2018 HCCA Compliance Institute HIPAA Update: Policy & Enforcement

Policy Update:
Marissa Gordon-Nguyen
HHS OCR Senior Advisor

2

OCR Responds to Nation's Opioid Crisis

- Opioid abuse crisis and national health emergencies have heightened concerns about providers':
  - ability to notify patients' family and friends when a patient has overdosed
  - reluctance to share health information with patients' families in an emergency or crisis situation, particularly patients with serious mental illness and substance use disorder
  - uncertainty about HIPAA permissions for sharing information when a patient is incapacitated or presents a threat to self or others

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 Materials for Professionals and Consumers
  - Fact Sheets for patients, families, and health care providers
  - Information-sharing Decision Charts

Dangerous Patients and Public Safety Disclosures

- Disclosures are permitted without the patient's authorization or permission to law enforcement, family, friends or others who are in a position to lessen the threatened harm—when disclosure "is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others."
- Disclosures must be consistent with applicable law.

Where to Find OCR's New Materials

- 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
- Future FERPA and HIPAA Joint Guidance

Proposed Changes to HIPAA Privacy and Enforcement Rules

- NPRM on Presumption of Good Faith of Health Care Providers
- NPRM on Changing Requirement to Obtain Acknowledgment of Receipt of Notice of Privacy Practices
- Request for Information on Distribution of a Percentage of Civil Monetary Penalties or Monetary Settlements to Harmed Individuals

Future HIPAA Guidance

- Texting
- Social Media
- Encryption

Cybersecurity Resources

- Newsletters http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- Health Information Technology Portal http://hipaaQsportal.hhs.gov
- Medscape *http://www.medscape.org/viewarticle/876110*

Enforcement Update:
Iliana L. Peters
Shareholder, Polsinelli, PC

HIPAA Breach Highlights

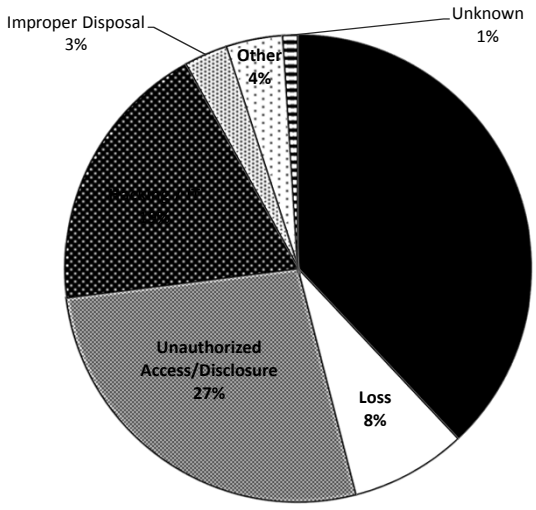
September 2009 – December 31, 2017

- Approximately 2,178 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 46% of large breaches
  - Hacking/IT now account for 19% of incidents
  - Laptops and other portable storage devices account for 25% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 176,589,175
- Approximately 307,061 reports of breaches of PHI affecting fewer than 500 individuals

11

HIPAA Breach Highlights

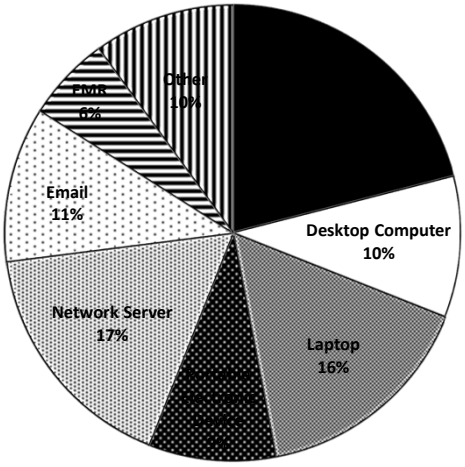
500+ Breaches by Type of Beach as of December 31, 2017



12

HIPAA Breach Highlights

500+ Breaches by Location of Beach as of December 31, 2017



13

General Enforcement Highlights

- Over 171,161 complaints received to date
- Over 25,637 cases resolved with corrective action and/or technical assistance
- Expect to receive 17,000 complaints

As of 12/31/2017

14

Recent 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

15

Audit Update: Marissa Gordon-Nguyen

16

Audit Program

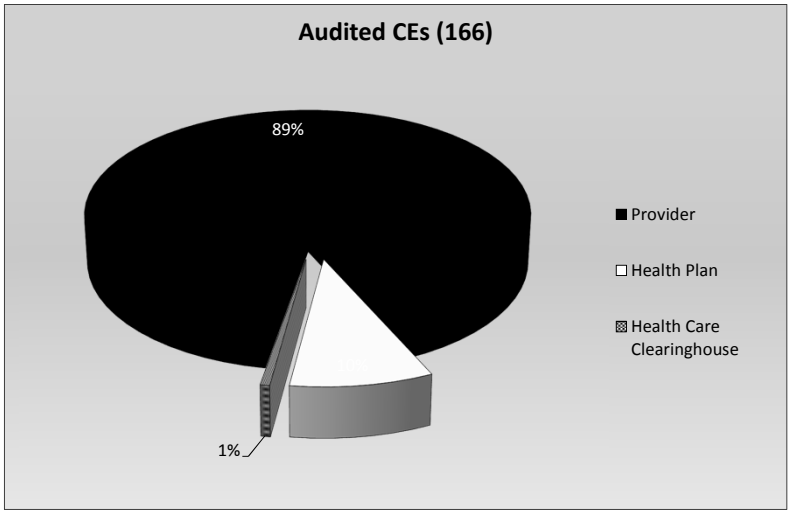
- Purpose: Identify best practices; uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
  - Also hope to learn from this next phase in structuring permanent audit program

17

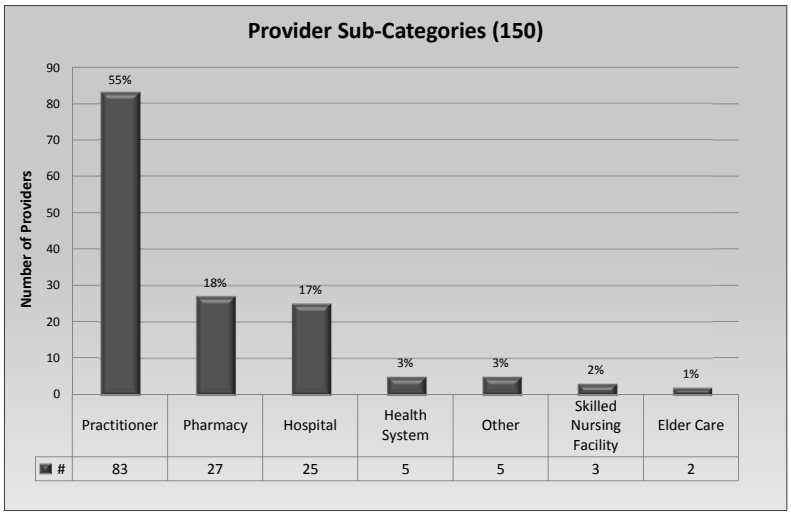
Audit Program Purpose & Status

- Support Improved Compliance
- Identify best practices; uncover risks & vulnerabilities; detect areas for technical assistance; encourage consistent attention to compliance
  - Intended to be non-punitive, but OCR can open up compliance review
- Learn from this phase in structuring permanent audit program
- Develop tools and guidance for industry self-evaluation and breach prevention
- Desk audits of covered entities completed – Sept 2017
- Desk audits of business associates completed – Dec 2017

Audited Covered Entities



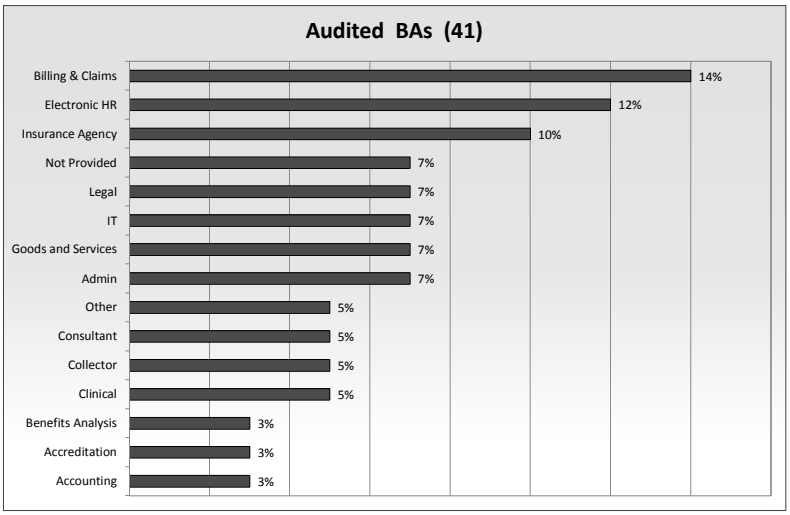
Audited Health Care Providers



Covered Entity Desk Audit Controls

Privacy Rule Controls	Notice of Privacy Practices & Content Requirements [§164.520(a)(1) & (b)(1)]
	Provision of Notice – Electronic Notice [§164.520(c)(3)]
	Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]
Breach Notification Rule Controls	Notification by a Business Associate [§164.410, with reference to Content of Notification §164.404(c)(1)]
Security Rule Controls	Security Management Process -- Risk Analysis [§164.308(a)(1)(ii)(A)]
	Security Management Process -- Risk Management [§164.308(a)(1)(ii)(B)]

Audited Business Associates



Business Associate Desk Audit Controls

Breach Notification Rule Controls	Notification by a Business Associate [§164.410, with reference to Content of Notification §164.404(c)(1)]
Security Rule Controls	Security Management Process -- Risk Analysis [§164.308(a)(1)(ii)(A)]
	Security Management Process -- Risk Management [§164.308(a)(1)(ii)(B)]

Ratings

Compliance Effort Ratings—Legend	
Rating	**Description**
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.

CE Desk Audit Ratings

		Rating					
Element #	Provision	1	2	3	4	5	N/A
P55	Notice	2	34	40	11	16	0
P58	eNotice	59	16	4	6	15	3
P65	Access	1	10	27	54	11	0
BNR 12	Timeliness	67	6	2	9	12	7
BNR13	Content	14	15	24	38	7	5
S2	Risk Analysis	0	9	20	21	13	0
S3	Risk Management	2	2	15	28	16	0

BA Desk Audit Ratings

		Rating					
Element #	Provision	1	2	3	4	5	N/A
BNR17	Notice to CEs	0	2	4	3	0	32
S2	Risk Analysis	3	4	16	12	6	0
S3	Risk Management	0	5	8	21	7	0

Industry Take-Away

Best Outcomes

- Providing timely notice of breach
- Posting of NPP on website
- Providing required NPP content

OCR will examine entity practices for lessons learned that can be shared in technical assistance

Most Room for Improvement

- Risk Management
- Risk Analysis
- Enabling Individual Access

Review OCR guidance and technical assistance

OCR is working to enhance technical assistance in those areas

Top Ten Compliance Issues: Iliana L. Peters

28

Recurring Compliance Issues

- Pattern of Disclosure of Sensitive Paper PHI
- 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

29

Recent FTC Enforcement Actions

- 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

30

OCR Resources

- https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- https://www.hhs.gov/hipaa/for-professionals/security/index.html
- https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

31

Polsinelli Resources

- **Polsinelli serves clients nationally:**
  - https://www.polsinelli.com/
  - **100+** services and **70+** industry areas
  - **800+** Attorneys
  - https://www.polsinelli.com/professionals/ipeters
  - **20 Cities – Metropolitan offices in:**
    - Atlanta
    - Boston
    - Chicago
    - Dallas
    - Denver
    - Houston
    - Kansas City
    - Los Angeles
    - Nashville
    - New York
    - Phoenix
    - St. Louis
    - San Francisco
    - Silicon Valley
    - Washington, D.C.
    - Wilmington

32