


**PRIVACY AND THE
PHYSICIAN/PATIENT
RELATIONSHIP**

San Juan Regional Compliance Conference
The Health Care Compliance Association
May 17, 2018




LCDA. MIGLISA L. CAPÓ SURIA, LL.M.
VP LEGAL AFFAIRS

1

**HEALTH INSURANCE PORTABILITY AND
ACCOUNTABILITY ACT-RECAP**

- APPROVED IN 1996. 42 USC 1320d et seq.
- Amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, as part of the American Recovery and Reinvestment Act of 2009. The amendment:



- Expands the privacy and security rules and increases penalties.
- Establishes new requirements for accountability and restrictions on fundraising and marketing.
- Extends its applicability directly on business associates and subcontractors.
- Bans the sale of PHI-requires authorization in case of fundraisers/marketing.
- Requires notification to OCR in breaches of +500 individuals.

2

PHI IDENTIFIERS 45 CFR § 164.514

<ul style="list-style-type: none"> • Name • Address • Birthdate • Age (w/conditions +89) • Telephone • E-mail address • Social security number • Medical record number • Health plan beneficiary number 	<ul style="list-style-type: none"> • Account number • License number • Vehicle identifier (serial number/license plate) • Device identifier • Full face image • Biometric Identifier (fingerprint/voice) • URL/IP address
--	--

3

APPLICABLE LEGISLATION-PUERTO RICO

• Carta de Derechos y Responsabilidades del Paciente 24 LPRA § 3049

Todo paciente, usuario o consumidor de servicios de salud médico-hospitalarios en Puerto Rico tiene Derecho a:

(a) Comunicarse libremente, sin temor y en estricta confidencialidad con sus proveedores de servicios de salud médico hospitalarios.

(b) Tener plena confianza en que su información médica y de salud será mantenida en **estricta confidencialidad** por sus proveedores de servicios de salud médico-hospitalarios y no será divulgada sin la autorización escrita del paciente o de su tutor, y en todo caso únicamente para fines médicos o de tratamiento, incluyendo la continuación o modificación del cuidado médico o tratamiento o con fines de prevención, control de calidad o relacionados con el pago de servicios de salud médico-hospitalarios.

(c) Tener la confianza de que la divulgación no autorizada de información contenida en récords médicos o de salud se hará **únicamente por orden judicial previa o mediante autorización específica de ley**, incluyendo, pero sin limitarse a, para fines de investigaciones relacionadas con la perpetración de fraudes o la comisión de delitos.

(d) Todo proveedor y toda entidad aseguradora deberán mantener la confidencialidad de aquellos expedientes, récord clínico o documentos que contengan información sobre el estado médico de un paciente. Todo proveedor y toda entidad aseguradora deberán también tomar medidas para proteger la intimidad de sus pacientes, salvaguardando su identidad.

• Puerto Rico Medical Licensing and Discipline Board - Code of Professional Ethics, No. 11:

"El profesional de la medicina respetará el derecho del paciente a la confidencialidad del manejo de la información relacionada a su caso. Consecuentemente, el médico guardará con celo esmerado las confianzas de sus pacientes, así como cualquier otra información que sea consecuencia directa o indirecta de su relación profesional. Las únicas excepciones a este deber serán cuando una orden o norma jurídica obligue a revelar el secreto médico o cuando por guardar la confidencialidad la vida del paciente, del médico mismo o de terceras personas estrar en peligro o riesgo".

4

OTHER RELEVANT PROVISIONS

• Oath of Hippocrates:

"Whatever in connection with my professional practice or not in connection with it I see or hear in the life of men which ought not to be spoken abroad I will not divulge as recommending that all such should be kept secret".

• American Medical Association, Fundamentals Elements of the Patient-Physician Relationship (www.ama-assn.org/ama/pub/category/2510.htm):

"The patient has the right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient, unless provided bylaw or by the need to protect the welfare of the individual or the public interest."

5

HIPAA-DISCLOSURES NOT REQUIRING AUTHORIZATION/REQUIRING AUTHORIZATION

In relation to a physician/patient relationship, it is important to know:

- ✓Physician may make disclosures to other health care providers if both have a relationship with patient or if the disclosure is made for treatment purposes. 45 CFR § 164.506.
 - ✓General rule: PHI of a patient with full mental capacity may only be disclosed to a third party (relative) with the authorization of such patient.
 - ✓Psychotherapy notes may not be disclosed. A summary may be produced. A fee may apply. 45 CFR 164.524
 - ✓Judicial disclosures require a court order. No attorney subpoenas allowed. Minimum necessary standard applies.
 - ✓HIPAA applies to patients who died.
 - ✓Patient right of access/copies of record; Patient may require amendments.
 - ✓In Puerto Rico, the original of the patient's chart in a medical office belongs to the patient. In hospitals, it belongs to the facility, patient only has a right to photocopy after payment.
- 6

**BREACH-NOTIFICATION
Rule 45 CFR §§ 164.400-414**

- Impermissible use or disclosure of PHI unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
 - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 - The unauthorized person who used the protected health information or to whom the disclosure was made;
 - 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.

7

3 EXCEPTIONS

1. Unintentional, but by employee in good faith and acting within authority.
2. Inadvertently, but acting within authority.
3. The recipient not able to retain information.

NOTIFICATION: 60 DAYS DEADLINE
 >500= individual notice or via e-mail
 +500 = Media notice and OCR

8

PENALTIES

Civil penalties 45CFR 160.404:

- No knowledge: \$100 -\$50,000 for each violation; cap of \$1,500,000 for identical violations during a calendar year.
- Reasonable cause: \$1,000 -\$50,000 for each violation; cap of \$1,500,000 for identical violations during a calendar year.
- Willful neglect corrected within 30 days: \$10,000 -\$50,000 for each violation; cap of \$1,500,000 for identical violations during a calendar year.
- Willful neglect: \$50,000 for each violation; cap of \$1,500,000 for identical violations during a calendar year.

Criminal penalties:

- Unknowingly or with reasonable cause: Up to one year (\$50K fine).
- Under false pretenses: Up to five years (\$100K fine).
- For personal gain or malicious reasons: Up to ten years (\$250K fine).

9

MOST COMMON PHYSICIAN PRIVACY BREACHES

Most facility breaches (i.e. hospitals) now involve sophisticated cyber attacks (ransomware) and authorized usage.

However, at the physician level (medical office), the most common breaches still involve *the more simple type of breaches* such as:

- ✓ Error in delivery of results (manual delivery).
- ✓ Failure to encrypt PHI sent via e-mail.
- ✓ Error in sending PHI via fax.
- ✓ Physician indiscretion #1 (PHI discussions too loud-overheard by others).
- ✓ Physician indiscretion #2 (posting PHI on social media).
- ✓ Failure to properly destroy PHI (records).
- ✓ Failure to erase PHI stored in equipment (office imaging equipment, photocopiers, computers) when replacing such.
- ✓ Stolen USBs and laptops.

10

**PHYSICIAN PRIVACY BREACHES-SAFEGUARDS
WHAT YOU AS COMPLIANCE OFFICER NEED TO DO...**

- Train employees-Alert them that gossiping on PHI to co-workers and outsiders exposes all to fines.
- Double check document delivery (manual and faxes).
- Delete all data from leased photocopiers before returning.
- Delete all data from computers and imaging equipment before sale or disposal.
- Engage a records destruction company.
- Train employees about charts left visible to others.
- Prohibit text messages with PHI unless both the sender and the recipient have installed encryption programs.
- Train employees about celebrity privacy and exposure.
- Prohibit any PHI discussions on social media.

11

PHYSICIAN PRIVACY BREACHES-SAFEGUARDS

- Implement a robust encryption system for e-mails and for laptops and other devices (i.e. mobile phones).
- Encrypt data on USBs.
- Implement a policy on the management of PHI outside the office.
- Don't leave laptops or USB data storage devices (pen drives) in a parked vehicle.
- Implement the same safeguards at home (i.e. home computers).
- Beware of former employees. Eliminate all access, change passwords.
- Only discuss PHI with patient or authorized representative. Beware of unauthorized requests (i.e. ex-wife, common law wife, neighbor).
- Ban PHI discussions in public areas (i.e. elevators) .
- Careful with use of **unprotected clouds** (information sharing applications).

12

EXAMPLES OF MD OFFICE BREACHES

- Many cases of identity theft or fraudulent use of medical charts.
- In Texas, an employee at a medical office entered a guilty plea after selling PHI to a drug trafficker of an FBI agent who was a patient. She sold the PHI for \$500.00 and went to jail for 10 years and had to pay a \$250K fine. U.S. v Ramirez No. 7:05CR-00708, SD Tex., March 6, 2006.
- An employee of a Florida clinic accessed patient files and stole PHI of 1,100 patients and sold it to her cousin, who used it to bill Medicare \$7 million worth of false claims. U.S. v. Ferrer, S.D. Fla. 06-CR-60261, Jan. 11, 2006.

13

HIPAA LIABILITY DOES NOT STOP UPON MD OFFICE CLOSURE

OCR v. Filefax (an Illinois warehouse). Resolution of Feb 13, 2018

- Filefax was a medical files storage facility that went bankrupt. OCR got a tip that a dumpster was found with 2,150 patient charts. Filefax's receiver claimed they were on the way for destruction. OCR imposed a \$100K fine and a Corrective Action Plan to safely dispose (via contract with Iron Mountain) of all the medical charts.
- Lesson to the medical offices: (i) Don't forget about charts sent to storage facilities; (ii) investigate the financial strength of your business associates.
- In a related case- the Center for Children's Digestive Health (Pediatric clinics in Illinois) paid the HHS \$31,000 for failing to have a BA with Filefax while sending 10,728 files to storage. April 20, 2017, Resolution Agreement.

14

WHAT IF THE MD OFFICE CLOSES? WHAT IF THE MD OFFICE PARTNERS SPLIT?

- If the medical office closes, state law mandates that a public notice be published to return the original to the patient.
- If the practice splits, and each MD goes separate ways, each physician can take the charts of their own patients, provided that the patient authorizes such continuance of care.
- If the MD resigns or is separated from the practice, the latter keeps the charts, but the MD leaving may require photocopies of the charts of his patients to seek continuation of care. Pullman v. Gormley, NY Sup Ct. No. 11999/06, November 3, 2006.

15

PHYSICIAN PRACTICE: OCR ENFORCEMENT ACTIONS

- **Phoenix Cardiac Surgery – two cardiologists.**
 - The MD office posted clinical and surgical appointments for its patients on an **Internet-based calendar that was publicly accessible.**
 - OCR determined that Phoenix Cardiac Surgery had implemented few policies and procedures to comply with the HIPAA, had limited safeguards to protect PHI and was lax about HIPAA training.
- Violations:
- No training.
 - Posted over 1,000 separate entries of PHI on a publicly accessible, Internet-based calendar over a two year period.
 - Transmitted ePHI daily from an Internet-based email account to the employee's personal Internet-based email accounts.
 - Failed to appoint a security official.
 - Failed to conduct a risk assessment.
 - No BA agreements from the Internet-based calendar vendor and from the Internet-based public email provider.
 - OCR imposed a \$100,000 penalty and required PCS to adopt a Corrective Action Plan. Resolution Agreement April 17, 2012.

16

OCR-BEWARE WITH PATIENT TESTIMONIALS

A physical therapy practice known as *Complete P.T.* posted patient testimonials, including full names and full face photographic images, on its website without obtaining valid, HIPAA-compliant authorizations.

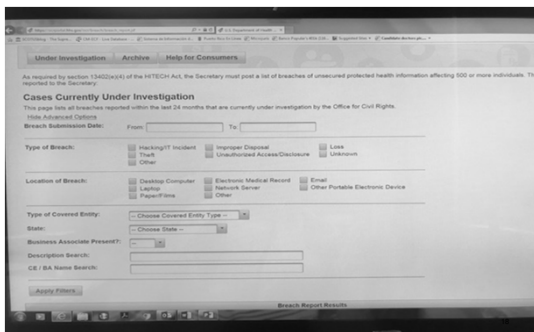
OCR's investigation revealed that Complete P.T.:

- Failed to reasonably safeguard PHI.
- Impermissibly disclosed PHI without an authorization; and
- Failed to implement policies and procedures.
- Was required to pay \$25,000, and to adopt and implement a corrective action plan. February 2, 2016 Resolution Agreement.

17

WALL OF SHAME

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



FREQUENTLY ASKED....

• **Are prior authorizations required when a doctor or health plan distributes promotional gifts of nominal value?**

• **Answer:**

• No. In a specific exception, the HIPAA Privacy Rule allows covered entities to distribute items commonly known as promotional gifts of nominal value without prior authorization, even if such items are distributed with the intent of encouraging the receiver to buy the products or services.

This authorization exception generally applies to items and services that are not health-related. A covered doctor, for instance, may send patients items such as pens, note-pads, and cups with a logo without prior authorization. Similarly, dentists may give patients free toothbrushes, floss and toothpaste.

19

FREQUENTLY ASKED....

• **May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?**

• **Answer:**

• Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

20

• A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed. See 45 CFR 164.510(b)(3).

21

OCR GUIDELINE- MD OFFICE CONTRACTS

• **Private Practice Ceases Conditioning of Compliance with the Privacy Rule**

Covered Entity: Private Practice
Issue: MD Conditions Compliance with the Privacy Rule

• A physician practice requested that patients sign an agreement entitled "Consent and Mutual Agreement to Maintain Privacy." The agreement prohibited the patient from directly or indirectly publishing or airing commentary about the physician, his expertise, and/or treatment in exchange for the physician's compliance with the Privacy Rule. A patient's rights under the Privacy Rule are not contingent on the patient's agreement with a covered entity. A covered entity's obligation to comply with all requirements of the Privacy Rule cannot be conditioned on the patient's silence. OCR required the covered entity to cease using the patient agreement that conditioned the entity's compliance with the Privacy Rule. Additionally, OCR required the covered entity to revise its Notice of Privacy Practices.

22

OCR GUIDELINE-MD OFFICE WAITING ROOMS

• **Private Practice Implements Safeguards for Waiting Rooms**

Covered Entity: Private Practice
Issue: Safeguards; Impermissible Uses and Disclosures

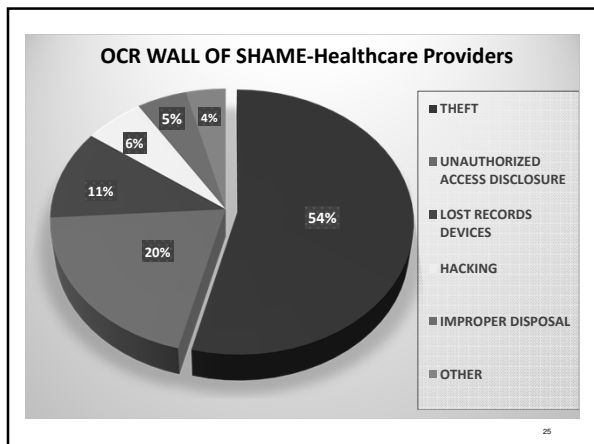
• A staff member of a medical practice discussed HIV testing procedures with a patient in the waiting room, thereby disclosing PHI to several other individuals. Also, computer screens displaying patient information were easily visible to patients. Among other corrective actions to resolve the specific issues in the case, OCR required the provider to develop and implement policies and procedures regarding appropriate administrative and physical safeguards related to the communication of PHI. The practice trained all staff on the newly developed policies and procedures. In addition, OCR required the practice to reposition its computer monitors to prevent patients from viewing information on the screens, and the practice installed computer monitor privacy screens to prevent impermissible disclosures.

23

DISCLOSURES-BREACHES

- HIPAA requires reporting to OCR breaches involving 500+ individuals.
- In 2018 alone, more than 84 cases have been reported so far.
- Mainly cyber attacks requiring Ransom \$\$\$\$.

24



TOP 2017 HIPAA BREACHES-U.S.

Entity	# patients	Type of Breach	Description
Commonwealth Health Corp.	697,000	Employee took PHI on device for a personal project.	Kentucky-hospitals
Airway Oxygen	500,000	Ransomware attack	Home medical supplier in Michigan
Womens Health Care Group	300,000	Ransomware attack	OB practice in PA
Urology Austin	279,663	Ransomware attack	
Peachtree Neurological Clinic	176,295	Ransomware attack	Atlanta clinic
Harrisburg Gastroenterology	93,323	Unauthorized access	Gastro office
Vision Quest Eyecare	85,995	Cyber attack	Indianapolis
Wash. Univ School of Medicine	80270	Phising attack	E-mail account
Emory Healthcare	79,930	Ransomware	Hackers deleted patient data; atypical as attacks involve locking system not deletion
Primary Care Specialists	65,000	Cyber attack	Memphis Md office. System locked.

TOP HIPAA FINES 2017

Entity	Amount	Description	Facility
Memorial Healthcare Systems	\$5.5M	Unauthorized access to PHI by employees	Operates 6 hospitals in Florida
Children's Medical Center	\$3.2M	Losing (i) unencrypted phone with PHI on 3,800 patients (ii) unencrypted laptop w/PHI of 2,462 patients.	Dallas
CardioNet	\$2.5M	Theft of laptop from employee's car	Mobile cardiac telemetry
Memorial Hermann Health System	\$2.4M	Issuing a press release with a patient's name.	Texas medical center
21 st Century Oncology	\$2.3M	Sale of PHI of 2 million people (SS# and diagnosis)	Florida provider of cancer care services
MAPFRE	\$2.2M	Theft of an USB drive with names and SS# of 2,209 individuals.	Puerto Rico

HIPAA Breaches- Puerto Rico				
COVERED ENTITY	# PATIENTS	DATE	TYPE	LOCATION
Triple-S Management Corp., Triple-S Salud (en 2014 pagó multa de \$3.5M)	475,000	11/4/10	Hacking/IT Incident, Unauthorized Access/Disclosure	Network Server
Triple-C, 3rd party admin for Triple-S	398,000	1/24/14	Theft	Network Server
Medical Card System/MCS-HMO/MCS Advantage/MCS Life	115,000	11/9/10	Unauthorized Access/Disclosure	Other, Other Portable Electronic Device
Triple-S Salud Inc.	56,853	5/29/14	Unauthorized Access/Disclosure	Paper/Films
MMM Healthcare	32,390	5/9/11	Theft	Desktop Computer
PMC Medicare Choice	24,361	5/9/11	Theft	Desktop Computer
American Health Inc.	17,776	4/3/14	Theft	Other
Triple-S Salud Inc.	13,336	11/8/13	Unauthorized Access/Disclosure	Paper/Films
American Health Inc.	11,531	5/18/14	Unauthorized Access/Disclosure	Paper/Films
T & P Consulting dba Quantum Health Consulting	10,000	3/12/12	Theft	Laptop, Other Portable Electronic Device
Triple-C, 3rd party admin for Triple-S	8,000	1/24/14	Theft, Unauthorized Access/Disclosure	Network Server

28

COVERED ENTITY	# PATIENTS	DATE	TYPE	LOCATION
Quantum Health Consulting	7,923	3/13/12	Theft	Laptop
Triple-S Salud Inc.	7,911	4/15/14	Theft	Other Portable Electronic Device
T & P Consulting dba Quantum Health Consulting	7,706	2/28/12	Theft	Laptop
T&P Consulting DBA Quantum HC	7,606	3/15/12	Theft	Laptop, Other Portable Electronic Device
VA Caribbean Healthcare System	6,006	5/26/11	Theft	Paper/Films
Accuprint	5,848	8/15/11	Theft	Other
Triple-S Salud Inc.	5,795	4/2/14	Theft	Other
PHMHS	5,000	9/11/13	Theft	Network Server
Quantum Health Consulting	4,645	3/12/12	Theft	Laptop
Dr. Axel Vélez	2,800	7/13/11	Theft	Desktop Computer

29

COVERED ENTITY	# PATIENTS	DATE	TYPE	LOCATION
Departamento de Salud de Puerto Rico	2,621	2/2/11	Unknown	Desktop Computer
MAPFRE Life	2,209	9/29/11	Theft	Other
Centro de Ortodoncia Inc.	2,000	9/13/11	Theft	Paper/Films
MSO of Puerto Rico	1,907	2/17/10	Theft	Paper/Films
Hospital Auxilio Mutuo	1,000	12/13/10	Hacking/IT Incident, Theft, Unauthorized Access/Disclosure	Desktop Computer, Laptop
Alberto Gerardo Vázquez Rivera	679	6/28/13	Theft	Laptop
MSO of Puerto Rico	605	2/17/10	Theft	Paper/Films

30

HIPAA & USE OF CAR AS MOBILE OFFICE

Lincare case could be used as guideline for physicians who visit patients at home.

The employee of a HHA removed charts from the facility and left them in the car and at home.

There was a breach involving 278 charts. Lincare got a fine of \$239,800.

The investigation revealed that the entity lacked policies to maintain its PHI secure.

The provider must have safeguard policies and track all PHI that is removed from the facility- either electronic or paper.



31

LINCARE CASE

Director of OCR v Lincare Decision #4505, Jan 13, 2016:

- Employee had the PHI of 270 patients and 8 full medical charts in her car and home.
- She fights with her husband, they split and she leaves home – leaving her PHI at home.
- Husband calls the OCR...@.
- OCR decides that providers that remove PHI for the facility need to develop policies to guarantee the safety of such PHI and must register every time they remove and return such files with PHI.
- Violations: disclosure to husband, failing to protect PHI and failure to establish policies and procedures.

32

OTHER CONSIDERATIONS:

- A physician who is co-defendant in a malpractice suit does not have a right to Access a medical chart without a court order or patient authorization, unless the reason to seek such chart is for continuation of care. 42 CFR § 164.506@ (2).
- A MD must be careful to produce medical charts of patients to third parties who are not legal representatives. Also, always require ID and proof of such legal representation. For instance, birth certificate to demonstrate son/daughter. No PHI to common law partners or neighbors.

33

QUESTIONS



34

MIGLISA L. CAPÓ SURIA, LLM
VP LEGAL AFFAIRS
mcapo@metropaviahealth.com
Tel. (787) 625-8763



35
