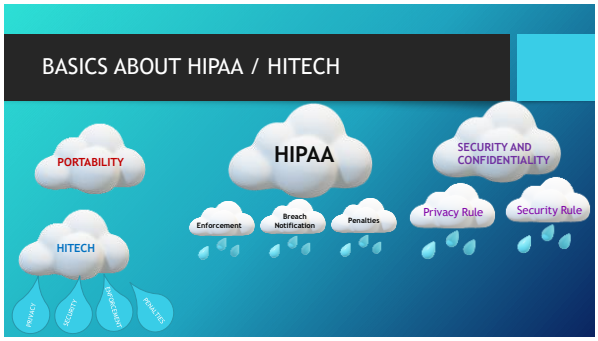
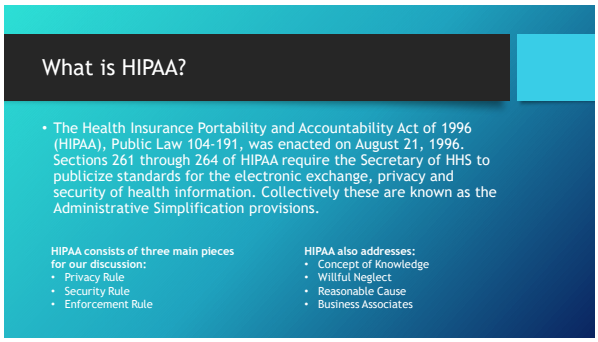

HIPAA Compliance
For Privacy Officer
EXCELLENTIA
Presented by:
Roger Manning
Managing Partner
Excellentia Advisory Group

1


BASICS ABOUT HIPAA / HITECH
PORTABILITY
HIPAA
SECURITY AND CONFIDENTIALITY
HITECH
Enforcement
Breach Notification
Penalties
Privacy Rule
Security Rule
PRIVACY
SECURITY
ENFORCEMENT
PENALTIES

2


What is HIPAA?
• The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the Administrative Simplification provisions.
HIPAA consists of three main pieces for our discussion:
• Privacy Rule
• Security Rule
• Enforcement Rule
HIPAA also addresses:
• Concept of Knowledge
• Willful Neglect
• Reasonable Cause
• Business Associates

3

What is Protected Health Information (PHI)?

- The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e .g ., name, address, birth date, Social Security Number).

4

WHAT ARE IDENTIFIERS?

- Name
- Address
- Date of Birth
- Telephone or fax numbers
- Email address
- Medical Record Number or Account #
- License numbers of any kind (Drivers, Professional)
- Account Number
- Photos
- Social Security Number
- Health Plan beneficiary number
- Or any documents that contain any one or combinations of personal information such as residence in facility or special facility (ie: behavioral health, addiction, etc.)

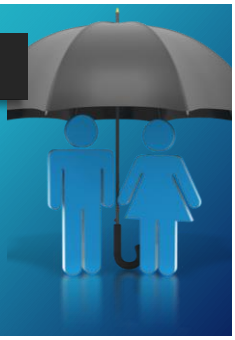
5

Who Must Comply with HIPAA as Covered Entities?

Healthcare Providers	Health Plans	Health Care Clearinghouse
DOCTORS	Health Insurance Companies	Any entity that processes non-standard health info…
CLINICS	HMOs	From another entity
PSYCHOLOGISTS	PPOs / Other Health Plans	
DENTISTS	Case Managers	
CHIROPRACTORS	Other Third-Party Payors	
NURSING HOMES	Any government program that pays of healthcare….	
PHARMACIES	Medicare, Medicaid, VA and	
HOSPITALS	Military programs	
SURGERY CENTERS		

6

BUSINESS ASSOCIATES



- Originally not covered under HIPAA but not through HITECH act
- BAs are covered entities
- If the entity or individual providing services will need to have access or will be in position to observe PHI unintentionally, then they will need to sign a Business Associates agreement.
- Business Associates should have their own training but when in doubt, put them through your HIPAA training

7

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

- Passed in 2009 but deadline was September 2013 to finalize
- Adopted to encourage community to adopt "meaningful use" of EHR.
  - Better Coordination
  - Reduce Disparities
  - Improve Public Health
- Ensure info is adequately secured
- Dictates how Business Associates are viewed under HIPAA. BAs are required to be HIPAA-compliant.
- Breach Notification Rule - notify individuals within 60 days. If over 500 people are affected, must notify H.H.S.
- Provides for Consumer Rights to have access to their EHR
- Prohibits using PHI for marketing purposes

8

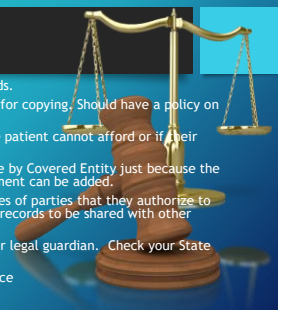
MINIMUM NECESSARY RULE

- A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

- A HIPAA-covered entity (CE) must have written policies on provided Protected Health Information to reasonably limit uses and disclosures to the minimum necessary.
- When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.
- De-identify information when possible

9

CONSUMER RIGHTS



- Patients have a right to their medical records.
- You have a right to charge a reasonable fee for copying. Should have a policy on this ie: costs, time frame to deliver
- Cannot deny access to medical record if the patient cannot afford or if their surgery center / clinic bill is overdue.
- Changing or Altering Records cannot be done by Covered Entity just because the patient requests it. Statement of Disagreement can be added.
- Patient must give an authorization and names of parties that they authorize to have information shared with as well as for records to be shared with other covered entity providers or BAs.
- Have a right for a Personal Representative or legal guardian. Check your State Laws.
- Have a right to receive a Privacy Policy Notice

10

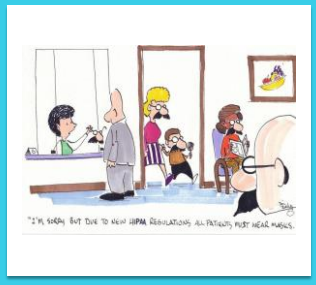
PRIVACY RULE –ACTION PLAN

- Keep conversations private – private areas, sound-proofed rooms, use of first name only, quieter speaking tone.
- When listening to voice mail messages, DO NOT USE SPEAKER PHONE!
- If you happen to see a patient in the public place, be very careful in greeting them. They may not want others to know they have been a patient of yours.
- Keep caregiver traffic conversations away from the front desk area and keep noise levels to a minimum in that area.

11

WAYS TO PROTECT PRIVACY

When calling patients in waiting rooms for appointments or talking to them in our healthcare facilities, talk to them in a way that does not disclose their full name, doctor, or reason for their visit to others who may overhear.



12

WAYS TO PROTECT PRIVACY

- Being sure no one can see your computer screen while you are working.
- Never sharing your access code.
- Logging off when not working on your computer.
- Changing your code and notifying your supervisor if your code becomes known by anyone else.

13

WAYS TO PROTECT PRIVACY

- Even when a patient has someone with them, they may not want that person to hear their private information, so ask the person to wait outside. If the patient requests them to stay, that is OK.
- Do not post patients' names and diagnosis or doctor's name and private information in any public areas such as waiting rooms, nursing stations, or assignment boards.
- Never leave documents unattended.
- Store, file, shred, or destroy according to your departmental policy.
- Make sure fax numbers are correct and use a cover sheet with a confidentiality statement.
- Leave minimal information on voice mail messages.

14

WHEN MUST COVERED ENTITY DISCLOSE?

- If an individual patient requests access to their health information, you must provide it.
- To officials from HHS during an investigation
- During an emergency situation that could impact the life of the individual

15

WHEN MINIMUM NECESSARY RULE – NOT IMPOSED

(a) disclosure to or a request by a health care provider for treatment;

(b) disclosure to an individual who is the subject of the information, or the individual's personal representative;

(c) use or disclosure made pursuant to an authorization;

(d) disclosure to HHS for complaint investigation, compliance review or enforcement;

(e) use or disclosure that is required by law; or

(f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules. (ie: These standards are often referred to as electronic data interchange or EDI standards)

16

LIMITING THE USES BY COVERED ENTITIES

- Limited access to keep within the scope of job duties;
  - Identify either persons, classifications or job titles who need PHI access
- Have Policies & Procedures for routine, recurring disclosures, or requests for medical records to keep to minimum necessary;
- Policies in place for non-recurring disclosure requests such as Reasonable Reliance ie:
  - Professional associated with patient (ie: attorney, accountant, guardian, Power of Attorney)
  - Business Associate Agreement (ie: Boston Scientific, Stryker, Med School students)
  - Emergency staff
  - Researcher

17

FAQs

- Can I share PHI with a business associate without prior authorization? YES
- Do I still need to adhere to HIPAA during a public health emergency? NO
- What an unresponsive individual or a child? What about locating the individual's family members? NO and YES
- Can I share PHI with a Workers Comp representative? YES
- When should I release PHI to a police officer? YES and NO

18

FAQs

- What are the rules regarding leaving messages for patients? Can my office send reminder emails? What about voicemails?
- What am I allowed to disclose to family and friends in the waiting room?
- Are there limits to what I can or should disclose to family and friends?
- Can I use interpreters to discuss medical conditions or treatment options?

19

RECORDS RETENTION 45 C.F.R. § 164.530(j)

- A covered entity must maintain, until **six years after** the later of the date of their creation or **last effective date**, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented .

20

RECORDS RETENTION – EMPLOYMENT RECORDS

- State and Federal Laws regulate the retaining and access to certain PHI or other Personally Identifiable Information in employment records.
  - SSNs, I-9 forms and Medical Records
- First, I-9s must be kept separate from rest of personnel files. Locked.
- Second, check any employment forms for SSNs. If any are found, they must be kept separate from main file and locked.
- Employee medical records should be kept separate and locked.
- Limited access should be granted to the sensitive Personal Information.
- Policy should be in place for HIPAA training and confidentiality agreement signed by all employees.

21

SECURITY RULE

- A major goal of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

22

SECURITY RULE – ADMINISTRATIVE SAFEGUARDS

23

RISK ASSESSMENT

A Risk Assessment and analysis process includes but not limited to:

- Evaluate the likelihood and impact of potential risks to e-PHI;
- Implement appropriate security measures to address the risks identified in the risk analysis;
- Document the chosen security measures and, where required, the rationale for adopting those measures;
- Identify those individuals responsible for correcting risks;
- Set target dates of completion, and
- Maintain continuous, reasonable, and appropriate security protections.

24

RISK ASSESSEMENT TOOLS

- HIPAA Physical Risk Assessment
- HIPAA Technology Security Risk Assessment
- HIPAA Administrative Risk Assessment

25

PHYSICAL RISK ASSESSMENT EXAMPLES

- PH1 - §164.310(a)(1) Standard Do you have an inventory of the physical systems, devices, and media in your office space that are used to store or contain ePHI?
- PH2 - §164.310(a)(1) Standard Do you have policies and procedures for the physical protection of your facilities and equipment? This includes controlling the environment inside the facility.
- PH4 - §164.310(a)(1) Standard Do you have physical protections in place to manage physical security risks, such as a) locks on doors and windows and b) cameras in nonpublic areas to monitor all entrances and exits?
- PH5 - §164.310(a)(2)(ii) Addressable Do you plan and coordinate physical (facilities) and technical (information systems, mobile devices, or workstations) security-related activities (such as testing) before doing such activities to reduce the impact on your practice assets and individuals?
- PH6 - §164.310(a)(2)(ii) Addressable Have you developed policies and procedures that plan for your workforce (and your information technology service provider or contracted information technology support) to gain access to your facility and its ePHI during a disaster?
- PH7 - §164.310(a)(2)(i) Addressable If a disaster happens, does your practice have another way to get into your facility or offsite storage location to get your ePHI?
- PH8 - §164.310(a)(2)(iii) Addressable Do you have policies and procedures for the protection of keys, combinations, and similar physical access controls?
- PH9 - §164.310(a)(2)(iii) Addressable Do you have policies and procedures governing when to re-key locks or change combinations when, for example, a key is lost, a combination is compromised, or a workforce member is transferred or terminated?
- H10 - §164.310(a)(2)(ii) Addressable Do you have a written facility security plan?
- PH11 - §164.310(a)(2)(iii) Addressable Do you take the steps necessary to implement your facility security plan?

26

THE TOOL

HIPAA SECURITY RISK ASSESSMENT-PHYSICAL									
Performed by Excellentia Advisory Group, LLC			Date:	July 12, 2019 - XYZ Surgery Center					
Surveyor Initials	Key Activity	Policy	Risk	Impact	Responsible Party	Remediation Plan	Deadline		
	PH1 - §164.310(a)(1) Standard Do you have an inventory of the physical systems, devices, and media in your office space that are used to store or contain ePHI?								

27

ADMINISTRATIVE RISK ASSESSMENT

- A61 - §164.308(b)(1) Standard Does your practice maintain a list of all of its service providers, indicating which have access to your practice's facilities, information systems and ePHI?
- A62 - §164.308(b)(1) Standard Does your practice have policies and implement procedures to assure it obtains business associate agreements?
- A63 - §164.308(b)(2) Required If your practice is the business associate of another covered entity and your practice has subcontractors performing activities to help carry out the activities that you have agreed to carry out for the other covered entity that involve ePHI, does your practice require these subcontractors to provide satisfactory assurances for the protection of the ePHI?
- A64 - §164.308(b)(3) Required Does your practice execute business associate agreements when it has a contractor creating, transmitting or storing ePHI?
- O1 - §164.314(a)(1)(i) Standard Does your practice assure that its business associate agreements include satisfactory assurances for safeguarding ePHI?
- O2 - §164.314(a)(2)(i) Required Do the terms and conditions of your practice's business associate agreements state that the business associate will implement appropriate security safeguards to protect the privacy, confidentiality, integrity, and availability of ePHI that it collects, creates, maintains, or transmits on behalf of the practice and timely report security incidents to your practice?

28

THE TOOL

HIPAA SECURITY RISK ASSESSMENT-ADMINISTRATIVE

Performed by Excellentia Advisory Group, LLC Date: July 12, 2019 -XYZ Surgery Center

Surveyor Initials	Key Activity	Policy	Risk	Impact	Responsible Party	Remediation Plan	Deadline
	A1 - §164.308(a)(1)(i) Standard Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its electronic protected health information (ePHI)? How well are they followed?						

29

HOW TO KEEP YOUR ASC / CLINIC COMPLIANT

- Creating log-ins with lock capability after 5 minutes of inactivity
- Securing log-ins - limiting access for virtual log-ins
- Passwords
- Don't allow employees to use thumb-drives or ability to download to external devices
- Telephone call back
- Automatic log off and audit trail
- Security and separate information
- On-going training

30

EMPLOYEE TRAINING

- Upon New Hire
- Annually
- Periodically if observations or Risk Assessment mandate
- Consider employee classification-specific training
  - Clinicians get different training than front desk personnel
- Training on Scope of Duties
- Training dependent on environment
  - Paper vs. electronic
  - Diversification of electronics and scope or size of organization

31

ENFORCEMENT RULE – CONCEPT OF KNOWLEDGE

In order to properly enforce a violation, the level of knowledge must be established.

- Knowledge that the violation took place.
- "Lack of knowledge" is not an acceptable excuse if due to a failure to self-inform about compliance obligations or to investigate complaints or other indications of non-compliance.

Remember – "Ignorance of the law is no excuse."

32

ENFORCEMENT RULE – CONCEPT OF KNOWLEDGE

Willful Neglect

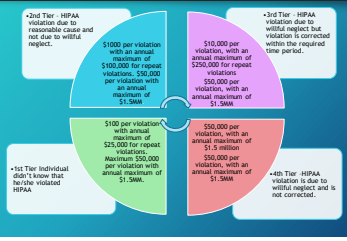
- Defined as the "conscious, intentional failure or reckless indifference to the obligations" to comply with HIPAA

Reasonable Cause

- Shown not to be willful neglect.
- **For example**, a company went into a HIPAA audit and provided a gap analysis that was incomplete because a particular item had not yet been addressed. The violation is due to reasonable cause and not willful neglect.
- **Minimum fine:** $1,000 per incident with annual maximum of $100,000 for repeat violations.
- **Maximum fine:** $50,000 per incident with annual maximum of $1.5 million for repeat violations.
-

33

ENFORCEMENT RULE



34

HIPAA BREACH GUIDELINES

BREACH NOTIFICATION RULE

- The HIPAA Breach Notification Rule, 45 CFR §§ 164 .400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
- **Site reference:** http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

35

HIPAA BREACH GUIDELINES

BREACH DEFINITION

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

- An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least one of the following factors:
- The nature and extent of the protected health information involved, including the types of identifiers released for identification;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

36

BREACH REPORTING STEPS

- Notify the Individuals
- Place Notice on home page of website, if applicable
- Media – more than 500 or if 10+ individuals can't be contacted
- Provide remedy, toll free number, credit monitoring, etc.
- All of the above within 60 days
- Secretary of HHS within 60 days if >500 people affected
- Notify HHS within 60 days of year-end if <500 people affected

Alert! – Personal Liability Check

When the HHS investigates and they find the physician has **appropriate safeguards** regarding the employee access to medical records and he had delivered **adequate training** to the employee, the employee's knowledge of the violation **cannot be passed on to the physician** because the employee was acting adversely to the covered entity.

37

IS THIS REALLY SOMETHING THAT HAPPENS?

Date	Organization	Fine Total	Link to OCR Settlement
February 7, 2019	Cottage Health	$3,000,000	Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million
May 6, 2019	Touchstone Medical Imaging	$3,000,000	Tennessee Diagnostic Medical Imaging Services Company Pays $3,000,000 to Settle Breach Exposing Over 300,000 Patients' Protected Health Information
May 23, 2019	Medical Informatics Engineering	$100,000	Indiana Medical Records Service Pays $100,000 to Settle HIPAA Breach – May 23, 2019
September9, 2019	Bayfront Health St. Petersburg	$85,000	OCR Settles First Case in HIPAA Right of Access Initiative
October 2, 2019	Elite Dental Associates	$10,000	Dental Practice Pays $10,000 to Settle Social Media Disclosures of Patients' Protected Health Information
October 23, 2019	Jackson Health System	$2,150,000	OCR Imposes a $2.15 Million Civil Money Penalty against Jackson Health System for HIPAA Violations
November 5, 2019	University of Rochester Medical Center	$3,000,000	Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement
November 7, 2019	Texas Health and Human Services Commission	$1,600,000	OCR Imposes a $1.6 Million Civil Money Penalty against Texas Health and Human Services Commission for HIPAA Violations
November 27, 2019	Sentara Hospitals	$2,175,000	OCR Secures $2.175 Million HIPAA Settlement after Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information
December12, 2019	Korunda Medical	$85,000	OCR Settles Second Case in HIPAA Right of Access Initiative
December30, 2019	West Georgia Ambulance	$65,000	Ambulance Company Pays $65,000 to Settle Allegations of Longstanding HIPAA Noncompliance
	2019 TOTAL:	$15,270,000	

38

2018 BREACH PENALTIES

Date	Organization	Fine Total	Link to OCR Settlement
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	The University of Texas MD Anderson Cancer Center	$4,348,000	Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations
September 20, 2018	Boston Medical Center (BMC), Brigham and Women's Hospital (BWH), and Massachusetts General Hospital (MGH)	$999,000	Unauthorized Disclosure of Patients' Protected Health Information During ABC Television Filming Results in Multiple HIPAA Settlements Totaling $999,000
October 16, 2018	Anthem	$16,000,000	Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History
November 26, 2018	Allergy Associates of Hartford, P.C.	$125,000	Allergy practice pays $125,000 to settle doctor's disclosure of patient information to a reporter
December 4, 2018	Advanced Care Hospitalists PL (ACH)	$500,000	Florida contractor physicians' group shares protected health information with unknown vendor without a business associate agreement
December 11, 2018	Pagosa Springs Medical Center (PSMC)	$111,400	Colorado hospital failed to terminate former employee's access to electronic protected health information
December 12, 2018	Cottage Health	$3,000,000	Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million
	2018 TOTAL:	$28,683,400	

39

2017 BREACH PENALTIES

Date	Organization	Fine Total	Link to OCR Settlement
January 9, 2017	Presence Health	$475,000	First HIPAA enforcement action for lack of timely breach notification settles for $475,000
January 18, 2017	MAPFRE	$2,200,000	HIPAA settlement demonstrates importance of implementing safeguards for ePHI
February 1, 2017	Children's Medical Center of Dallas	$3,200,000	Lack of timely action risks security and costs money
February 16, 2017	Memorial Healthcare Systems	$5,500,000	$5.5 million HIPAA settlement shines light on the importance of audit controls
April 12, 2017	Metro Community Provider Network (MCPN)	$400,000	Overlooking risks leads to breach, $400,000 settlement
April 20, 2017	The Center for Children's Digestive Health (CCDH)	$31,000	No Business Associate Agreement? $31K Mistake
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
June 7, 2017	Rite Aid	$1,000,000	Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case
December 18, 2017	21st Century Oncology	$2,300,000	$2.3 Million Levied for Multiple HIPAA Violations at NY-Based Provider
	2017 TOTAL:	$20,393,200	

40

2016 BREACH PENALTIES

Date	Organization	Fine Total	Link to OCR Settlement
February 3, 2016	Lincare, Inc.	$239,800	First Judicial Case Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $1.2 mil
February 16, 2016	Physical Therapy	$25,000	Physical therapy provider settles violations that it impermissibly disclosed patient information
March 16, 2016	North Memorial	$1,550,000	$1.55 million settlement underscores the importance of executing HIPAA business associate agreements
March 17, 2016	Feinstein Research	$3,900,000	Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement
April 20, 2016	Raleigh Orthopaedic	$750,000	$750,000 settlement highlights the need for HIPAA business associate agreements
April 21, 2016	New York Presbyterian	$2,200,000	Unauthorized Filming for "NY Med" Results in $2.2 Million Settlement with New York Presbyterian Hospital
June 29, 2016	Catholic Health Services of Philadelphia	$650,000	Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement
July 18, 2016	Oregon Health & Science University	$2,700,000	Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Science University
July 21, 2016	University of Mississippi Medical Center	$2,750,000	Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)
August 4, 2016	Advocate Health	$5,550,000	Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million
September 23, 2016	Care New England Health System	$400,000	HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements
October 17, 2016	St. Joseph's	$2,140,000	$2.14 million HIPAA settlement underscores importance of managing security risk
November 22, 2016	UMass	$650,000	UMass settles potential HIPAA violations following malware infection
	2016 TOTAL:	$23,564,800	

41

ARE THESE BREACHES?

- An employee accesses the medical record of her ex-husband to obtain a new address for personal reasons.
- A policeman on the scene of an auto accident picking up PHI on the road-way that was in a secure carrying case by a healthcare worker.
- An emergency medical technician provides PHI to an inquisitive police officer.
- A relative is provided PHI about a patient in a clinic.
- Your healthcare worker takes a photo of herself and your patient who happens to have cancer and places a heartfelt message on your company website.
- Your company does not have a PHI security policy in place and allows employees to insert thumb-drives into the company computer to download or upload documents.

42

COMMON BREACH SCENARIOS

- Releasing of a medical record without consent
- Loosing PHI on laptop or other electronic device
- Discussing a patient by name on Facebook or twitter
- Posting photos on the internet without consent
- Release of more information than was consented
- Releasing information to employers without consent
- Releasing or selling medical information to the press or other companies/vendors
- Accidentally leaking information, such as to a partner or child
- Releasing medical information at an accident

43

NOTICE MUST BE GIVEN TO AFFECTED INDIVIDUAL

- **Without unreasonable delay, but never more than 60 days after learning of the breach.**
- **In writing by mail or, if the individual has agreed, by email.**

44

SUBSTITUTE NOTICE

- **What if provider has incomplete or out-of-date contact information for affected individuals?**
  - **For 10 or more individuals, provider can post notice on its website or publish in major print or broadcast media where the affected individuals likely reside.**
  - **For fewer than 10 individuals, provider can give notice by alternative form of written, telephone, or other means.**

45

CONTENTS OF THE NOTICE

- Description of the breach (what happened)
- Type(s) of information disclosed
- Steps effected individuals should take to protect themselves from potential harm
- What the provider is doing to investigate the breach, mitigate the harm, and prevent further breaches
- Contact information for the provider (including a toll-free number if substitute notice is provided on a website or by media)

46

NOTICE TO HHS

Submit	Submit electronically through HHS website
Notify	If breach affects 500 or more individuals, notify HHS secretary without unreasonable delay and no later than 60 days after breach
Notify	Otherwise, notify HHS no later than 60 days after the end of the calendar year in which the breach occurred
Expect	Expect an investigation

47

NOTICE TO MEDIA

For breach affecting more than 500 residents of a state, provider must give notice to prominent media outlets serving that state

Notice must be provided without unreasonable delay and no later than 60 days following discovery of the breach

Must include the same information required for the notice to individuals

48

NOTICE BY BUSINESS ASSOCIATE

- Business associates must notify provider if breach occurs
- Notice must be given without unreasonable delay and no more than 60 days after discovery
- Notice must include identification of each individual affected and any information provider needs to include in its notice to individuals

49

STATE LAWS

- 46 states have enacted data security laws: http://www.ncsl.org/default.aspx?tabid=13489
- Requirements vary by state, but many include PHI, employee data, and consumer data
- Notice required to affected state residents, state attorney general, and consumer agencies
- Challenge: Multi-state breach

50

BREACH NOTIFICATION LOG

- Date of Breach
- Date of Discovery of the Breach
- Approximate # of Individuals affected
- Type of Breach - (theft, unauthorized access, loss, improper disposal, hacking, IT incident or other)
- Location of breach information (paper, server, laptop, PC, other)
- Type of Unsecured PHI that was involved (identifiers ie; name, SSN, DOB, diagnosis codes, account numbers, disability info, etc.)

51

POLICIES & PROCEDURE SUGGESTIONS

- Medical Record Designated for Disclosure
- Minimum Necessary Uses and Disclosures for PHI
- Policy as to Which Positions Has Access to PHI and Roles
- Policy on Which Outside Entity Has Right to PHI and Level of Disclosures
- Policy on Patient Notices Regarding Privacy Practices
- Emailing and Faxing of PHI
- Business Associate Agreements / Business Associate Decision Tree
- Destruction of PHI
- Facility Access Controls to Outside Persons
- Security of Electronic Devices
- Consumer Rights Policy on Copying, Costs and Sharing with Consumer

52

53

EMPLOYER WRAP TO REDUCE VIOLATIONS

- HIPAA Compliance Manual
- Dedicated HIPAA Privacy/ Security Officer
- Yearly Training and at Time of New Hire
- Train Your Managers & Manager Risk Mitigation
- Yearly Risk Assessments
- Policy and Procedure Monitoring, Evaluation and Update
- Employee Counseling and Re-training
- Complaint and Breach Management
- Business Associate Agreements

54


Thank You – Any Questions?
Roger Manning
Managing Partner
Excellentia Advisory Group
(636) 875-5088 ext. 109
roger@excellentiagroup.com
EXCELLENTIA

55