



# Boost Your HIPAA Compliance: 5 Tips for Providing Patient Access while Protecting Privacy

*Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB*

*Vice President, Privacy, Compliance and HIM Policy, MRO*

*September 18, 2017*



# Agenda

1. OCR Enforcement Actions
2. The Patient Right of Access under HIPAA
3. 2016 FAQs on Patient Access
4. 5 Tips for Providing Patient Access while Protecting Privacy
5. What is on the Horizon
6. Questions

# About MRO

**2nd**

**Largest Disclosure  
Management  
Provider**

**Over  
6,000**

**Locations**

**20%**

**Growth**

**#1  
KLAS**

**Since 2013**

**98%**

**Client  
Retention**



# OCR Enforcement Actions

## OCR Enforcement Actions

- As of September 30, 2016, OCR has received over **141,754** complaints
  - **86,515** were deemed ineligible for OCR investigation
  - **24,501** led to OCR investigations, which resulted in required changes in privacy practices, corrective actions, or technical assistance
  - **15,746** resulted in OCR intervention and the provision of technical assistance, without the need for an investigation
  - **11,099** investigations found no violations
  - **~1,105** led to OCR compliance reviews

# Breaches under HIPAA – 45 CFR §§ 164.400-414

	Previously (Pre-Final Omnibus Rule)	Currently (Post-Final Omnibus Rule)
How to determine whether an impermissible use or disclosure of PHI constitutes a Breach ...	The impermissible use or disclosure of PHI is a Breach if such use or disclosure poses a significant risk of financial, reputational, or other harm to the individual	The impermissible use or disclosure of PHI is presumed to be a Breach unless the CE or BA demonstrates there is a low probability that the PHI has been compromised, based on a risk assessment

- The Final Omnibus Rule on Breach Notification for Unsecured PHI under the HITECH Act replaced the HITECH Act's Breach Notification Rule's "harm" threshold
- Harm is still used to help the enforcement agency determine the penalties for violations
- In addition to the number of individuals affected and the duration of the breach, physical harm, financial harm, and reputational harm are all considered when the penalties are assessed for data breaches

# Breaches under HIPAA – 45 CFR §§ 164.400-414

- 3 Exceptions to the Definition of Breach
  - The unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA, if such acquisition, access, or use was made in good faith and within the scope of authority
  - The inadvertent disclosure of PHI by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the CE or BA
  - In both cases, the information cannot be further used or disclosed in a manner not permitted by the HIPAA Privacy Rule
  - If CE or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information

# Breaches under HIPAA – 45 CFR §§ 164.400-414

- If an impermissible use or disclosure of unsecured PHI is determined to be a Breach, CEs and BAs must provide notification of the Breach to affected individuals, the Secretary, state entities (under applicable state law) and, in certain circumstances, to the media

Breach Notification Timeline Requirements			
Breach Type	To the Individual	To the Secretary	To the Media
If Breach affects < 500 individuals	Without unreasonable delay, and in no case later than 60 days following the discovery of the Breach	Must be provided no later than 60 days after the end of the calendar year in which the Breach was discovered	N/A
If Breach affects > 500 individuals	Without unreasonable delay, and in no case later than 60 days following the discovery of the Breach	Without unreasonable delay, and in no case later than 60 days following the discovery of the Breach	Without unreasonable delay, and in no case later than 60 days following the discovery of the Breach

# Breaches under HIPAA – 45 CFR §§ 164.400-414

- CEs and BAs must only provide the required notifications if the breach involved “Unsecured PHI”
  - “Unsecured PHI” is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by HHS’ Guidance on Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- The Guidance specifies encryption and destruction as the technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals



# Breaches under HIPAA – 45 CFR §§ 164.400-414

U.S. Department of Health and Human Services  
Office for Civil Rights

Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Welcome | File a Breach | HHS | Office for Civil Rights | Contact Us

Please Note: The Breach Notification Portal will be offline for maintenance from Sat Jul 01 05:00 AM EDT to Sat Jul 01 02:00 PM EDT. Any information being entered when the Portal is taken off-line will be lost.

## Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary.

State ↕	Covered Entity Type ↕	Individuals Affected ↕	Breach Submission Date ↕	Type of Breach	Location of Breached Information
NY	Health Plan	808	01/03/2017	Unauthorized Access/Disclosure	Other
WA	Health Plan	1375	01/03/2017	Hacking/IT Incident	Network Server
KY	Healthcare Provider	822	01/05/2017	Theft	Other
MD	Healthcare Provider	600	01/06/2017	Loss	Other Portable Electronic Device
CA	Healthcare Provider	500	01/09/2017	Theft	Paper/Films
WI	Healthcare Provider	4800	01/10/2017	Unauthorized Access/Disclosure	Email
CA	Healthcare Provider	10164	01/11/2017	Hacking/IT Incident	Network Server
AL	Healthcare Provider	1090	01/12/2017	Unauthorized Access/Disclosure	Electronic Medical Record
CA	Healthcare Provider	3594	01/13/2017	Theft	Laptop
MD	Healthcare Provider	1320	01/13/2017	Hacking/IT Incident	Email
ND	Healthcare Provider	600	01/16/2017	Hacking/IT Incident	Network Server
VA	Healthcare Provider	5454	01/16/2017	Hacking/IT Incident	Network Server

Since January 2017, there have been 148 breaches involving CEs and BAs affecting 500 or more patients

Source:  
[https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf;jsessionid=D94DC7725DDFD8B74F9960A3996C7F01](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=D94DC7725DDFD8B74F9960A3996C7F01)

# Breaches under HIPAA – 45 CFR §§ 164.400-414

## Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Breach Report Results					
State ↕	Covered Entity Type ↕	Individuals Affected ↕	Breach Submission Date ↕	Type of Breach	Location of Breached Information
CT	Healthcare Provider	1278	05/26/2017	Hacking/IT Incident	Email
CT	Healthcare Provider	6000	06/07/2017	Theft	Desktop Computer, Laptop
CT	Health Plan	5002	06/20/2017	Unauthorized Access/Disclosure	Other

Since January 2017, there have been 3 breaches involving a CT CE or BA affecting 500 or more patients

# OCR Enforcement Actions

## Resolution of OCR Investigations

If the evidence indicates that the CE was not in compliance, OCR will attempt to resolve the case by obtaining one or more of the following:

- Voluntary Compliance

- Corrective Action

- Resolution Agreement

- Agreement signed by HHS and a CE or BA
- Under which the CE or BA agrees to perform certain obligations and make reports to HHS, generally for a period of 3 years
- During the period, HHS monitors the CE or BA's compliance with its obligations.
- May include the payment of a resolution amount

- Civil Money Penalties (CMPs)

- Imposed if the CE does not take action to resolve the matter in a way that is satisfactory
- If CMPs are imposed, the CE may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case

# OCR Enforcement Actions

## Civil Money Penalties

- Imposed if the CE does not take action to resolve the matter in a way that is satisfactory
- CMPs for HIPAA violations are determined based on a tiered civil penalty structure

HIPAA Violation	Minimum Penalty	Maximum Penalty
Unknowing	\$100 per violation, with an annual maximum of \$25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	\$50,000 per violation, with an annual maximum of \$1.5 million
Reasonable Cause	\$1,000 per violation, with an annual maximum of \$100,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
Willful neglect but violation is corrected within the required time period	\$10,000 per violation, with an annual maximum of \$250,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
Willful neglect and is not corrected within required time period	\$50,000 per violation, with an annual maximum of \$1.5 million	\$50,000 per violation, with an annual maximum of \$1.5 million

# OCR Enforcement Actions

## Resolution Agreements and Civil Money Penalties

- 50 resulted in the application of corrective measures, which included payment of a resolution amount in lieu of civil money penalties
  - Over \$60 million
- 3 resulted in the assessment of CMPs
  - Over \$7 million

# OCR Enforcement Actions

## 2016-2017 Resolution Agreements and Civil Money Penalties

- 2017
  - 8 Resolution Agreements
    - Over \$11 million collected
  - 1 Civil Money Penalty
    - Over \$3 million collected
- 2016
  - 12 Resolution Agreements
    - Over \$20 million collected
  - 1 Civil Money Penalty
    - \$239,800 collected

# OCR Enforcement Actions

## Top HIPAA Privacy and Security Rule Compliance Issues Identified by OCR (2015)

- Lack of administrative, physical and technical safeguards of PHI
  - Failure to conduct regular risk analyses and assessments
    - Organizations are failing to identify all of the electronic PHI (ePHI) created, maintained, received or transmitted by the organization
  - Lack of data back up plans
- Impermissible uses and disclosures of PHI
  - Breaches resulting from risks previously identified by organizations but never mitigated
  - Lack of access auditing
- Use or disclosure of more than the “minimum necessary” PHI
- Lack of Patient Access
  - Facility policies constituting barriers to access (e.g., required auth. forms)
- Failure to enter into Business Associate Agreements (BAAs)

Source:

<http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html>  
Source: ACC Webcast: ACC Health Law Committee Keep Cool Summer A/C Series (Advocacy/Career Development): Tips for Working with the HHS Agencies – June 15, 2016

# Recent Resolution Agreements and Civil Money Penalties

## Children's Medical Center of Dallas

(2/1/17)

- Breaches involving (1) the loss of an unencrypted, non-password protected BlackBerry device at the DFW Airport containing the ePHI of approximately 3,800 individuals and (2) the theft of an unencrypted laptop containing the ePHI of 2,462 individuals.
- OCR's investigation revealed Children's noncompliance with HIPAA Rules, specifically, a failure to implement risk management plans, contrary to prior external recommendations to do so, and a failure to deploy encryption or an equivalent alternative measure on all of its laptops, work stations, mobile devices and removable storage media until 2013.

Civil Money Penalty:

**\$3,200,000**



# Recent Resolution Agreements and Civil Money Penalties

## Memorial Healthcare System

(2/17/17)

- PHI of 115,143 individuals had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff.
- Although it had workforce access policies and procedures in place, MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules.
- Further, MHS failed to regularly review records of information system activity on applications that maintain electronic PHI by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.

Resolution Agreement Payment:  
**\$5,500,000**

# Recent Resolution Agreements and Civil Money Penalties

## CardioNet (4/24/17)

- CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.
- Stolen laptop resulted in a breach of the ePHI of 1,391 individuals.
- OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft.
- Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented.

Resolution Payment:  
**\$2,500,000**

# Recent Resolution Agreements and Civil Money Penalties

## Memorial Hermann Health System Texas

(5/10/17)

- Patient presented a fake driver's license when she checked in for an appointment, suspecting forgery, the staff notified the police and the patient was later arrested
- The patient's arrest led to an uproar in the community because of her immigration status
- To assure activists that it is not the system's policy to ask for a patient's immigration status and to demonstrate that staff had not intended to get the patient into trouble with immigration officials, Memorial issued a press release with the patient's name without her authorization
- While reporting the suspected crime to the police did not violate HIPAA, that press release did

Resolution Payment:

**\$2,400,000**

# Recent Resolution Agreements and Civil Money Penalties

## St. Luke's-Roosevelt Hospital Center Inc

(5/23/17)

- OCR received a complaint alleging that a staff member impermissibly disclosed the complainant's PHI to the complainant's employer.
- This impermissible disclosure included sensitive information concerning HIV status, medical care, STDs, medications, sexual orientation, mental health diagnosis, and physical abuse.
- OCR's subsequent investigation revealed that staff impermissibly faxed the patient's PHI to his employer rather than sending it to the requested personal post office box
- Additionally, OCR discovered that the provider was responsible for a related breach of sensitive information that occurred 9 months prior to the aforementioned incident but had not addressed the vulnerabilities in their compliance program to prevent impermissible disclosures

Resolution Payment:

**\$387,200**

# Introduction to Patient Access under HIPAA

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the privacy and security of individuals' identifiable health information and establishes an array of patient rights
- With limited exceptions, the HIPAA Privacy Rule provides individuals (Patients) and their Personal Representatives with a legal, enforceable right to see and receive copies of the Patient's protected health information (PHI) upon request from their health care providers and health plans (Covered Entities)

# Introduction to Patient Access under HIPAA

- The HIPAA Privacy Rule generally requires Covered Entities to provide Patients and their Personal Representatives, upon request, with access to the Patient's PHI in one or more "designated record sets" maintained by or for the Covered Entity
- This includes the right to:
  - Inspect or obtain a copy of the Patient's PHI –and–
  - Direct the Covered Entity to transmit a copy to a designated person or entity of the Patient's choice
- Patients and their Personal Representatives are entitled to:
  - Copies of the Patient's PHI,
  - In the format of their choosing (paper or electronic),
  - For a "reasonable, cost-based" fee, and
  - Within 30 days of their request

# The FAQs on Patient Access

- In January, February and May 2016, the OCR published FAQs on patient access to PHI
- The publication of the FAQs was prompted by recent OCR investigations, which found patients faced obstacles in obtaining information
- The purpose of the FAQs is to educate patients about their rights and to guide healthcare providers on providing patients with timely PHI access

# The FAQs on Patient Access

## **NOTE:** The FAQs did not change the HIPAA Regulation

- The FAQs do not have the force of law
- The FAQs document is HHS' interpretation of its own regulation
- If there is a conflict between the FAQs and the regulation, the regulation wins
- If there is ambiguity between the FAQs and the regulation, guidance is given deference
- The FAQs are subject to change or legal challenge



# Outline of the FAQs

## 1. What PHI is the patient entitled to?

- Defining the “Designated Record Set”

## 2. Who is a personal representative?

## 3. Requests for Access

- Format and Verification

## 4. Providing Access

- Format, Timeliness and Fees

## 5. Denial of Access

## 6. Individual’s Right to Direct PHI to Another Person

## 7. State Law

# OCR FAQs: What PHI is the patient entitled to?

Included in Right to Access	Excluded
<ul style="list-style-type: none"><li>• medical records;</li><li>• billing and payment records;</li><li>• insurance information;</li><li>• clinical laboratory test results;</li><li>• medical images, such as X-rays;</li><li>• wellness and disease management program files; and</li><li>• clinical case notes, among other information, used to make decisions about patients</li></ul>	<ul style="list-style-type: none"><li>• PHI that is not part of a designated record set because the information is not used to make decisions about patients</li><li>• Examples:<ul style="list-style-type: none"><li>○ Quality assessment or improvement records</li><li>○ Patient safety activity records</li><li>○ Business planning, development, and management records</li><li>○ Hospital peer review files</li><li>○ Practitioner or provider performance evaluations</li><li>○ Health plan quality control records used to improve customer service</li><li>○ Formulary development records</li><li>○ Psychotherapy notes</li><li>○ Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding</li></ul></li></ul>

# OCR FAQs: Who is a personal representative?

- **Personal representative** (45 CFR 164.502(g))
  - a person with authority under State law to make healthcare decisions for the patient
- **Personal representatives also have the right to:**
  - Access PHI about the patient in a designated record set; AND
  - Direct the CE to transmit a copy of the PHI to a designated person or entity of the patient's choice, upon request, consistent with the scope of such representation
- **Examples:**
  - Healthcare Power of Attorney
  - Parent or Legal Guardian of a Minor Child
  - Executor or Administrator of a Deceased Patient's Estate

# OCR FAQs: Requests for Access – Format and Verification

- Requiring a Written Request
  - CEs may ...
    - Require patients to request access to PHI in writing
      - must inform patients of such a requirement
    - Offer patients the option of using electronic means (e.g., email, secure web portal) to make requests for access
    - Require patients to use the entity's own supplied form
      - form cannot create a barrier to or unreasonably delay the patient from obtaining access to PHI
  - » Examples of Barriers to Access
    - requiring access be requested in person
    - require that requests be mailed
    - require the use of a web portal to request PHI

**NOTE: Patients do not need to submit HIPAA-compliant authorizations to obtain copies of their PHI**

# OCR FAQs: Requests for Access – Format and Verification

- Verifying the Identity of a Patient-Requester
  - CEs are required under the HIPAA Privacy Rule to take reasonable steps to verify a patient-requester's identity
  - There is NO mandated form of verification (e.g., driver's license)
    - How the identities of patient-requesters are verified is up to the CE
      - In person
      - In writing
      - By email
      - By phone
  - *However ....*
    - Verification methods cannot create barriers or delays to access

# OCR FAQs:

## Requests for Access – Format, Timeliness and Access

- Must provide patients with access to PHI in the form and format requested
  - Paper
  - Electronically (CD-ROM, Email, etc.)
- Must provide patients with access to PHI within 30 calendar days of receiving the request
  - If access cannot be provided within 30 days, the deadline may be extended by an additional 30 days by notifying the patient of the delay

*Note: For Summaries or Explanations of PHI, see the FAQs for guidance*

# OCR FAQs:

## Requests for Access – Format, Timeliness and Access

- **Format:** Must provide patients with:
  - A convenient time and place to pick up or inspect copies of PHI (if requested)
  - OR
  - have copies of the PHI mailed or emailed to patient (depending on the capabilities of the Covered Entity and the level of security risk that such transmission may introduce to their IT system)
- Covered Entities are not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access
  - However, mail and email are generally considered readily producible by all Covered Entities

# OCR FAQs:

## Requests for Access – Format, Timeliness and Access

- **Format: Unencrypted Email**
  - When a patient has requested that PHI be sent to a third party by unencrypted email or another unsecured manner, the Covered Entity must oblige the request, warn the patient of the security risks, and have them accept all risks to the PHI associated with the unsecured transmission
  - The Covered Entity is not responsible for breach notification or liable for disclosures that occur in transit



# OCR FAQs:

## Requests for Access – Fees

45 CFR 164.524(c)(4)

- **Fees:**

- The HIPAA Privacy Rule permits CEs to impose a reasonable, cost-based fee if the patient requests a copy of his or her PHI
- The “reasonable, cost-based” fee may only include the cost of:
  - **Labor**
    - for copying the PHI requested by the patient, whether in paper or electronic form
  - **Supplies**
    - for creating the copy of the PHI (e.g., cost of paper, CD-ROM, USB, etc.)
  - **Postage**
    - If applicable
  - **Preparation of an explanation or summary of PHI**
    - if agreed to by the patient

# OCR FAQs: Requests for Access – Fees

Can be included in Labor Costs	<u>Cannot</u> be included in Labor Costs
<ul style="list-style-type: none"><li>• <u>Labor costs associated with:</u><ul style="list-style-type: none"><li>• Creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, <u>once</u> the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied</li><li>• Photocopying paper PHI</li><li>• Scanning paper PHI into an electronic format</li><li>• Converting electronic information in one format to the format requested by or agreed to by the individual</li><li>• Transferring (e.g., uploading, downloading, attaching, burning) electronic PHI from a CE's system to a web-based portal (where the PHI is not already maintained in or accessible through the portal), portable media, email, app, personal health record, or other manner of delivery of the PHI</li></ul></li></ul>	<ul style="list-style-type: none"><li>• <u>Labor costs associated with:</u><ul style="list-style-type: none"><li>• Reviewing the request for access</li><li>• Verification</li><li>• Reviewing the PHI in the medical or other record</li><li>• Documentation</li><li>• Segregating or otherwise preparing the PHI that is responsive to the request for copying</li><li>• Ensuring compliance with HIPAA (and other applicable law) in fulfilling the access request (e.g., verification, ensuring only information about the correct individual is included, etc.)</li><li>• Searching for, retrieving, and otherwise preparing the responsive information for copying, including:<ul style="list-style-type: none"><li>• locating the appropriate designated record sets about the individual</li><li>• Reviewing the records to identify the PHI that is responsive to the request</li><li>• Ensuring the information relates to the correct individual</li><li>• Segregating, collecting, compiling, and otherwise prepare the responsive information for copying</li></ul></li></ul></li></ul>

# OCR FAQs:

## Requests for Access – Fees

Can be included in Supply Costs	<u>Cannot</u> be included in Supply Costs
<ul style="list-style-type: none"><li>• <u>Supply Costs Associated with:</u><ul style="list-style-type: none"><li>• Creating the paper copy or electronic media</li><li>• <i>For Electronic copies of PHI</i><ul style="list-style-type: none"><li>• If requested on physical media, the costs of:<ul style="list-style-type: none"><li>• Physical media such as a compact disc (CD)</li><li>• Universal serial bus (USB) flash drive</li><li>• Postage</li></ul></li></ul></li></ul></li></ul>	<ul style="list-style-type: none"><li>• <u>Supply Costs Associated with:</u><ul style="list-style-type: none"><li>• Hardware (computers, scanners, etc.)</li><li>• Software that is used to generate an electronic copy of an individual's PHI</li><li>• Cost of obtaining such new technologies needed to comply with specific individual requests</li><li>• Costs associated with maintaining systems and recouping capital for data access, storage and infrastructure</li></ul></li></ul>

# OCR FAQs:

## Requests for Access – Fees

- The FAQs provide 3 methods that may be used to calculate the “reasonable, cost-based” fee for patient requests:
  - Fee based on Actual Costs
    - Actual labor and supply costs to fulfill the request, as long as those costs are limited to the labor and supply costs (e.g., paper, CD-ROMs, USBs, etc.), and permitted and postage (if applicable)
    - Example:
      - » Time how long it takes to make and send the copy in the form and format and manner requested or agreed to by the patient and multiply the time by the reasonable hourly rate of the person copying and sending the PHI
  - Fee based on Average Costs
    - Average labor and supply costs to fulfill the request, as long as those costs are limited to the labor and supply costs permitted, and postage (if applicable)
  - Flat Fee for Electronic Copies of PHI Maintained Electronically
    - Flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed \$6.50, inclusive of all labor, supplies, and any applicable postage
    - Not the maximum fee that can be assessed

# OCR FAQs:

## Requests for Access – Fees

- The FAQs go on to say ...
  - CEs must inform patients in advance of the approximate fee that may be charged for copies of their PHI
    - Failure to provide advance notice is an unreasonable measure that may serve as a barrier to the right of access
  - CEs should post on their web sites or otherwise make available to patients an approximate fee schedule for regular types of access requests
  - If asked, CEs should provide the patient with a breakdown of the charges for labor, supplies, and postage, if applicable, that make up the total fee charged
  - PHI cannot be withheld from a patient due to unpaid medical bills
  - Patients cannot be charged for inspecting their PHI

*Note: The HIPAA Regulation does not make mention of these “requirements”*

# OCR FAQs: Denial of Access

Under very limited circumstances, CEs can deny patient requests for access to PHI

<b>Unreviewable grounds for denial (45 CFR 164.524(a)(2)):</b>	<b>Reviewable grounds for denial (45 CFR 164.524(a)(3)).</b>
<p>Requests for:</p> <ul style="list-style-type: none"><li>• Psychotherapy notes</li><li>• Information compiled in reasonable anticipation of, or for use in a legal proceeding</li><li>• PHI for an inmate held by a CE that is a correctional institution or a provider working for one, if providing the copy would jeopardize health, safety, security, custody, or rehabilitation<ul style="list-style-type: none"><li>◦ <i>inmate retains the right to inspect her PHI</i></li></ul></li><li>• PHI in a designated record set that is part of a research study that includes treatment and is still in progress<ul style="list-style-type: none"><li>◦ <i>Patient must have agreed to the temporary suspension of access in advance and access will be reinstated upon completion of the research</i></li></ul></li><li>• PHI in the Privacy Act protected records (i.e., certain records under the control of a federal agency), if denial of access is permitted by the Act</li><li>• PHI obtained by someone other than a healthcare provider (e.g., a family member of patient) under a promise of confidentiality, and providing access to the information would be reasonably likely to reveal the source of the information</li></ul>	<p>Requests for:</p> <ul style="list-style-type: none"><li>• PHI that a licensed healthcare professional has determined in the exercise of professional judgment that if disclosed, would <u>reasonably likely</u> endanger the life or physical safety of the patient or another person</li><li>• PHI that the disclosure of which is <u>reasonably likely</u> to cause substantial harm to a person (other than a healthcare provider) referenced in the PHI</li><li>• PHI by a patient's personal representative, the disclosure of which would <u>reasonably likely</u> cause substantial harm to the patient or another person</li></ul>

# OCR FAQs: Denial of Access

- **Carrying Out the Denial - 45 CFR 164.524(b)(2)**

- If a CE denies access, in whole or in part, to PHI requested by a patient, the CE must provide a denial in writing to the individual no later than within 30 calendar days of the request
- The denial must be in plain language and describe the basis for denial
- Patient may submit a complaint to the CE or to the OCR
- If a CE does not maintain the requested PHI, the CE must inform the patient where to direct the request for access
- The CE must provide the patient with access to any other PHI requested, after excluding the PHI to which the entity has a ground to deny access
- Complexity in segregating the PHI does not excuse the obligation to provide access to the PHI to which the ground for denial does not apply

- **Review of Denial - 45 CFR 164.524(d)(4)**

- If the denial was based on a reviewable ground for denial and the patient requests review, the CE must promptly refer the request to the designated reviewing official
- The reviewing official must determine, within a reasonable period of time, whether to reaffirm or reverse the denial
- The CE must then promptly provide written notice to the patient of the determination of the reviewing official, as well as take other action as necessary to carry out the determination

# OCR FAQs:

## Patient's Right to Direct the PHI to Another Person

45 CFR 164.524(c)(3)

- Patients have the right to direct a CE to transmit copies of their PHI directly to another person or entity designated by the patient → “Patient Directive”
- Patient Directives must ...
  - Be in writing
  - Be signed by the patient (or the patient's personal representative)
  - Clearly identify the designated person
  - Indicate where to send the PHI
- Patient Directives ...
  - Do not need to be accompanied by a HIPAA-compliant authorization
  - Can be submitted by the patient, the patient's personal representative, or the Designated Person or Entity
  - Must be treated like a Patient Request
    - Copies of PHI must be provided in the format requested
    - For a reasonable, cost-based fee
    - No later than 30 days from the date the request was submitted



# OCR FAQs: Patient's Right to Direct the PHI to Another Person

- Example of a Patient Directive

Mrs. Minnie Mouse  
123 Mickey Way  
Celebration, FL  
12345

January 11, 2016

VIA CERTIFIED MAIL  
Goofy Medical Center  
Attn: Release of Information  
456 Snow White Lane  
Celebration, FL 12345

Re: Patient: Mrs. Minnie Mouse  
DOB: October 1, 1971

Dear Records Custodian:

This request is made pursuant to HITECH Act 42 USC §17935(e)(1), and its implementing regulations, 45 CFR 164.524(e)(4)(i), I am requesting in an electronic format only the following records:

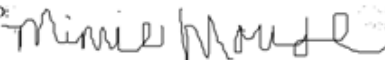
Date(s) of Service: ALL

Specific Records Requested: ALL RECORDS

Provide the records in electronic form in a .pdf file format on compact disc (CD) for the cost of labor and of a CD. Page charges for a digital file that can be copied to a single CD are not reasonable cost-based fees. The HITECH Act directs that a patient shall have the right to obtain electronic records for a reasonable cost-based fee.

Please be aware that the HITECH ACT was written specifically to allow a patient to direct medical records to "any" third parties and take advantage of the reasonable cost-based benefits of HIPAA. The rule includes attorneys or anyone else the patient designates in his letter requesting records. The final ruling by the U.S. Department of Health and Human Services specifically distinguishes the patient letter from a 3<sup>rd</sup> party HIPAA authorization, which is not required.

Please send the records to Dewey, Cheatem & Howe  
666 Crooks Lane  
Orlando, Florida 32804

SIGNED: 

## Patient-Directive Check List

- ✓ In writing;
- ✓ Signed by the patient;
- ✓ Clearly identifies the designated person; and
- ✓ Indicates where to send the records

# OCR FAQs: Patient's Right to Direct the PHI to Another Person

## Example of a Patient Directive

2/15/16  
To: 1000 Acre Hospital - Medical Records  
From: Christopher Robin  
Dear Medical Records Department, *see the enclosed letter for.*  
I am the Administrator of my friend Winnie-the-Pooh's estate. I need all of the medical records and billing records from his most recent stay - 8/2015 - 10/2015 at 1000 Acre Hospital. Please send them to me on a CD-ROM, here is the info:  
Patient: Winnie the Pooh (DOB: 1-1-31)  
mail CD-ROM w/ records to:  
135 Honeybrook Ave  
1000 Acres, CA 121212  
Sincerely, *Christopher Robin*  
Admin/Executor of Winnie-the-Pooh's estate

FILED  
SUPERIOR COURT OF WASHINGTON  
COUNTY OF KING  
IN THE MATTER OF THE ESTATE OF  
**Winnie the Pooh**  
JANICE MICHEL  
CLERK  
SEATTLE, WA  
NO. [REDACTED]  
LETTERS TESTAMENTARY  
(Certificate of Qualification)

The last Will of the above named deceased, was duly exhibited, proven and filed on **1 Oct. 2015**, and, it appears in and by said Will that  
**Christopher Robin**  
was named Executor and has been appointed by court order and has qualified by filing an oath and bond (if required) and is authorized to execute said Will according to law.  
WITNESS my hand and seal of said Court this **10 Oct. 2015**  
M. JANICE MICHEL, CLERK AND  
KING COUNTY SUPERIOR COURT CLERK  
JANICE MICHEL, Deputy Clerk  
SEAL  
SC015 CODE: LTR5

### Note:

This is an example of a personal representative's Patient Directive


### Patient-Directive Check List

- ✓ In writing;
- ✓ Signed by the patient;
- ✓ Clearly identifies the designated person; and
- ✓ Indicates where to send the records

# OCR FAQs:

## Patient's Right to Direct the PHI to Another Person

- Example of a Patient Directive

<div><b>LAW FIRM, LLC</b> Attorney at Law</div> <p><b>FAX COVER SHEET</b></p> <p><b>TO:</b> [Redacted] Medical Center, Fax: [Redacted]</p> <p><b>FROM:</b> [Redacted] Esq. [Redacted]</p> <p><b>RE:</b> Request for All Medical and Billing Records for [Redacted] from 6/30 [Redacted] to Present</p> <p><b>TOTAL PAGES (including this page):</b> 2</p> <p><b>ORIGINAL TO FOLLOW:</b> NO</p> <p><b>CONFIDENTIALITY NOTICE</b></p> <p>The information contained in this facsimile message is privileged and confidential, and intended only for the use of the individual(s) and/or entity(ies) named above. If you are not the intended recipient, you are hereby notified that any unauthorized disclosure, copying, distribution, or taking of any action in reliance on the contents of the telecopied materials is strictly prohibited and review by any individual other than the intended recipient shall not constitute waiver of the attorney-client privilege. If you have received this transmission in error, please immediately notify us by telephone (collect) to arrange for return of the materials. Thank you!</p>	<p>Date: <u>04-29-2016</u></p> <p>Medical Center [Redacted]</p> <p><b>Re: Health Records Request from 6/30 [Redacted] until Present</b></p> <p>Dear Records Custodian:</p> <p>I am a patient of Dr. [Redacted]. My birth date is [Redacted]. I request copies of any and all of my medical records including, but not limited to, radiological films, billing records, and outside records. Provide the records in electronic form on CD in the Adobe Acrobat (.pdf) format per the requirements of 45 C.F.R. § 164.524(c)(1)(i), as amended effective September 23, 2013. As you are aware, 42 U.S.C. § 17935(a)(2) and 45 C.F.R. § 164.524(c)(1) limit the cost of obtaining the records to the actual labor costs for reproducing them in the requested electronic format, the actual cost of the portable media (in this case, CD), and postage.</p> <p>Please send the records to [Redacted] as follows: [Redacted]</p> <p>SIGNED: [Redacted]</p>
--	--

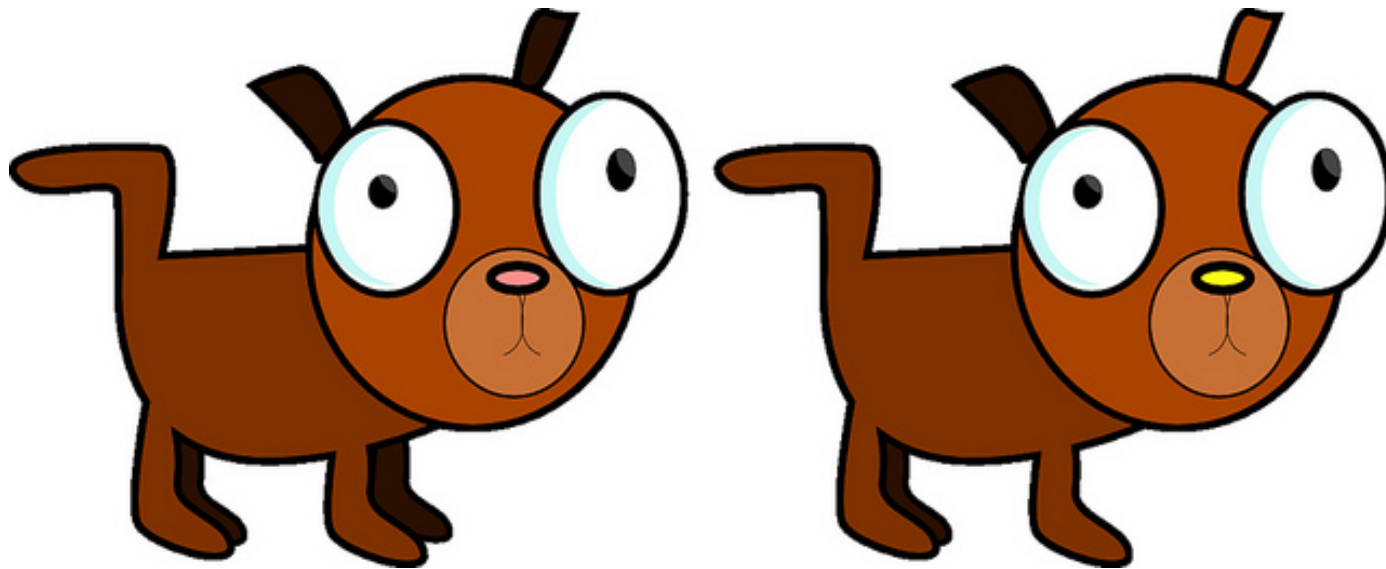
### Patient-Directive Check List

- ✓ In writing;
- ✓ Signed by the patient;
- ✓ Clearly identifies the designated person; and
- ✓ Indicates where to send the records

# OCR FAQs:

## Patient's Right to Direct the PHI to Another Person

- Telling the difference between Patient and 3<sup>rd</sup> Party Requests



# OCR FAQs: Patient's Right to Direct the PHI to Another Person

- Example of a Third Party Request

Hospital  
[Redacted]  
JAN 25 11:00 AM  
[Redacted]

Re: [Redacted] Dec'd  
DOB: [Redacted] Date of Death: [Redacted]

Dear Sir/Madam:

Please be advised that this law firm represents the Estate of [Redacted] through his Executrix, [Redacted]. Enclosed please find a signed HIPAA authorization together with a copy of the Estate papers authorizing the release of records.

Upon receipt of this letter, kindly forward to me any and all records pertaining to [Redacted] at your earliest convenience. Please also include copies of any and all photographs pertaining to [Redacted].

Pursuant to the HITECH Act, 42 U.S.C.A. § 17935, please provide the records in electronic form on CD-rom. Pursuant to the HITECH Act, the fee for the CD-rom cannot exceed the cost of the CD-rom and labor necessary to respond to this request. See 42 U.S.C.A. § 179355(e)(2) (2009); 45 C.F.R. §164.524(c)(4) (2002).

Please provide me with a pre-payment invoice, via fax, to [Redacted] prior to sending the CD-roms.

Thank you for your courtesy and cooperation.

Very truly yours,  
[Signature]  
Danielle Drew  
Paralegal to [Redacted]

1. I (the undersigned) authorize [Redacted] Hospital  
(Name) (City/State) [Redacted]  
To release information from the record(s) of: [Redacted]  
Date of Birth: [Redacted] Sex: [Redacted] Soc. Sec. No.: [Redacted]  
Covering the period(s) from [Redacted] to [Redacted]

2. Information to be released (check all that apply):  
☐ Progress Notes ☐ Radiology ☐ Diagnostic Tests ☐ Billing Records ☐ X-Ray Films  
☐ Lab ☐ History & Physical ☐ EKGs ☐ Operative/Procedure Report ☐ Discharge Summary  
☐ Complete Medical Records (including information regarding insurance, demographics, referral documents and records from other facilities). Other: Any and All Records and to Family

3. Information is to be released to: [Redacted]

4. Purpose of disclosure: Review

5. I understand this consent may be revoked in writing at any time. With the exception to the extent that disclosure of information has already occurred prior to the receipt of revocation by the above named provider. If written revocation is not received, authorization will be considered valid for a period of time not to exceed 90 days from the date of signing. To initiate revocation of this authorization direct all correspondence to [Redacted]

6. I understand that this consent is to include disclosure of (PLEASE INITIAL):  
☒ Alcohol and/or drug abuse report ☒ Psychiatric records  
☐ Sexually transmitted disease information ☐ HIV/AIDS information

7. A photocopy of this authorization is to be considered as valid as the original.

8. I understand that the information used or disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by Federal Law.

SIGNATURE: [Redacted]  
DATE: [Redacted]  
Student or personal legal representative (first-of-its-kind of legal guardian to sign only if patient is a minor, legally incompetent or deceased)

PRINT NAME: [Redacted]  
Relationship to plaintiff of personal legal representative signing for patient: [Redacted]

## Patient-Directive Check List

✓ In writing;

X Signed by the Patient;

Clearly identifies the designated person; and

Indicates where to send the records

# Patient Directives v. Third Party Requests

Documentation Provided	Request Type	Applicable Fee
<b>Request Letter signed by patient</b>	Patient Request or Patient Directive	Patient Rate
<b>Authorization</b>	Patient Request	Patient Rate
<b>Authorization + Cover Letter signed by Attorney</b>	Third Party Request	Applicable State Rate
<b>Authorization + Cover Letter signed by Attorney and Patient</b>	Patient Directive	Patient Rate
<b>Authorization + Cover Letter signed by Attorney + Request Letter signed by Patient</b>	Patient Directive	Patient Rate
<b>Cover Letter signed by Attorney + Request Letter signed by Patient</b>	Patient Directive	Patient Rate
<b>Cover Letter signed by Attorney + Subpoena + Authorization/Court Order</b>	Third Party Request	Applicable State Rate

# OCR FAQs: State Law

- HIPAA is a unique federal law in that it allows for state law to supersede HIPAA if the state law provides greater privacy protection of PHI and is not contrary to the HIPAA Privacy Rule
  - Example: State Law requires that access be provided to the Patient in less than 30 days
- *However*, if a State Law limits access in a way that is contrary to the HIPAA Privacy Rule, then it will be preempted by HIPAA
  - Example: State law that prohibits certain laboratories from disclosing test reports directly to a Patient

*State laws do not apply when a patient exercises her HIPAA right of access*

# [onchealthit@service.govdelivery.com]

## ONC Health IT

- **Sent:** Tuesday, July 11, 2017 2:03 PM
- **Subject:** Improving the Medical Records Request Process
  - ONC posted a new report and blog post identifying a number of ways to simplify the process for patients and health systems to request and share medical records.
  - The report looks at the challenges patients and caregivers face in obtaining their health information and the processes and request forms used by more than 50 health systems across the country.
- **Action:**
  - Download the Improving the Health Records Request Process for Patients Report
  - Read the blog post
  - Map the suggested process to your current processes
  - Modify and improve patient request workflow as needed



## 5 Tips for Providing Patient Access while Protecting Privacy

- 1. Review your patient access policies to ensure they do not create barriers to patient access**
- 2. Provide several means of providing patients with access to their PHI**
- 3. Compare your definition of a “designated record set” with the OCR’s FAQs on Patient Access**
- 4. Make sure your denial of access procedure aligns with the FAQs**
- 5. Review the fees that you are assessing to patients for copies of medical records!**

# What is on the Horizon

- **Fees for Copies of Records Requested by Patients**
  - While CEs are permitted to assess a fee for copies of PHI to patients, CEs should provide such copies for FREE
  - CEs should not assess a fee where the patient cannot afford the fee
    - *The OCR will continue to monitor whether the fees that are being charged to patients are creating barriers to this access, will take enforcement action where necessary, and will reassess as necessary the provisions in the HIPAA Privacy Rule that permit these fees to be charged!*
- **More Guidance from the OCR is coming**
- **Resolution Agreement or Civil Money Penalty related to Patient Access are coming**
- **Beware of phishing and ransomware**
- **Make sure you are monitoring your BAs**

# Helpful Tools

- OCR FAQs on Patient Access
  - <http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/>
- Phase 2 of HIPAA Audits
  - <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when>
- Administrative Safeguards
  - HHS - Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework: <http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/>
  - HHS Guidance on Risk Analysis: <http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html>
  - ONC's Security Risk Assessment Tools: <https://www.healthit.gov/providers-professionals/security-risk-assessment>
  - HHS Security Rule Guidance Material: <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>
- “Minimum Necessary” Rule
  - HHS Guidance on the Minimum Necessary Requirement: <http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html>
- Technical and Administrative Safeguards
  - HHS Guidance on Technical Safeguards: <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>
  - HHS Guidance on Physical Safeguards: <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf>

Join MRO for our Free Privacy & Security  
Webinar Series

<http://info.mrocorp.com/webinar-series>

Tuesday, September 19, 2017 – 3 pm Eastern

Healthcare Privacy And Security: What's On The  
Horizon



# Questions?

Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB  
Vice President, Privacy, Compliance and HIM  
Policy

Phone: 610-994-7500 x 526

[rbowen@mrocorp.com](mailto:rbowen@mrocorp.com)

<https://www.linkedin.com/in/rita-bowen-74206012/>

