Healthcare
Year In Review
2019

CMGMA
November 15, 2019

Presentation by Jennifer L. Cox, J.D.
Cox & Osowiecki, LLC
Hartford, Connecticut

Today's Program

Federal Update:

- PPACA status, including Section 1557
- EHR Rules: Meaningful Use, Promoting Interoperability
- Information Blocking

Connecticut Update:

- Cases affecting healthcare providers
- Subpoenas and Court Orders
- New Connecticut laws
- Regulatory and Agency Changes

HIPAA Important Issues Review:

- Outline of Patient's Right To Access Records
- Nuts and Bolts of Business Associate relationships
- Enforcement Activity

Q&A

PPACA Under Trump Administration

- PPACA was not repealed, but does not get strong support from the administration
  - Ongoing, drawn out federal litigation to end PPACA
  - Disruption in insurance/exchanges
    - Many states have only 1-2 choices on the exchange
- Some states (including Connecticut) reacting by making mini-PPACA rules in state law
- Reducing civil rights protections that were given under PPACA

PPACA Section 1557 & Conscience Rules

- HHS has proposed to roll back some PPACA Section 1557 rules, based on legal theory that Congress has not given HHS power to regulate gender identity or abortion rights through HHS program rules
  - Requirements relating to interpreters for Limited English Proficiency and Deaf and Hard of Hearing would remain, but notices, signage, and handout requirements might be relaxed
- **New proposed rules** to allow individual workforce to refuse to participate in any care that offended their religious or moral views (court rulings pending)

Federal Healthcare Policies During Trump Administration

Various areas moving ahead at status quo, mostly bipartisan basis:

- HIPAA
- Promoting Interoperability, EHR “incentive” programs (MIPS/MACRA and MU)
- Veteran’s Health
- **Information Blocking***
- Telehealth
- FDA issues
- Opioid crisis efforts
  - Federal laws to help support affected individuals

Federal Rules Information Blocking Meaningful Use and MACRA/MIPS

- Both MU and MACRA/MIPS programs include obligations for providers to attest that they are not information blocking
- The “Prevention of Information Blocking Attestation” is elaborate, and has three statements, each of which has accompanying guidance and definitions

Meaningful Use and Promoting Interoperability

Three Core EHR Anti-Blocking Obligations Already In Place

Statement #1

- Statement 1: A health care provider must attest that they did not knowingly and willfully take action (such as to disable functionality) to limit or restrict the compatibility or interoperability of CEHRT.

Statement #2 (parts 1 and 2)

- Statement 2: A health care provider must attest that they implemented technologies, standards, policies, practices, and agreements reasonably calculated to ensure, to the greatest extent practicable and permitted by law, that the CEHRT was, at all relevant times:
  1. Connected in accordance with applicable law;
  2. Compliant with all standards applicable to the exchange of information, including the standards, implementation specifications, and certification criteria adopted at 45 CFR Part 170…

Statement #2 (parts 3 and 4)

…[to the greatest extent practicable and permitted by law, that the CEHRT was, at all relevant times]:

3. Implemented in a manner that allowed for timely access by patients to their electronic health information (including the ability to view, download, and transmit this information); and
4. Implemented in a manner that allowed for the timely, secure, and trusted bidirectional exchange of structured electronic health information with other health care providers (as defined by 42 U.S.C. 300jj(3)), including unaffiliated providers, and with disparate CEHRT and health IT vendors.

Statement #3

- Statement 3: A health care provider must attest that they responded in good faith and in a timely manner to requests to retrieve or exchange electronic health information, including from patients, health care providers (as defined by 42 U.S.C. 300jj(3)), and other persons, regardless of the requestor's affiliation or technology vendor.

Expecting Final Federal Rules on Information Blocking From 21st Century Cures Act

- 21st Cures Act defines "information blocking" broadly as a "practice that . . . is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information" if that practice is known by a developer, exchange, network, or **provider** as being likely to "interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information."

42 U.S.C. §300jj-52(a).

- **You will need to pay attention when the final regulations come out…**we await regulations to implement this very, very soon! It's been a long wait, and rules have been promised **"any day now"** end of 2017… January 2018…summer 2018

Shift Caused By Information Blocking Focus

- HIPAA created a dichotomy between disclosures that are mandatory (e.g., patient access under 45 CFR 164.524; "required by law") versus others that are ***permitted*** but not required (e.g., for the healthcare operations of the other provider)
- Depending how the final version of the federal interoperability rules, **you might be forced to share access to your EMR/EHR with all providers, even when you cannot obtain patient's express consent**

Connecticut Legislative And Agencies Update

Connecticut Cases Affecting Medical Practices

Doe v. Cochran. July 16, 2019. CT Supreme Court 4-3 decision.

- Case created new liability to non-patient.
- Fact pattern:
  - Male patient went to PCP to be checked for STDs, told the physician it was meant as clearance before entering intimate relationship
  - Incorrect "negative" reported to patient (lab result showed positive, unclear why the wrong result was communicated)
  - Girlfriend of patient infected with herpes
- Girlfriend is allowed to sue the doctor (that's a change from decades of law principles)

HIPAA & Privacy Violation
Hefty Price Tag

- **Byrne v. Avery.** Trial ended December 2018
- **$853,000** jury verdict for privacy violation after an OB/Gyn practice **did not object to a subpoena**, but instead sent the subpoenaed records to a probate court.
- This case was the subject of an earlier Connecticut Supreme Court case that asked whether a person can sue for what is essentially a HIPAA violation, when HIPAA itself says you cannot.
- Answer: Yes.

Subpoena Alone – Not Enough

Court Orders, Subpoenas, and Litigation Matters

Immediate Lessons Learned

- Do not mail HIPAA-protected records to court as solution to subpoena (without more careful analysis)
- A lawyer who issues the subpoena – but has not provided an authorization, court order, or satisfactory assurance who tells it's okay to simply mail the records to court is **incorrect**

Be Very Careful With Lawyer Requests!

- Lawyers can subpoena records – but that does not mean you are legally able to comply under HIPAA and state law
- A patient's authorization, court order, or "satisfactory assurances" are needed before you may release a record in response to a subpoena
- Do not comply with lawyer's subpoena without meeting this rule – which probably means your own motion to quash (or "letter to quash"), or court order, because in Connecticut you never run out of time to object

HIPAA Rules For Judicial And Administrative Proceedings

- **A subpoena is not a court order**
- You may release in response to an order from a court or administrative tribunal (but only as much as the order allows – read it carefully)
- You are allowed to appeal a court order (rare circumstance)
- You will not be held accountable if you choose to comply with a court order, even if the court ends up being wrong
- Other parties might object

Judicial And Administrative Proceedings

Absent an order of, or a subpoena issued by, a court or administrative tribunal, a covered entity may respond to a subpoena or discovery request from, or other lawful process by, a party to the proceeding only if the covered entity obtains either:

(1) satisfactory assurances that reasonable efforts have been made to give the individual whose information has been requested notice of the request; or

(2) satisfactory assurances that the party seeking such information has made reasonable efforts to secure a protective order that will guard the confidentiality of the information

Satisfactory Assurances

- Satisfactory assurances:
  - If covered entity receives from a requesting party a written statement and accompanying documentation demonstrating that:
    - The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); and
    - The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and
  - The time for the individual to raise objections to the court or administrative tribunal has elapsed; and
    - No objections were filed; or
    - All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

Judicial And Administrative Proceedings: Operational Tips

- Have a satisfactory assurance form available if you are going to rely on this
- Keep in mind: most lawyers are not healthcare lawyers and have a low level understanding of HIPAA, and they think that state litigation rules of practice trump HIPAA (not true)
- Distinguish federal, state and agency subpoenas – complicated rules that may need attorney review
- Some federal agencies have powers to compel disclosure (e.g., Department of Labor in OSHA investigation)
  - ask for citations and paperwork

2019 New Laws

2019 Legislative Session

Law Changes – Connecticut

- “Surprise billing” -- stricter controls on billing out-of-network when seeing a patient at a facility
- Essential elements of PPACA required under state law continue to be added (e.g., clarifying pre-existing condition insurance rules, mandatory coverages, maximum cost sharing, medical necessity definitions)
- Attempts to close loophole on cost sharing for mammography and follow up ultrasound

Law Changes – Connecticut

- Restricts carriers from taking adverse actions against in-network providers who discuss legitimate care options with patients
- Tasks DSS to see if there's a way to pay for telehealth encounters for Medicaid patients
- Allows certain people to store Epi-pens for use on as yet unknown patient

Law Changes – Connecticut

- Adds inflammatory breast and GI cancers to list of topics eligible under “risk management” prong of required CME
- Allows more automatic licensure action based on out-of-state licensure discipline
- HIV treatment of minors: clarification that physicians and APRNs may provide prophylactic HIV treatment to minors (not vaccines)

Law Changes – Connecticut

Change of **scope** for:

- APRNs (scores of updates – could be seen as widening the gap to PAs scope)
- Changes the description of the relationship between PA and physician from “dependent” to “collaborative” (nothing else changes, written delegation agreement is still needed with PAs)
- Creates mid-level “associate” status for professional counselors and MFTs while working toward full licensure

Law Changes – Connecticut

Change of **scope** for:

- Only B.A. or Master's level trained social workers can be called "Social Worker"
- Art therapists, new licensure category

Law Changes - Connecticut

- Requires compounding pharmacies to comply with various chapters of the USP
- Updates medical marijuana requirements
- Opioid prescribing and treatment changes

Business Laws Affecting Everyone

- Paid FMLA start in 2022
  - Payroll deduction starts 2021
  - Pool of employees who can take leave and paid leave, significantly expanded to include taking care of close friend (not just close family)
- Stricter requirements for sexual harassment training, now triggered if you have three (3) or more employees
- Increases minimum wage $1/hr every year until max at $15.00 in 2023

Likely Issues During 2020 Session

- Debate over vaccine exemptions
- Enhanced privacy protections
- PAs seeking more parity with APRN scope
- Site neutral payment rules
- Explore expansion state health plan (to non-state employees)

HIT & Office Of Health Strategy

- HIT oversight and OHCA oversight was shifted to Office of Health Strategy
  - OHCA was renamed
  - Oversees:
    - Health System Planning Unit, handles CONs (formerly OHCA handled CONs)
    - HITO, HIE
    - APCD
- **A new state-run HIE entity has emerged! Affects hospitals first, physicians next**

HIPAA Still Critically Important

HIPAA Review and Refocus:
Key Issues

Who Is Directly Covered By HIPAA?

Covered Entities (CEs):

- **Health Plans** (including private carriers and Medicare, Medicaid, and other government healthcare payer programs)
- **Health Care Providers** who bill electronically
- **Healthcare Clearinghouses** (billing switch or other company that puts data into standard billing transaction)

Business Associates (BAs) of any of the above CEs, and their subcontractors

What Does HIPAA Cover?

- HIPAA Privacy and Security Rules are designed to protect PROTECTED HEALTH INFORMATION, abbreviated as **PHI**
- Essentially, PHI comprises information you have or know about an individual **(patient or enrollee)** because you are a CE (or BA)
  - **It does not need to be health care specific information to be PHI**
- When PHI is electronic it is called **EPHI**

Best Practices Handling, Internal/Staff Access and Use

- **Policies or practices needed** to set limits for:
  - Texting, phone messages
  - Bring Your Own Device, staff's personal telephone number/email
  - Taking records offsite
  - Social Media use
  - Remote access
  - Staff/workforce system access rights
  - Scope of records available to each worker/staff member
    - Records should be complete – but not everyone needs to see every part

Retention of HIPAA Records and Policies: Six Years For HIPAA Documentation

- Retention Obligations:
  - Authorizations
  - Correspondence or memos about access decisions
  - Patient amendment requests and responses
  - Accounting requests and responses
  - All policies and procedures
  - Security Risk assessment materials
- **Do not confuse this with record retention for health records, which is *generally:* 7 years for last date of care (or 3 years after patient died) in community setting; 10 years for hospitals and facilities**
  - Some exceptions apply to retention schedule for medical records, the time period differs by setting/licensure

Vendors and Contractors

Business Associates

Business Associates

- A business associate is any entity that **on behalf of** a covered entity or **on behalf of** another BA :
  - Creates
  - Receives
  - Maintains or
  - Transmits PHI
- Maintains includes physical and virtual storage vendors (e.g., box storage facilities and cloud services) **even if they do not view or access PHI**
- OCR guidance available on BAs, including for specific activities (e.g., Cloud Services)

Business Associates

Business Associates:

- Must comply with the Security Rule and the Breach Rule
- Must observe Privacy Rule to extent CE would need to
- Are directly responsible for their own HIPAA fines
  - But CE not off the hook
- Subcontractors will be held to same standards as business associates (including need for BAA paperwork between BA and subcontractor)
- Must comply with the minimum necessary standard

Business Associate Specific Situations

Definition of BA clarifies:

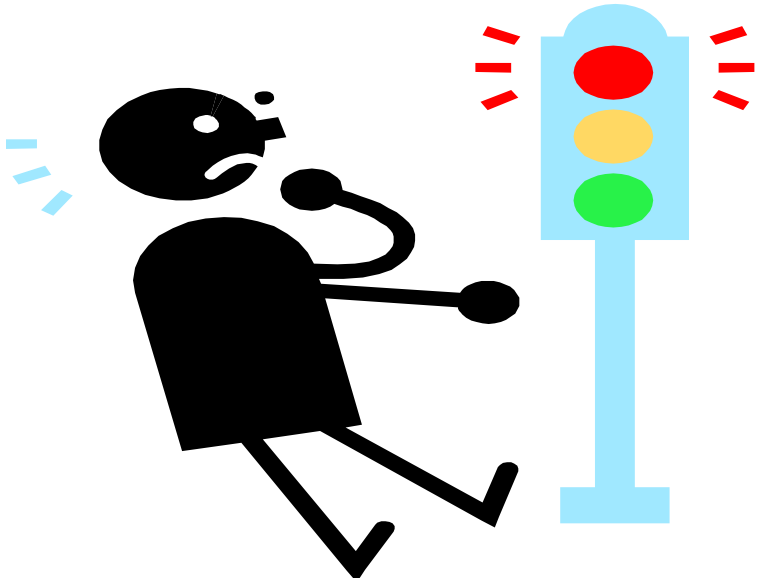
- HIO/HIEs, e-prescribing gateway, or other entity that performs transmission services and might require access to PHI (e.g., for audit or troubleshooting) is a BA
- Paper Record Storage company is a BA
- BA includes personal health record vendor working for a CE (but not a stand-alone personal health record company)

Business Associate Relationships "To Do" List For Practices

- Be sure you have identified all BA situations
  - Check every entity or person you pay for services
  - Check all independent contractors that are not "workforce"
  - Check every relationship where you exchange or share data
- Ensure there is a BAA between you that was updated on or after January 2013
- Have a process for reviewing all new contractors to determine if BAA needed
  - Water delivery company = no BAA
  - Paper record storage company = BAA
- Review OCR resources on BAs:
  - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

Failure To Comply With The HIPAA Privacy Rule

Breach



Breach Rule Baseline

A breach occurs upon acquisition, access, use, or disclosure of PHI in a manner not permitted by the **Privacy Rule**

Potential Penalties for breach and/or noncompliance with HIPAA are staggering and include fines by the federal government (rare but possible), but more commonly requirements to provide identity protection services for affected individuals, which adds up quickly

Breach Rule Basics

- **Breach is connected to the Privacy Rule (not the Security Rule)**
- Security Rule failures might also be breaches if they compromise privacy of PHI
- Security fails are “security incidents” under the Security Rule
- Stolen or lost laptop (or other portable device or media **containing PHI**) likely to be a breach if the device or media is not encrypted

Breach Rule Three Exceptions

A breach occurs upon acquisition, access, use, or disclosure of PHI **in a manner not permitted by the Privacy Rule**, unless:

1. Unintentional access or use by workforce or someone acting within authority, no downstream access
2. Inadvertent disclosure within the organization by or between authorized persons
3. Disclosure made to unauthorized person but he/she could not have retained or copied the PHI

Low Probability Of Compromise

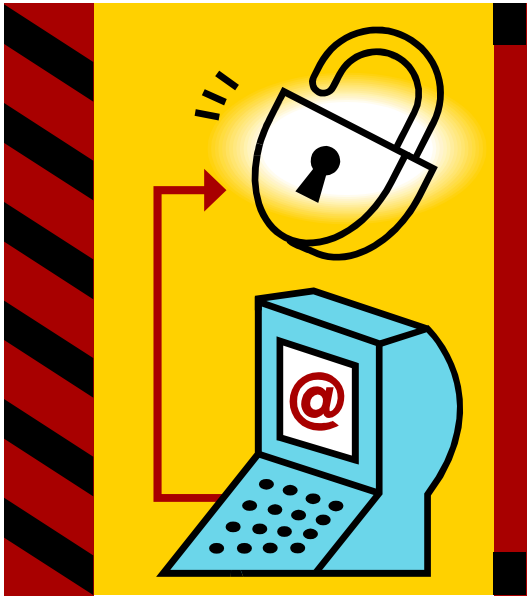
If none of the three exceptions is met, a breach has occurred, unless CE/BA demonstrates a "low probability" of PHI compromise based on *at least* these factors:

- Nature and extent of the types of PHI, and likelihood of re-identification
- Who received the PHI improperly
- Whether PHI was actually acquired or viewed
- Extent to which risk is mitigated

- **Fact specific test: analyze on a case-by-case basis!!**

Breach: Unencrypted Portable Devices And Media Are Dangerous

- **Encryption is (semi) immunizer to breach**



If No Exception Exists You Must Report The Breach To Patients And OCR

- If you find a Breach of unsecured PHI (or EPHI) occurred, and no exception fits, you must report to the involved **individuals and to the federal government**
- Very specific rules for notice or reporting must be observed
- The timeline is very short – contemplates 60 days from when the breach was (or should have been) detected
  - Sometimes you find out well after that time would have run – there is no explanation for what your timeline is at that point (other than ASAP)
- Rule anticipates CE will be involved if BA has a breach, that BA will not contact patients directly, and most BAAs have requirements for BA to contact CE and keep them apprised

Breach Reporting – To Patients

Breach notices to individuals must include a brief description of:

- What happened, with the dates of both the breach and discovery
- The types of information involved
- Steps the individual can take to protect against potential harm (e.g., contact credit card companies or obtain credit bureau monitoring)
- What CE is doing to mitigate the harm and protect against further breaches (e.g., filed police report about stolen computer; retraining employees)
- Contact information to allow individuals to ask questions or receive additional information (which must include toll-free number, email address, web site, or postal address).

Breach Reporting – To HHS/OCR

- If 500 or more persons' records are involved:
  - Immediately notify HHS (through its website)
  - Publish press release for local media
- If **fewer than 500 persons' data are involved**, you are not required to immediately report, but you are required to file an annual report (electronic portal forms are on the HHS website)
  - By close of February (60 days after close of calendar year)
- You must use the online reporting system (which historically was not encrypted)

- Odd provision, law enforcement delay: law enforcement may request that you delay any notice, report or posting to avoid interference with criminal investigation or with national security. Very specific rule.

Specific Requirements, Breach Rule Compliance

By rule, CE and/or BA **must have all of the following** for Breach compliance, **crafted specifically to follow Breach Rule requirements:**

- Workforce training (specific to Breach Rule)
- Complaint process (specific to Breach Rule)
- Workforce sanction policy (identifies Breach Rule)
- No retaliation for reporting or exercising rights
- No forced waiver of rights
- Formal policies and procedures
- Retention of all policies, procedures and key supporting communications or materials for a minimum of six (6) years

Breach Compliance Planning: Operational Tips

- Have a response team
  - Have a quick response team for tactically urgent situations
  - Have an off-hours response plan
- Have point people for addressing potential or reported breach situations (not just one person, who might be on vacation or unreachable)
- Ensure your actual processes are consistent with your policies and procedures

Patient Access Rights

OCR Issued In-Depth Guidance In 2016 On Patient Access Rights

(They want you to pay careful attention. Did you?)

Patient Access Rights: 35-page FAQ Settles Many Questions

- OCR "new" (2016) 35-page FAQs on direct access:

www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/#newlyreleasedfaqs

- Mapped as: HHS Home > HIPAA > For Professionals > Privacy > Guidance > Individuals' Right under HIPAA to Access their Health Information

This 35-page FAQ From 2016 Should Be Required Reading

This is serious – and OCR wants you to pay attention….

Baseline: Patient Access Rights Are Incredibly Strong

- Patient has a *very strong right* to access his/her own record and information, although not an absolute right
  - There are very few times when you can deny a patient's access request
- There has not been a HIPAA Rule change (Rule change would require a rule making process and public comment); but this lengthy FAQ contains new information

Designated Record Set

Individuals have a **right to access** PHI in a "designated record set," which is defined (at 45 CFR 164.501) as a group of records maintained by or for a covered entity that comprises the:

- Medical records and billing records about individuals maintained by or for a covered health care provider
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals
- "Record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity

FAQ Stand Out Issues

- Copy fees must be limited
- 30 days is the maximum time to fill request
- Creating burden for patients about record request is unacceptable
- You really would have to send patient records in unencrypted email to the patient (if patient insists and is warned of risk)
- Lab PHI access has nuances

How Many Days, Maximum, to Fill Record Request For Connecticut Providers?

30 Days

30 days is the “outer limit”

- There are virtually no exceptions to this rule
- Exceedingly rare that you would be allowed to withhold a record from a patient

Invalid Reasons to Deny Access

- Request is for electronic records
- Patient lives in Sri Lanka
- We had staff out sick
- Patient is mean and insulting
- Case is in litigation
- This isn't our patient anymore
- Physician does not think the patient needs the record (not a safety issue)
- Patient has an outstanding bill
- We had more requests than usual
- Patient refuses to pay the copy fee
- Patient just got a copy last month, and has submitted a new request
- ***Patient refuses to sign my full authorization form***

Copy Fees Must Be Reasonable And Cost-Based For Access

Copy fee for direct **"access"** requests may only include:

- Supplies and **labor** for copying PHI, postage, and cost for preparation of a summary (if individual agrees to take summary)
- Labor costs include compiling, extracting, scanning and burning to media
- Cost of electronic media (only if patient agrees)

- **Copy fees for third party requests are not as confined**

OCR: Labor Costs MAY Include

- *Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied.*

OCR: Labor Costs MAY Include

For example, labor for copying may include labor associated with the following, as necessary to copy and deliver the PHI in the form and format and manner requested or agreed to by the individual:

- *Photocopying paper PHI.*
- *Scanning paper PHI into an electronic format.*
- *Converting electronic information in one format to the format requested by or agreed to by the individual.*

OCR: Labor Costs MAY Include

Continued…

- *Transferring (e.g., uploading, downloading, attaching, burning) electronic PHI from a covered entity's system to a web-based portal (where the PHI is not already maintained in, or accessible through, the portal), portable media, e-mail, app, personal health record, or other manner of delivery of the PHI.*
- *Creating and executing a mailing or e-mail with the responsive PHI.*

Labor Cost May NOT Include…

- *Reviewing the request for access.*
- *Searching for, retrieving, and otherwise preparing the responsive information for copying. This includes labor to locate the appropriate designated record sets about the individual, to review the records to identify the PHI that is responsive to the request and to ensure the information relates to the correct individual, and to segregate, collect, compile, and otherwise prepare the responsive information for copying.*

In Case You Missed the Point…

OCR is moving toward free or mostly free records:

- *While we allow labor costs for these limited activities, we note that as technology evolves and processes for converting and transferring files and formats become more automated, we expect labor costs to disappear or at least diminish in many cases.*

Methods for Fee Calculation

Subject to the rule caps and detail, these three methods are expressly acceptable:

- Actual cost
  - For that record request
- Average Cost
  - Based on developed schedule of labor costs, plus supplies and postage
- **Per page fee is not acceptable proxy *for e-copies***
    - **Flat fee of $6.50 or less is a "safe harbor"**

Practical Implementation: First Determine If the Request Is Direct

- Direct patient requests are governed by Access rule, found at HIPAA section [45 CFR] 164.524
  - Distinguish this from requests that come from a third party, based on authorization from the patient allowing covered entity to disclose
- Be ready to tell patient copy fees in advance

Practical Considerations

- Cost caps apply to paper and electronic (although suggested $6.50 is directed to e-copies)
- **State fee cap of $0.65 per page is a maximum!!!**
- You may not hold a copy request for failure to pay copy fees
- Do not charge when records are being requested in connection with a social security application or Veteran's benefits application
- DSS has been telling community providers not to charge for Medicaid patient copies

Why Is $6.50 Important?

- $6.50 is the guidance “safe harbor” cap for e-copies.
- This would be the fee for an entire record if the provider has not instead met one of the two available mathematical equations

$6.50

OCR Enforcement of HIPAA

Resolution Agreements provide a guide to OCR's thought process and enforcement focus

Watching For HIPAA Danger Zones

- Office for Civil Rights (OCR) has a variety of notices and tools designed to help organizations remain HIPAA compliant, including, a running list of Resolution Agreements:
  - www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/
- The Resolution Agreements are designed to be parables to industry on what OCR thinks is important in HIPAA compliance
- Tracking and reviewing these should be part of routine compliance processes
- The Resolution Agreements are summarized on the following slides

HIPAA Enforcement Continues

Most Recent OCR
Penalty Activities

Just Say No To Film Crews

- **September 2018**. $990,000
- Boston Medical Center, Brigham and Women's Hospital, and Massachusetts General Hospital compromised PHI by inviting film crews on premises to film an ABC television network documentary series, without **first obtaining authorization** from patients
- Obtaining consent *after* filming is not enough

Huge Data Loss Results In A Very Hefty Penalty

- **October 15, 2018.** $16 million
- Anthem failed to protect data of 78.8 million individuals from hacking
- Failure to have necessary security systems
- Failed to have adequate system activity review

Repeat Lesson: Do Not Speak To Reporters

- **November 26, 2018.** $125,000
- Allergy Associates of **Hartford**, P.C. released PHI to a reporter in February 2015
- Patient had made a complaint about service animal. A physician-workforce member discussed the issue with the reporter after the complaint was made. Practice didn't discipline the physician.
- OCR's investigation found that the doctor's discussion with the reporter demonstrated a reckless disregard for the patient's privacy rights and that the disclosure occurred *after* the doctor was instructed by group's Privacy Officer to either not respond to the media or respond with "no comment."
- Must also adopt a corrective action plan for ongoing HIPAA compliance

Repeat Lesson: BAA Is Essential For Vendors That Handle PHI

- **December 4, 2018.** $500,000.
- Advanced Care Hospitalists (ACH), a hospitalist contract/staffing service, working in Florida
- 2011 and 2012 ACH used a third-party billing company, but **failed to obtain a BAA**
- Billing company was less than professional, failed to protect PHI; hospital came across patient data on open website, informed ACH
- ACH also failed to have BAA policy, SRA, or other basic HIPAA policies

Repeat Lesson: Must Terminate Employee Access When Job Ends

- **December 11, 2018**. $111,400.
- Colorado critical access hospital failed to terminate access rights of an employee for months after separation
- Also failed to have a BAA with scheduling vendor

Failing to Fix Known Errors, Failing to Have Adequate Security

- **February 7, 2019**. $3,000,000.
- Cottage Health three hospitals in California, reported breaches in 2013 and 2015, both relating to improper configuration of servers, allowing access over the internet and without requiring unique ID/password.
- Exposed patient names, addresses, dates of birth, diagnoses, conditions, lab results, other treatment information to anyone with access to Cottage Health's server, and exposed ePHI over the unsecured
  - Failed to conduct accurate and thorough SRA
  - Failed to deploy routine security measures
  - Failed to obtain BAA with vendor

Cover Up (Or An Anemic Response) Can Make Things Worse

- **May 6, 2019**. $3,000,000
- Touchstone Medical Imaging (Tennessee) was informed by the FBI that their server had been accessed by unauthorized entity
- Response to FBI's notice was underwhelming and self-serving, concluding no breach
- In reality, Touchstone failed to: properly recognize issue, provide timely breach notice, or remediate exposure of 300,000 patients' PHI
- Also failed: to have BAAs, to have adequate SRA

Adequate SRA Is Mission Critical

- **May 23, 2019**. $100,000.
- Medical Informatics Engineering (MIE), an Indiana based company, provides software and medical record services to providers
- July 2015, MIE reported breach of 3.5 million patient records – hacking event using compromised ID/password
- OCR found MIE failed to perform adequate SRA prior to breach

When Protecting Privacy Turns Into Denying Access

- **September 2019.** $85,000
- Bayfront Health (Florida)
- Took 9 months to provide mother with prenatal records
  - EMR probably sees this as different patient
- 30 days for access is the maximum – you have to work through the issues within that time

"She Started It!" Is Not a HIPAA Concept – Avoid Social Media Disclosures

- **October 2019.** $10,000.
- Elite Dental practice (Dallas, TX)
- Responded to a patient's social media post
- Practice wanted to defend itself against allegations
- DO. NOT. ENGAGE. on social media with a patient

HIPAA Must Be A Priority

- **October 2019.** $2,150,000.
- Jackson Health (Miami, Florida)
- Multiple HIPAA failures
  - Failed to detect breaches
    - Paper and digital
  - Failed to timely report breaches (some discovered and reported years later)
  - Failed to conduct SRA

Q & A