Healthcare Year In Review
2018 Edition

CMGMA
November 16, 2018

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

Today's Program

- Review federal approach to healthcare issues
- Connecticut cases affecting healthcare practice
- New Connecticut laws
- Update on Electronic Prescribing mandates
- Opioid crisis developments
- State malpractice case statistics
- HIPAA Important Issues Review
  - Business Associate compliance
  - Breach core rules
  - Individual's Right to Access Records
  - Enforcement Activity
- Subpoenas and Court Orders
- 21st Century Cures Act & Information Blocking
- Q&A

Federal Healthcare Policies During Trump Administration

Key initiatives:

- Not repealing – but *diluting* PPACA
  - Allowing less robust coverage to count
  - Favoring private insurance
  - Allowing employers more flexibility
  - Changing (restricting?) how states can innovate
- Revising payment rules and programs, little by little
- Reducing civil rights protections (e.g., LGBT rights)

Federal Healthcare Policies During Trump Administration

More or less staying the course already in process during Obama administration:

- HIPAA
- Health IT (including MIPS/MACRA and MU)
- Veteran's Health
- FDA issues
- Opioid crisis efforts

Connecticut Cases Affecting Medical Practices

- *Gagliano*. High verdicts keep coming.
  - $12 million verdict upheld against hospital for error of surgical resident (who was not the hospital's employee)
- *Cochran*. (Pending appeal at CT Supreme Court)
  - Question of whether a physician is liable to a third party who is directly affected (made sick) by a failure in the care or report to a patient.
- *Avery*. HIPAA can be used as the standard of care for a privacy law suit.

Law Changes – Connecticut

- Pregnant women may exercise Advance Directives rights
- Essential elements of PPACA required under state law (in case federal law changes)
- Maternal deaths to be studied
- New requirements for DPH obtaining expert input on amniotic fluid embolisms, and making AFE education widely available

Law Changes – Connecticut

- Biological product prescribing restricted
- Connecticut Prescription Drug Monitoring and Reporting System to be enhanced
- APRNs may perform advance directive functions (previously only MD/DO could)
- Removes limit of six PAs that one MD/DO can supervise

Law Changes - Connecticut

- HIT oversight and OHCA oversight shifted to Office of Health Strategy
  - OHCA renamed Health System Planning Unit
- Prohibition on DPH disclosing personnel records collected during an investigation
- Updated telehealth law to allow for limited amount of substance use disorder care via telemedicine (consistent with federal law)

Law Changes – Connecticut

- Modernizes outdated language of “venereal disease” to be STDs
- Allows local health districts to combine activities and operations
- Change of scope for:
  - Podiatrists
  - Respiratory care therapists

Update: Mandatory E-Prescribing Of Controlled Substances (EPCS)

- Connecticut law was updated in 2017 to mandate that all controlled substance prescribing be done either:
  - through appropriate e-prescribing technology
  - with a waiver from DCP that allows a practitioner to continue using paper prescriptions for controlled substances
  - with a paper prescription in limited circumstances (situational exceptions to e-prescribing)

Update: Mandatory E-Prescribing Of Controlled Substances (EPCS)

- Drug Control Division of the Department of Consumer Protection oversees enforcement of EPCS
- Website has information on the EPCS process and waivers
  - https://portal.ct.gov/DCP/Drug-Control-Division/Drug-Control/EPCS-Information-Page
- Eventually waivers will not be permitted

Opioid Crisis Issues

- Increasing restrictions on dose and days of opioids
- Alternative pain management favored
- More PDMP tracking
- Required EPCS
- Plan for reversal drugs to be more widely available
- New federal funding for addressing opioids

Current State of Malpractice Claims

Connecticut Closed Claims Reporting System Provides Detailed Information About Claims

2018 Closed Claims Report

Includes claims data for calendar years 2013 through 2017

- **2,827** total closed claims over the past five years
  - **1,640** reported by commercial insurers
  - **1,187** reported by self-insurers

- Resolution
  - **1,444** resolved in favor of the plaintiff
  - **1,383** resolved in favor of the defendant

2018 Report: Payments

- Of **1,444** claims, **$892 million** paid to claimants
  - **$617,986** average indemnity payout to a claimant
- 684 of 1,444 claims paid out less than $200,000
- Million dollar plus claims:
  - 20% of all claim counts
  - 68% of all indemnity payments – more than **$610 million**

Highest Indemnity Payments 2018
Average By Specialty

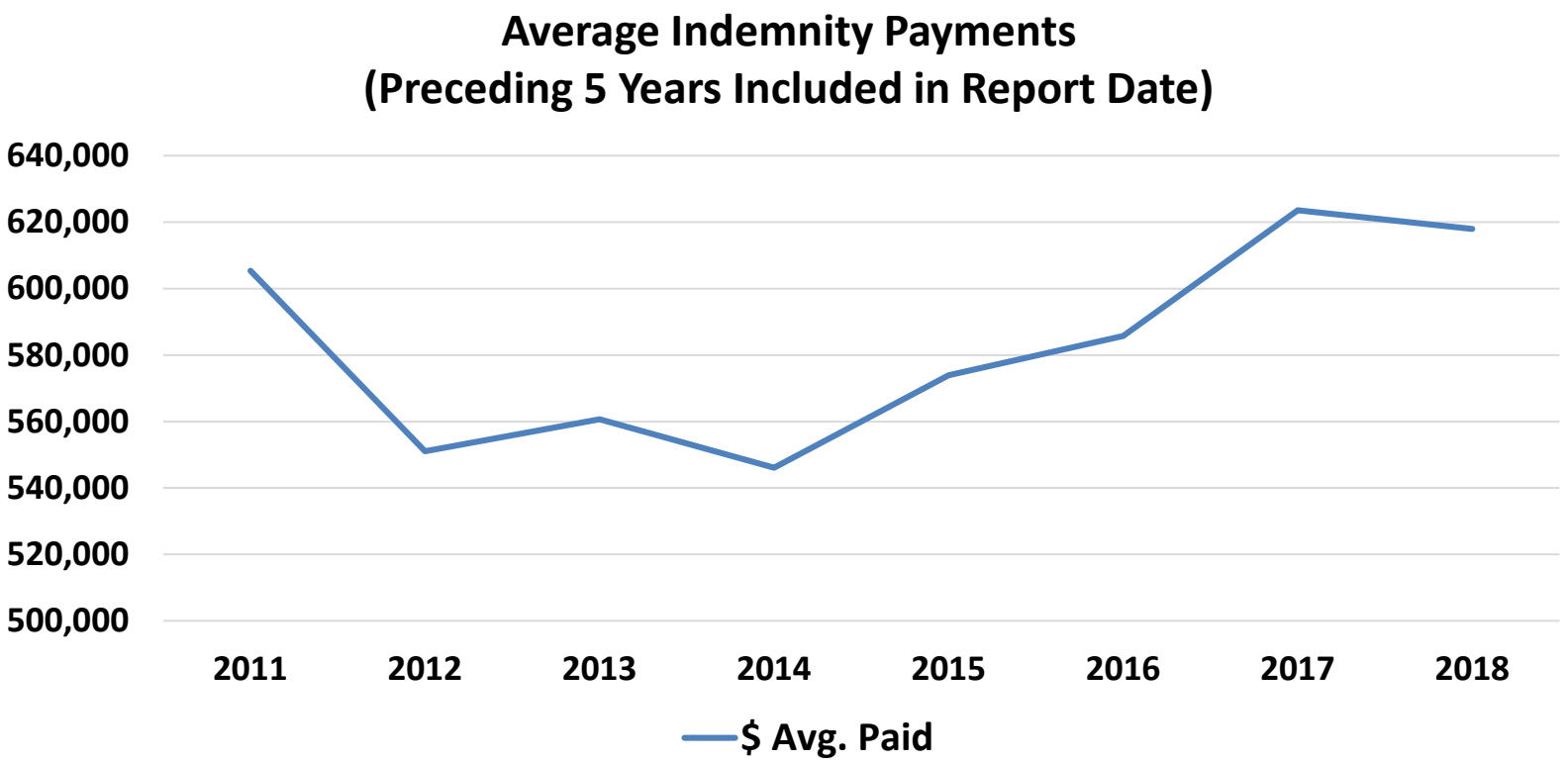
Hospitals-General: $810,752 for 590 claims
Hospital – Other: $554,890 for 26 claims

Gynecology/OB-GYN:	$640,375 for 48 claims
Physicians "other":	$636,313 for 316 claims
Emerg. & Ambulance:	$596,272 for 41 claims
Radiology/Imaging:	$586,585 for 44 claims
Medical Group Practice:	$559,290 for 59 claims
Orthopedics:	$550,276 for 49 claims
Anesthesiology:	$529,700 for 20 claims

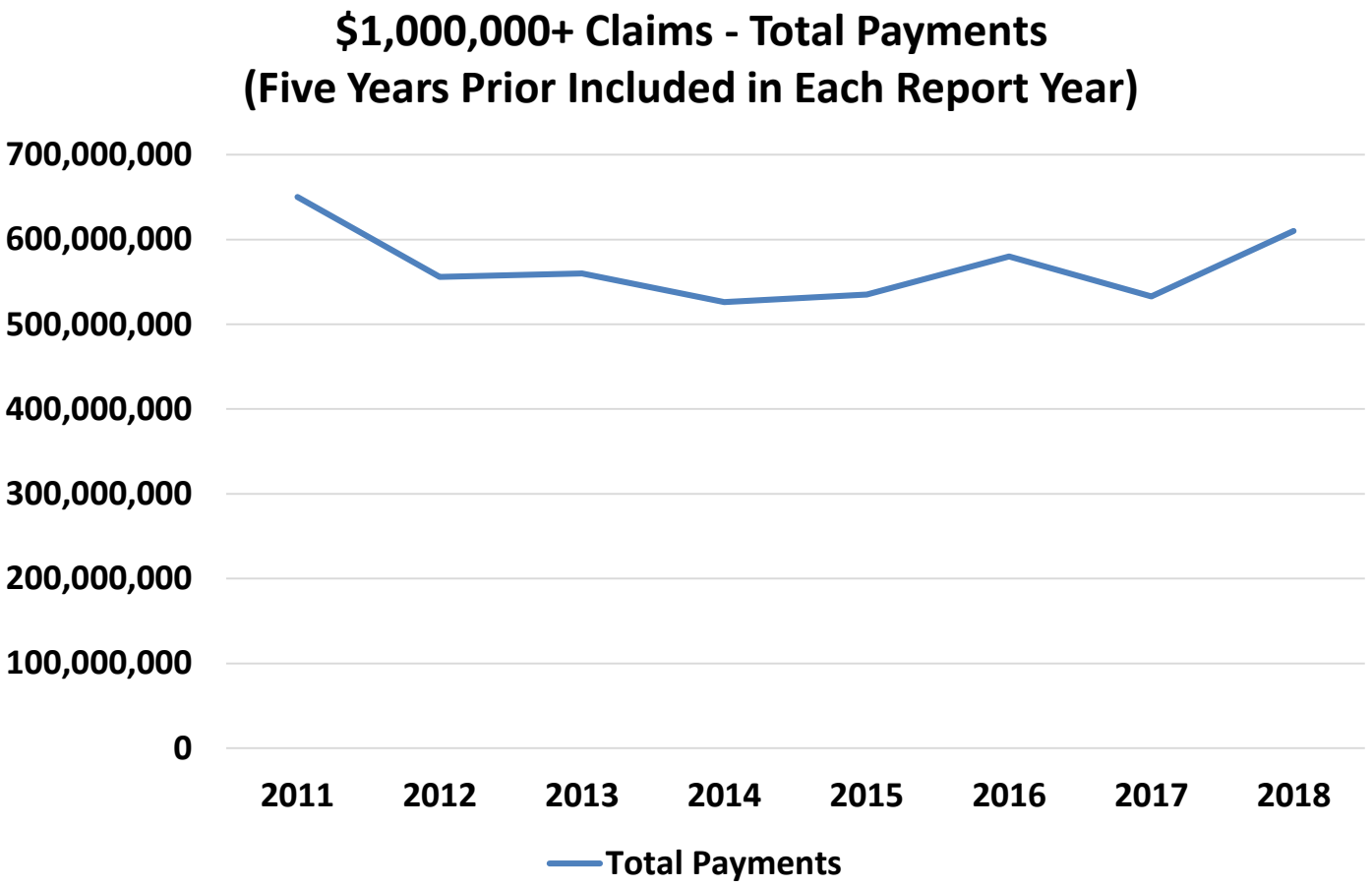
Trends in Indemnity Payments

Indemnity Payments (Five Years Prior Included in Each Report Year)								
Report Year	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
% No Payments	53%	53%	54%	54%	55%	54%	53%	49%
% With Payments	47%	47%	46%	46%	45%	46%	47%	51%
$ Total Paid	$951.6M	$861M	$836M	$798M	$797M	$865M	$911M	$892M
$ Avg. Paid	$605,327	$550,998	$560,656	$546,114	$573,878	$585,778	$623,558	$617,986

Average Indemnity Payments



Trends in Million Dollar Plus Claims



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:

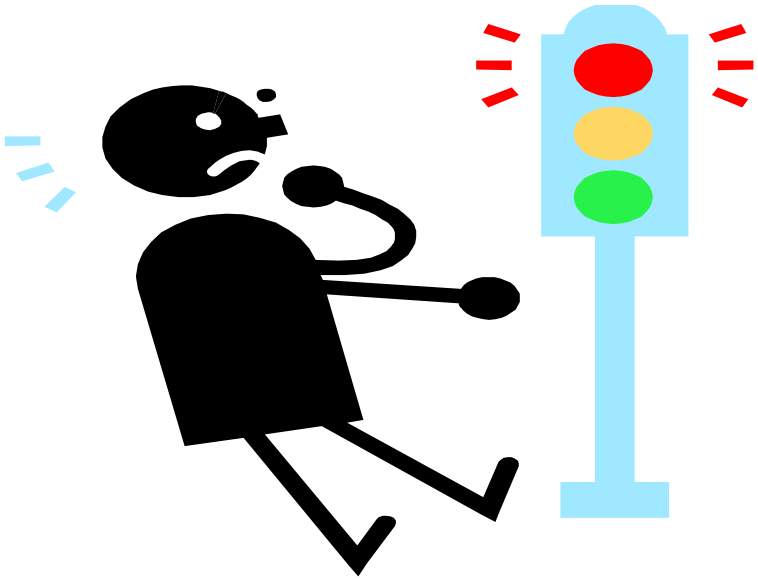
- HIO/HIEs, e-prescribing gateway, or other entity that performs transmission services and might require access to PHI (e.g., for audit or troubleshooting) is a BA
- Paper Record Storage company is a BA
- BA includes personal health record vendor working for a CE (but not a stand-alone personal health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

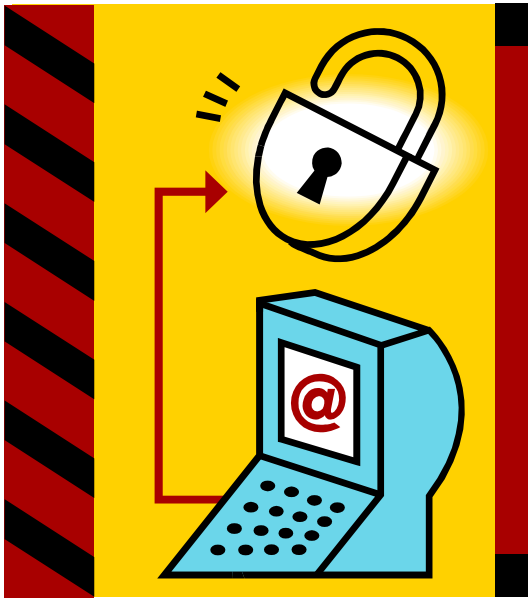
If none of the three exceptions is met, a breach has occurred, unless CE/BA demonstrates a "low probability" of PHI compromise based on *at least* these factors:

- 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

Does the 35-page FAQ Contain New Rules?

Sort of….

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

Enforcement Picks Up Again

OCR Activity Since This Time Last Year

Cyber Threats Are Real

- **December 2017**, 21st Century Oncology, Florida, to pay $2.3 million
- Cancer care services and radiation oncology in 179 treatment centers, including 143 centers located in 17 states in the USA
- **Failed to conduct security risk assessment**; failed to implement security measures sufficient to reduce risks and vulnerabilities; failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and disclosed protected health information (PHI) to third party vendors without a written business associate agreement
- FBI brought cyber hacking of their system to their attention

Entity-Wide Adherence Is Critical

- **February 2018**, Fresenius Medical Care North America (FMCNA) to pay $3.5 million to settle potential HIPAA violations
- FMCNA is a multi-state dialysis provider with over 60,000 employees that serves over 170,000 patients, operating dialysis facilities, outpatient cardiac and vascular labs, urgent care centers, with hospitalist and post-acute provider
- Five separate breaches across their system reflecting a failure to implement HIPAA properly, and unwillingness to prioritize HIPAA compliance
- Failed to conduct an accurate and thorough risk analysis

Paper Still Counts

- February 2018, Filefax, Northbrook Illinois, to pay $100,000 out of the receivership estate to settle potential HIPAA violations
- Filefax impermissibly disclosed the PHI of 2,150 individuals by leaving PHI in an unlocked truck with boxes of records in the Filefax parking lot, or by granting permission to an unauthorized person to remove the PHI from Filefax, and leaving the PHI unsecured outside the Filefax facility
- Out of business during OCR's investigation, but still required to pay the fine

Encryption of Portable Devices and Storage Media Is Critical

- **June 2018.** $4.3 million
- MD Anderson comprehensive cancer treatment and research center, at the Texas Medical Center, Houston, lost devices resulting in breach of over 33,500 individuals' data
- Three separate data breach reports in 2012 and 2013 involving theft of an unencrypted laptop from the residence of an employee, loss of two unencrypted USB thumb drives containing the unencrypted electronic protected health information
- MD Anderson had written encryption policies beginning in 2006, risk analyses had found that the lack of device-level encryption posed a high risk to the security of ePHI, but corrective measures were not taken
- Enterprise-wide solution for encryption began 2011, and failed to encrypt its inventory of electronic devices containing ePHI between March 24, 2011 and January 25, 2013

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

Subpoena Alone – Not Enough

Court Orders, Subpoenas, and Litigation Matters

Connecticut Subpoena Case

The case, *Byrne v. Avery*, involved records disclosed in response to a valid subpoena.

- Access full opinions at www.jud.ct.gov; Supreme Court opinion archived by date: January 16, 2018.

- Even though HIPAA expressly states it is not grounds for private right of action, Connecticut Supreme Court has opined that a common law privacy claim may be based on a breach of HIPAA Privacy.
- Three takeaways:
  - Expect more claims based on HIPAA Privacy or HIPAA Breach (although these were already happening)
  - HIPAA is now *de facto* "standard of care" for release of records
  - BE EXTREMELY CAREFUL when disclosing in response to a SUBPOENA

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

- 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

Connecticut Law On Information Blocking

To the fullest extent practicable, a hospital must use its EHR system to enable the secure two-way exchange of patient electronic health record with other licensed providers who (1) have a system that can exchange these records and (2) provide health care services to a patient whose records are being exchanged….Upon the request of a patient or the patient's health care provider, as long as:

- the transfer or receipt would be secure, not violate any state or federal law or regulation, and not constitute an identifiable and legitimate security or privacy risk, and
- for requests from a provider, the patient **consents to and has authorized** the exchange.

Under the act, if the hospital has reason to believe that such a record transfer would be illegal or present an identifiable and legitimate risk to security or privacy, it must promptly notify the requesting party.

See C.G.S. sections 19a-904c; 19a-904d

Federal Rules on Information Blocking: 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).

- **We await regulations to implement this. Government says to expect rules by [end of 2017…or January 2018…or summer 2018]…the end of 2018.**

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

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.

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)

More Sharing With Providers Will Be Required

- Information blocking rules transform many of the *permitted* types of sharing into "likely required" disclosures
- All providers will need to review their sharing process and policy steps and make adjustments to be sure they are not over-protecting records when a third party (including another provider) asks for access to the record
- When the request is patient-generated, you should already be facilitating sharing

Q & A