applications (EHR, PM, billing systems; documents and spreadsheets; database systems and 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.)
- April 24, 2017: CardioNet
  - $2,500,000
  - $2.5 million settlement shows that not understanding HIPAA requirements creates risk

25

HHS Risk Analysis Guidance

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment
- https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf

26

FTC Resources

- https://www.ftc.gov/
- https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
- https://www.ftc.gov/news-events/press-releases/2018/02/ftc-recommends-steps-improve-mobile-device-security-update
- https://www.ftc.gov/news-events/press-releases/2018/02/ftc-report-finds-some-small-business-web-hosting-services-could

27

Business Associate Agreements

- The HIPAA Rules generally require that covered entities and business associates enter into agreements with their business associates to ensure that the business associates will appropriately safeguard protected health information. See 45 C.F.R. § 164.308(b).
- April 20, 2017: Center for Children's Digestive Health
  - $37,000
  - No Business Associate Agreement? $31K Mistake
- February 13, 2018: Filefax, Inc.
  - $100,000
  - Consequences for HIPAA violations don't stop when a business closes

Vendor Cyber Risk Management

- FTC Guidance: https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series
- NIST Guidance: https://www.nist.gov/cyberframework
- HHS Cloud Guidance: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- HHS Business Associate Guidance: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es
- Remote Access Issues

29

Insider Threat

- Organizations must "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information," as part of its Workforce Security plan. See 45 C.F.R. § 164.308(a)(3).
- Appropriate workforce screening procedures could be included as part of an organization's Workforce Clearance process (e.g., background and OIG LEIE checks). See 45 C.F.R. § 164.308(a)(3)(ii)(B).
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization's workforce exit or separation process. See 45 C.F.R. § 164.308(a)(3)(ii)(C).
- February 16, 2017: Memorial Healthcare System (MHS)
  - $5.5 Million
  - https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html

30

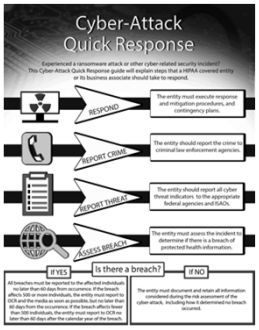
Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. See 45 C.F.R. § 164.312(e)(2)(ii).
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)
- June 10, 2015: St. Elizabeth's Medical Center (SEMC)
  - $218,400
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html

31

Ransomware Attacks

- Phishing and Ransomware
  - Security Awareness and Training and Security Reminders
  - Be Prepared
  - Practice!



32

Software Patching

- The use of unpatched or unsupported software on systems which access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software which should be monitored for patches and vendor end-of-life for support include:
  - Router and firewall firmware
  - Anti-virus and anti-malware software
  - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

33

Training

- Most settlements include a training requirement
  - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
- OCR Published a Monthly Cybersecurity Newsletter
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html
- OCR YouTube Page
  - https://www.youtube.com/user/USGovHHSOCR

34

United States Department of Health & Human Services
Office for Civil Rights

Corrective Action

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- Implementing specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

United States Department of Health & Human Services
Office for Civil Rights

Best Practices

Some Best Practices:

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

United States Department of Health & Human Services
Office for Civil Rights
Audit Program

AUDIT

United States Department of Health & Human Services
Office for Civil Rights
Audit Program

HITECH Audit Program

- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open a compliance review (for example, if significant concerns are raised during an audit)
  - Learn from Phase 2 in structuring permanent audit program

United States Department of Health & Human Services
Office for Civil Rights
Audit Program

History

- HITECH legislation: HHS (OCR) shall provide for periodic audits to ensure that covered entities and business associates comply with HIPAA regulations. (Section 13411)
- Pilot phase (2011-2012) – comprehensive, on-site audits of 115 covered entities
- Evaluation of Pilot (2013) – issuance of formal evaluation report of pilot audit program
- Phase 2 (2016-2017) - desk audits of 207 covered entities and business associates

United States Department of Health & Human Services
Office for Civil Rights

Phase 2 - Selected Desk Audit Provisions

- For Covered Entities:
  - Security Rule: risk analysis and risk management;
  - Breach Notification Rule: content and timeliness of notifications; **or**
  - Privacy Rule: NPP and individual access right
- For Business Associates:
  - Security Rule: risk analysis and risk management **and**
  - Breach Notification Rule: reporting to covered entity
- See auditee protocol guidance for more details: http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

United States Department of Health & Human Services
Office for Civil Rights

Status

- 166 covered entity and 41 business associate desk audits were completed in December 2017
- Website updates with summary findings will be published in 2018

United States Department of Health & Human Services
Office for Civil Rights

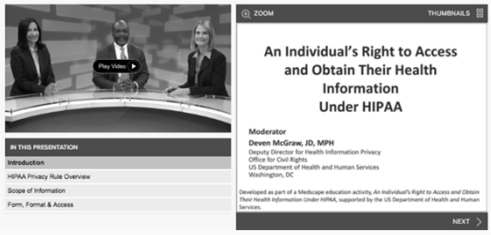
Provider Education: An Individual's Right to Access and Obtain their Health Information Under HIPAA

United States Department of Health & Human Services

Office for Civil Rights

Provider Education

Web-based Video Training for Free Continuing Medical Education and Continuing Education Credit for Health Care Professionals via Medscape



http://www.medscape.org/viewarticle/876110

United States Department of Health & Human Services

Office for Civil Rights

Consumer Facing Resources:

Right to Access Your Health Information Under HIPAA

United States Department of Health & Human Services

Office for Civil Rights

New Consumer Facing Tools

Phase 2 of OCR's *Information is Powerful Medicine* Campaign

United States Department of Health & Human Services

Office for Civil Rights

Pocket Brochure, Exterior and Interior Flap

Information is key to making good health care decisions. Understand your health history to ask better questions and make healthier choices. Track your lab results and medications, get x-rays and other medical images, or share your information with a caregiver or a research program.

United States Department of Health & Human Services

Office for Civil Rights

Pocket Brochure Interior View

Clear and concise

- **Get it:** Covers Form and Format and Manner of Access, Time and Timeliness, Fees
- **Check it:** Check to make sure your health information is correct and complete
- **Use it:** Right to Third Party Access, including a researcher.

United States Department of Health & Human Services

Office for Civil Rights

HHS.gov/GetItCheckItUseIt

Clear and concise

- Links to Fact Sheets and FAQs
- Videos
- Poster
- Brochure
- Digital Ads and Banners
- Mobile Platform
- Link to Join All of Us Research Initiative

United States Department of Health & Human Services

Office for Civil Rights

More Information

http://www.hhs.gov/hipaa

Join us on Twitter @hhsocr

steven.mitchell@hhs.gov

816-426-7278

49

Questions?

- Feel free to contact me for more information:
  - Iliana Peters: ipeters@polsinelli.com

50

POLSINELLI

Polsinelli PC, Polsinelli LLP in California | polsinelli.com

51