Healthcare Compliance 2020 Hot Topics

Featuring Kelly McLendon, RHIA, CHPS

And Sue Chamberlain, MSCTE, RHIA, CCS-P, CDIP

Harmony Healthcare
Exceptional People. Exceptional Results.

RRS MEDICAL
Secure PHI Transfer Technology and Solutions

CompliancePro SOLUTIONS

Speakers

Kelly McLendon

RHIA, CHPS

Compliance Pro Solutions
Managing Director

&

Sue Chamberlain

MSCTE, RHIA, CCS-P, CDIP

RRS Medical, VP of Compliance and Education

Compliance HOT Topics!

Harmony Healthcare
Exceptional People. Exceptional Results.

RRS MEDICAL
Secure PHI Transfer Technology and Solutions

CompliancePro SOLUTIONS

Our Educational Webinar Sponsors

Experts In;

Compliance

CompliancePro SOLUTIONS

CompliancePro Health provides automation of HIPAA privacy and security including incident and breach determination, HIPAA and general compliance workflows and content along with deep assessment capabilities.

PHI Transfer

RRS MEDICAL

RRS Medical is your source for Secure PHI Transfer technology and solutions. Every record we encounter is managed with your patient's healthcare journey in mind. Our Release of Information Solutions, Electronic Chart Indexing, Audit Response Service, and Patient Forms process and electronic requesting and delivery methodology are supported by innovation, process transparency, optimal compliance, and security standards

Human Capital Management

Harmony Healthcare provides value-driven health information management leadership interim and consulting solutions that assist with change management, initiate strategic directives, and drive overall departmental performance. As a human capital management organization, we provide non-clinical staffing and consulting solutions into a diverse range of healthcare organizations nationwide.

Thank You

Agenda

- Covid-19 and HIPAA
- 42 CFR Part 2 Changes Under the Cares Act
- Trends in Privacy and Security
- 21st Century Cures Act and Interoperability/Information Blocking
- Patient Access Rule Changes
- Enforcement

"After a while you learn that privacy is something you can sell, but you can't buy it back."

Bob Dylan, Chronicles, Volume One (2004)

Covid-19 OCR (and other) Guidance and Waivers

- OCR Resources: https://www.hhs.gov/civil-rights/for-providers/civil-rights-covid19/index.html
- HIPAA is *not suspended*
- When disaster protocols implemented HIPAA is relaxed for these areas only:
  - The requirements to obtain patient agreement to speak to family members involved in patient care (45 CFR 164.510(b))
  - Ability to opt out of a facility directory (164.510(a))
  - Mandatory NPP distribution (164.520)
  - Right to request restrictions on disclosures (164.522(a))
  - Right to request confidential communications (164.522(b)
- Telehealth technical security guidance
- Cyber Threat and Malware guidance, including VTC and Zoom hacking
- Restrictions on Media Disclosures
- 42 CFR Synchronization and minimization of consent requirement for substance abuse records
- Civil Rights during COVID, ventilator triaging and others

Covid-19 OCR (and other) Guidance and Waivers

- Enforcement discretion for Community based testing sites
- Business associate public health oversight enforcement discretion
- First responders and PHI receipt
- https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf

- If you believe that a person or organization covered by the Privacy and Security Rules (a "covered entity") violated your health information privacy rights or otherwise violated the Privacy or Security Rules, you may file a complaint with OCR. For additional information about how to file a complaint, visit OCR's web page on filing complaints at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

- DHS and HHS Civil Rights Stakeholder Teleconference on COVID-19 - FEMA's Office of Equal Rights (OER) will host another teleconference addressing the coronavirus disease 2019 (COVID-19)<https://www.cdc.gov/coronavirus/2019-nCoV/index.html

- HHS Initiatives to Address the Disparate Impact of COVID-19 on African Americans and Other Racial and Ethnic Minorities - HHS released a fact sheet on initiatives underway to address the disparate impact of COVID-19 on African Americans and other racial and ethnic minorities. To learn more about how these initiatives address President Trump's commitment to improve prevention, testing and treatment of COVID-19 in underserved communities, please click on the following link HHS Fact Sheet - PDF<https://www.hhs.gov/sites/default/files/hhs-fact-sheet-addressing-disparities-in-covid-19-impact-on-minorities.pdf>.

Covid-19 OCR Global Regulatory Activities

- 60+ US and global data protection agencies, both governmental and not have issued guidance during and about the Covid-19 pandemic

- Areas addressed include:
  - Health Data Collection and Management
  - Covid-19 Diagnosing
  - Covid-19 Record/Data Disclosure
  - Work-at-Home Practices
  - Return-to-Work Practices
- Some countries strike a more restrictive stance than others, *generally* here is a list of Do's and Don'ts
- Data Collection and Prevention Don'ts
  - Don't record taken temperatures
  - Conduct workforce surveys of family member health
  - Request and obtain information about social interactions outside work

- Abstracted from Fenwick & West article May 14, 2020 – Global Regulatory Guidance for Covid-19 Privacy and Security Issues

Covid-19 OCR Global Regulatory Activities

Do…Take non-recorded temperatures recoding only when people are sent home to quarantine

- Conduct surveys asking if workforce members are having symptoms
- Require home quarantine for workforce members who have suspected contacts with infected/symptomatic person(s)
- Require a Drs note to return to work if quarantined
- Use cell phone tracking to tack locations and confirm home quarantine, be careful of laws requiring consent

Disclosure of Names of Individuals with Confirmed or Suspected cases…Don'ts

- Discloser names of co-workers or other company personnel, but it's ok to list location(s) and who has to be careful with monitoring their health because of potential contact
- Executives and Direct Supervisors, to the extent possible and only on a need to know basis

Do…Disclosures made only in 3 limited circumstances

- To health and safety governmental agencies without consent of the individuals in cases of confirmed Covid-19
- To healthcare providers with consent of the individual to aid treatment – this may be superseded by HIPAA TPO
- To family members with consent of individual to help the family protect themselves and/or aid in treatment

- Abstracted from Fenwick & West article May 14, 2020 – Global Regulatory Guidance for Covid-19 Privacy and Security Issues

Covid-19 OCR Global Regulatory Activities

- Returning to the Workplace follow CDC, EEOC and other data protection authorities regulations and best practices
  - Testing…Do's Measure workforce wellness through temperature readings
  - Obtain consent to test
  - Minimize invasiveness
  - Appoint a designated tester
  - Designate a testing site to preserve privacy and maintain distancing
  - Limit record keeping to only suspected or confirmed cases
  - Store records separately from personnel records and treat as confidential employee health records
  - If records are kept of non-employees they are not employee health records, but should be kept confidentially
- Office Strategy…Do's
  - Stagger employee returns
  - Maintain social distancing (no cubicles next to each other, handshakes)
  - Continue heightened cleaning
  - Require infection control (tissues, no touch disposal, PPE
  - Provide necessary supplies
  - Posters encouraging good hygiene
  - Abstracted from Fenwick & West article May 14, 2020 – Global Regulatory Guidance for Covid-19 Privacy and Security Issues

HARMONY HEALTHCARE
Exceptional People. Exceptional Results.

RRS MEDICAL
Secure PHI Transfer Technology and Solutions

CompliancePro SOLUTIONS

Covid-19 OCR Global Regulatory Activities

- Contract Tracing…**Do's**
  - Use technology for contact tracing
  - Encourage participation, require if lawful
  - Collect the minimum amount of data to perform the tracing
  - Enforce tight access controls to the data limit to small groups or health authorities

- Disaster Recovery Resumption…**Do's**
  - Approach the same way as disaster recovery
  - Define the companies 'new normal' and educate the workforce
  - Identify and undo adjustments made during pandemic's crisis time

- Remote Working – **Do** encourage, especially for high risk groups

Abstracted from Fenwick & West article May 14, 2020 – Global Regulatory Guidance for Covid-19 Privacy and Security Issues

Coming Privacy Liabilities Following Covid-19

- Immunity for businesses for Covid related liabilities???
- Liability and lawsuits for businesses (others?) related to Covid claims of being made sick, unsafe employment conditions, etc.
- Class action lawsuits for privacy and security practices
  - Zoom caused lawsuits under various Federal and California laws, including CCPA
- Attorney Generals
  - Regulators declined to push CCPA back due to Covid-19, therefore expect regulators to continue to implement and enforce
- Covid-19 has increased technologies dependence and visibility, expect more regulations for privacy an security
- Be aware of all possibly impactful regulations that can be grounds for lawsuits or at least contrite even if no private right of action (e.g. HIPAA)
  - Children's Online Privacy Protection Act (COPPA)
  - Family Education Rights and Privacy Act (FERPA) – student records
  - HIPAA
  - Gramm, Leach, Bliley (GLBA)
  - State employment record and documentation rules

Important OCR Guidance:
Emergency Preparedness and Emergency Situations

- Hurricane Harvey – These announcements continued to evolve or the course of the storms
  https://www.hhs.gov/sites/default/files/hurricane-harvey-hipaa- bulletin.pdf

- Family and Friends
  https://www.hhs.gov/sites/default/files/provider_ffg.pdf

- For more detailed information regarding HIPAA privacy and disclosures in emergency situations
  https://www.hhs.gov/sites/default/files/hurricane-harvey-hipaa-bulletin.pdf

- For more detailed information regarding emergency situation preparedness, planning, and response
  https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html

- To utilize the Disclosures for Emergency Preparedness Decision Tool https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/decision-tool-overview/index.html

- Please view the Civil Rights Emergency Preparedness page to learn how nondiscrimination laws apply during an emergency
  https://www.hhs.gov/ocr/civilrights/resources/specialtopics/emergencypre/index.html

HHS/OCR Guidance Related Ransomware

- OCR Guidance issued December 19, 2019:
- Fall 2019 OCR Cybersecurity Newsletter
  - What Happened to My Data? Update on Preventing, Mitigating and Responding to Ransomware
- More in-depth ransomware guidance, identifies strategies for prevention, mitigation and recovery *(the usual suspects)*:
  - Risk Analysis 164.308(a)(1)(ii)(B)
  - Information System Activity Review 164.308(a)(1)(ii)(D)
  - Security Awareness and Training 164.308(a)(5)
  - Security Incident Procedures 164.308(a)(6)
  - Contingency Plan (164.308(a)(7)

42 CFR Part 2 - Confidentiality of Substance Use Disorder Patient Records

Final Rule – Implemented with Little Fanfare - February 2017 –
BUT *More and Different Rules* are in effect with Cares Act Section 3221
Another Final Rule issued July 15, 2020, implements August 14, 2020

Not updated since 1987. The rule states that SAMHSA is maintaining their content substantively unchanged from the 1987 final rule, except for a few areas such as:

- Modernizes rule to address both paper and electronic records
- Some definitions changed, including 'disclosure' and 'minor'
- What constitutes a Part 2 'program' changed, including 'general medical facility' that provides substance abuse treatment – Be aware if you have Substance Abuse Records, Treatment or even Diagnosis 42 CFR Part 2 applies
- Patient records subject to the part 2 regulations include substance use disorder records maintained by part 2 programs, as well as those records in the possession of 'other lawful holders of patient identifying information"
- Changed…(§ 2.32), SAMHSA clarifies that the prohibition on re-disclosure only applies to information that would identify, directly or indirectly, an individual as having been diagnosed, treated, or referred for treatment for a substance use disorder, such as indicated through standard medical codes

Harmony Healthcare
Exceptional People. Exceptional Results.

RRS MEDICAL
Secure PHI Transfer Technology and Solutions

CompliancePro SOLUTIONS

Cares Act 42 CFR – HIPAA Synchronization

- In 2018 there was a Final Rule published for CFR 42 Part 2…**BUT** much has changed and more will change under the Cares Act (Covid-19 Stimulus) Section 3221 Protecting Jessica Grubb's Legacy Act
- Major changes announced for the crisis, but to be augmented and implemented by HHS within a year from March – amendments made by section 3221 shall apply with respect to uses and disclosures occurring on or after March 27, 2021
- Finally HIPAA and SAMHSA are being synchronized
- Key Points
  - Consent only an affirmative, initial consent is necessary for CE, BA or program subject to 42 CFR part 2 for purposes of TPO as permitted by HIPAA – Consent can be revoked at any time
  - Redisclosure is no longer prohibited, defer to HIPAA rules if the initial affirmative consent has been obtained
  - Public Health disclosures – ok if requirements for de-identification under HIPAA are met
  - Notice of Privacy Practices (NPP) –Requires no later than 1 year from Cares Act Implementation (March 27, 2021) provide a notice NPP in plain language that includes statement of patient's rights and how the individual must exercise and description of permitted uses and disclosures without patient authorization
  - Basically bringing 42 CFR programs up to HIPAA standards for NPP
  - Breach per HIPAA

Trends in Privacy & Security for 2020

- Privacy across the board is becoming more important, but with the exception of HIPAA, privacy laws are progressing and evolving
- Criminal cybersecurity activities, including ransomware and other types of hacking continue to be a huge problem, but cyber security infrastructure is being evaluated more closely in many entities – including state bad actors e.g. Russia and China
- EHR dominance over paper records continues in the US, paper continues to decline in usage, but is nowhere near dead
- Paper records with PHI (and fax, copies that cause breaches) still account for many violations
- CEs continue to tighten getting satisfactory assurances of their business associates have privacy & security compliance programs
- But most BA's are not asked about their compliance from many of their vendors

Increasingly Confusing Mix of Privacy Rules

Questions being asked include, besides HIPAA, how, where and when do these other rules apply in any healthcare related organization?

- Employee Health Records and Covid-19
- 42 CFR part 2 Substance Abuse
- FERPA – Student Records (including medical records)
- CCPA (California Consumer Privacy Act)
- GDPR (EU's General Data Protection Rule)
- Washington and Nevada State Privacy, many others coming
- National Privacy Law? Not yet…

The Rise of Privacy – New Major Privacy Laws

GDPR – General Data Protection Rule – EU privacy law, very onerous fines, but it'll be long in implementing and complex

- Not well known who in US healthcare is impacted, but certainly medical tourism from the EU patients may be
- Since healthcare entities have other non-HIPAA data that is personally identifiable there may be other areas to address under this new rule
- Not many experts on this yet

CCPA – California Consumer Protection Act - Not well formed as they created it within a short deadline

- CCPA may say HIPAA entities are exempt, but figuring out how far that extends is dicey, what exactly is exempt, all data within an entity or just the PHI?
- Implementation expected in 2020, will undergo more, maybe extensive changes
- Expected to be the model privacy law for all other states

Both rules: Covers areas such as opt out and allowing consumer access to the information managed by an organization, e.g. managing if the data can be sold or used beyond it's initial uses

US State Privacy Law Rise and Fast Too!

- Per and article (cited later); '*The 2019 Privacy Legislation Bomb Cyclone*' by Maurice Wutscher LLP
- "The privacy concepts of the GDPR and CCPA include the requirement of consent, the right to access, correct and delete personal information, transparency through privacy policies, and data security and minimization
- These concepts struck a chord with many, and a number of US States introduced, but did not enact as of this date, legislation similar to or having elements in common with the CCPA. Those states include Hawaii, Massachusetts, New York, Pennsylvania, Rhode Island, Texas and Washington
- The outcome of consumer data privacy legislation (approximately 149 bills introduced and 14 enacted) and data breach notification legislation (approximately 80 bills introduced and 17 enacted) in 2019.
- Importantly, some of the legislation "not enacted" will carry over to 2020, and several state legislatures are still in session.

The Rise of Privacy

- Gartner said it believes that privacy concerns will “drive at least 10% of market demand” for security services through 2019 and impact a variety of segments, such as
  - Identity and Access management (IAM)
  - Identity Governance and Administration (IGA)
  - and Data Loss Prevention (DLP)

- If Worldwide spending on information security products and services will reach over $114 billion in 2018;
  - Then privacy driven components will account for $11.4 B and not including non-information security budget spending

Harmony Healthcare
Exceptional People. Exceptional Results.

RRS MEDICAL
Secure PHI Transfer Technology and Solutions

CompliancePro SOLUTIONS

NIST Privacy Framework

- A framework is a model of standards, best practices and likewise encouraged, if not outright mandated, behaviors to safeguard privacy and security of personal information. Typically contained within a spreadsheet or table-oriented document with text comments
- Assessment templates can be built from such frameworks so that they can be operationalized
- NIST has released a privacy framework (to go with, but be separate from, it's security framework)
- Integrating the existing NIST cybersecurity framework with the privacy framework
- Urged to stress 'competitive advantage' for businesses using privacy framework
- Seeking input on 'value' of privacy framework
- Stress intersection of privacy and security, despite plan for separate framework cores
- Separate privacy 'core' functions from cybersecurity framework
- Stresses 'breadth' of privacy framework as distinct from cybersecurity efforts

State Privacy (and Security) Law To Watch

- NY Privacy Act - Bolder than CCPA prohibit personal data from being, used, processed or transferred to a third party without opt-in consent
- New Jersey - Failed last year but up again
- Florida – Consumer can opt-out of same of covered information by request submitted to a designed request address, but contains no other rights
- Washington Privacy Act - Almost passed last year - other supporting bills like biometrics, facial recognition IoT, AI and bots are separate. Differs from CCPA, focus on an organization's use of data, not just people that reach out to them
- New Hampshire - CCPA copycat
- Virginia – elements of both CCPA and GDPR but different too
- Nebraska – CCPA like Zith 'consumer rights'
- Illinois – CCPA like
- Arizona – Not pushing for a law, call for a national law – *let's see how long that lasts* – CT, Texas, Hawaii and North Dakoda are studying privacy laws
- Vermont, Minnesota, Maryland, Rhode Island and Oregon have bills

New State Laws - NY SHEILD Act – Security Law – Good State Security Law Example

- NY SHIELD Act Gen Bus Law §899-bb- Effective March 21, 2020 – Exception for businesses fewer than 50 employees and less than $3M in gross revenues for last 3 years or $5M of year end assets
- Affects the entire NYC metro area, even CT and NJ
- Requires businesses that collect private information on NY residents to implement reasonable cybersecurity safeguards
- Similar to other states security requirements, including having a written information security plan (WISP)
- Designation of security official and staff to coordinate the security program
- Identify potential insider threats, assess existing safeguards, perform workforce security training
- Use service providers that also maintain compliance and require them to by contract
- Network risk assessments, info processing, transmission and storage
- Measures implemented to detect, prevent and respond to system failures, regular testing and monitoring of controls
- Physical safeguards to prevent unauthorized access, including disposal

New State Laws - NY SHEILD Act – Security Law - – Good State Security Law Example

- Entities required to comply and in full compliance with the following cybersecurity regimes are *automatically "deemed to be in compliance"* with the SHIELD Act's "reasonableness" standard:
- The federal Gramm-Leach-Bliley Act ("GLBA");
- The federal healthcare standards ("HIPAA/HITECH");
- The NYDFS Cybersecurity Regulation; or
- "Any other data security rules and regulations" promulgated by the federal or New York State government
- Special rules apply to "small business" with fewer than 50 employees, less than $3 million in annual revenue for the preceding three years, or less than $5 million in assets
- *Their security programs are deemed compliant if they are appropriate for the size and complexity of the business, but is still subject to the reasonable security requirement*
- *What is reasonable under the circumstances is informed in part by the sensitivity of the Private Information the small business collects from or about consumers*
- Up to $5000 per violation, even if there is no breach

Information Blocking

- Cerner vows to open EHR to third-party development
- Epic is kicking and screaming to resist the Cures Act APIs and opening of access, but I imagine that'll be futile
- Milbank Quarterly March 2017 Study Information Blocking:
- Occurs "frequently" among EHR vendors
  - 30 of 60 HIE leaders said vendors "routinely" engage in info blocking
  - Most common cause purposefully deploying products with limited interoperability
- Hospitals and health systems
  - 22% (of 60) said hospitals and health systems routinely control patient flow by selectively sharing patient info – although as HIM we are opposed to this apparently examples exist of common information blocking by thee facilities

ONC's 21st Century Cures Act Interoperability and Information Blocking Rules

- Based on Cures Act and the President's Executive Order (EO) 13813 on October 12, 2017, to promote health care choice and competition across the United States
- Section 1(c) of the EO, in relevant part, states that government rules affecting the United States health care system should re-inject competition into the health care markets by lowering barriers to entry and preventing abuses of market power
- Also states that government rules should improve access to and the quality of information that Americans need to make informed health care decisions
- For example, establishing Application Programming Interfaces (APIs) for several interoperability purposes, including patient access to their health information without special effort
- For API's the Health Level Seven's - Fast Healthcare Interoperability Resources (FHIR®) standards are important
- HIT certification criteria has to be updated to include API's, replacing certain former MU criteria
- Provides ONC's interpretation of the information blocking by identifying reasonable and necessary activities that would not constitute information blocking

ONC's 21st Century Cures Act Interoperability and Information Blocking Rules

- Adoption of the United States Core Data for Interoperability (USCDI) as a Standard
  - Proposes replacing the "Common Clinical Data Set" (CCDS) with USCDI as a standard, naming USCDI Version 1 (USCDI v1) in § 170.213 and incorporating it by reference in § 170.299
  - The USCDI standard, if adopted, would establish a set of data classes and constituent data elements that would be required to be exchanged in support of interoperability nationwide – much wider scope than CCDS
- Electronic Health Information Export
  - Intended to provide patients and health IT users, including providers, a means to efficiently export the entire electronic health record for a single patient or all patients in a computable, electronic format
  - This criterion would: (1) enable the export of ***EHI*** for a single patient upon a valid request from that patient or a user on the patient's behalf, and
  - (2) support the export of EHI when a health care provider chooses to transition or migrate information to another health IT system
  - This criterion would also require that the export include the data format, made publicly available, to facilitate the receiving health IT system's interpretation and use of the EHI

ONC's 21st Century Cures Act Interoperability and Information Blocking

Information Blocking

- The Cures Act requires that a health IT developer, as a Condition and Maintenance of Certification under the Program, not take any action that constitutes information blocking as defined in section 3022(a) of the Public Health Service Act (PHSA)
- Defines conduct by health care providers, and health IT developers of certified health IT, exchanges, and networks that constitutes information blocking
- Information blocking is defined in broad terms with *seven exceptions*
- First, limited to certain activities that clearly advance the aims of the information blocking provision; promoting public confidence in health IT infrastructure by supporting the privacy and security of EHI, and protecting patient safety
- Second, each exception is intended to address a significant risk that *regulated individuals and entities* (i.e., health care providers, health IT developers of certified health IT, health information networks, and health information exchanges) *will not engage in these reasonable and necessary activities because of potential uncertainty* regarding whether they would be considered information blocking
- Third, and last, each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt

ONC's 21st Century Cures Act Interoperability and Information Blocking

Information Blocking - *The Cures Act expands a scope of protections beyond HIPAA's boundaries, but notably HIPAA, other Federal law and State law still cannot be violated, so they still apply unless superseded by a stronger Cures Act rule or reg*

- 1. Preventing Harm
- 2. Promoting the Privacy of EHI - Extensive language designed to keep existing privacy protections in place and yet to be flexible and allow as much data exchange as can be established
- 3. Promoting the Security of EHI – Security, especially, not exclusively through the HIPAA security rule is encouraged
- 4. Recovering Costs Reasonably Incurred – *Oh boy another fee model…*
- 5. Responding to Requests that are Infeasible
- 6. Licensing of Interoperability Elements on Reasonable and Non-discriminatory Terms
- 7. Maintaining and Improving Health IT Performance

Harmony Healthcare
Exceptional People. Exceptional Results.

RRS MEDICAL
Secure PHI Transfer Technology and Solutions

CompliancePro SOLUTIONS

DOJ 10 General Compliance Guidelines – Great Guidance!

1. Compliance MUST be Properly Resourced
2. Compliance MUST have Independent Access to the Board of Directors or Audit Committee
3. Compliance MUST be Integrated with Other Functions
4. Compliance MUST Adopt a Risk-Based Approach
5. Compliance MUST Implement Metrics that Matter
6. Your Gatekeepers and Managers MUST be Trained Differently
7. Compliance MUST Adopt Stringent Third-Party Controls AND Continuous Monitoring of those Third-Parties
8. Compliance MUST Communicate its Policies and Procedures to Third-Parties
9. Companies MUST have a Robust Whistle-Blowing Process
10. Compliance MUST have Compliance Program Evaluations Performed

Acceptable Uses of PHI by Amazon, Google, etc

- Recently a partnership between Google and Ascension raised eyebrows and questions quickly arose about inappropriate access to Ascension's PHI (Mayo has a relationship too)
- The question is; if Ascension moves their server and infrastructure into the Google Cloud hosting is there a risk to the PHI from Google having some type of inappropriate access to the PHI as a result of them providing hosting infrastructure?
- Not if Ascension is only moving their servers and platform functionality to Google HW. This can be accomplished through the use of a Business Associate Agreement rendering Google a Business Associate
- They will then have the same obligations not to access or use data for which they have not been specifically authorized under the HIPAA rules

Patient Access Guidance Changes

- Warning, this decision is already under attack from trail lawyers that are trying to use a line in the Cares act to get reduced record copies – our opinion is that it's a mis-interpretation of the Cares Act, trying to get language in place in this next stimulus bill to fix
- Per OCR Listserve on January 29, 2020 an Opinion Memorandum was handed down from Federal Court in the CIOX lawsuit, effectively changing the guidance *in practice* about having to provide copies to third parties as directed by the patient to only the HIPAA published fee cost
- Basically OCR had exceeded their authority when they changed the privacy rule in several ways over the years, but especially with guidance issued in 2016 that allowed patient's under their 'Right of Access' to direct Covered Entities (or their BAs performing that task e.g. ROI companies) to allow patient's to direct to 3rd parties copies of their records and change them the so called HIPAA "Patient Fee'
- This caused attorneys and insurance companies, among others, to abuse the process by claiming HIPAA fees and copy rules should apply to their requests by posing as the patient in their request, all to save a few bucks
- This led to hundreds or thousands (who knows) complaints to OCR, wasting their time and resources and causing much grief and worry to CEs and their BAs
- This court opinion stops that behavior and OCR has clarified they will no longer enforce the 3rd party patient directive complaints

Patient Access Guidance Changes

- If your organization processes patient requests for information (copies) be aware that the new ruling makes it easier to define exactly which requests are charged the HIPAA based “Patient Fee’ vs the state mandated record charges that apply to 3rd party disclosures
- Although patient’s can direct copies of their PHI be sent to third parties as a part of their access rights, the fees that be changed is now increased to whatever the state law allows
- A signed, full authorization to disclosure form for patient directed PHI disclosures to 3rd parties is probably not required for patients to make these requests, but they should be honored
- No mention of having to use a stripped-down authorization form for patient directed requests, but it is assumed that these will still be applicable to patient directed requests only
- If a lawyer is making this kind of request, claiming the patient is requesting their copies be sent to the attorney charge them the full state record copy charges and ensure they get a signed authorization from the patient
- If dealing with the patient directly and they are directing the PHI be disclosed, you may charge whichever fee you wish (the HIPAA Patient Fee or State Record Copy Fee or none.
- Be aware that many attorneys abused the guidance issued in 2016 by OCR and *do not be bullied by them in the future!*

HIPAA Enforcement

- Unsecure how Covid-19 has impacted OCR's enforcement of HIPAA other than waivers, probably slowed the pace of investigations, fines, etc down
- So far no new fines have been issued that Kelly has seen
- OCR has been active in civil rights as well as HIPAA, it's a different division, but this could also be keeping OCR busy
- 1st and 2nd fines for Patient Access / Info Blocking - HHS fined its first hospital under an initiative to combat information blocking, charging that a Florida hospital took too long to fulfill a patient's record request
- CE must pay HHS' Office of Civil Rights (OCR) $85,000 for failing to give a mother timely access to records about her unborn child, the agency said Monday. And adopted a Corrective Action Plan (CAP)
- The fine is the first enforcement action taken under the Right of Access Initiative launched earlier this year to combat information blocking at healthcare facilities
- See next slides for details about the (2nd) Second Case…

HIPAA Enforcement

- OCR Settles (2nd) Second Case in HIPAA Right of Access Initiative - December 12, 2019 - From patient complaint in March 2019
- A CE in Florida has agreed to take corrective actions and pay $85,000 to settle a potential violation of HIPAA's right of access provision plus a one year CAP
- Despite repeatedly being asked, the CE failed to forward a patient's medical records in electronic format to a third party
- Not only did the CE fail to timely provide the records to the third party;
- …but they also failed to provide them in the requested electronic format;
- …and charged more than the reasonably cost-based fees allowed under HIPAA. OCR provided the CE with technical assistance on how to correct these matters and closed the complaint
- But wait…there's more…

HIPAA Enforcement

- Despite OCR's assistance, the CE continued to fail to provide the requested records, resulting in another complaint to OCR
- As a result of OCR's second intervention, the requested records were provided for free in May 2019, and in the format requested
- "For too long, healthcare providers have slow-walked their duty to provide patients their medical records out of a sleepy bureaucratic inertia. We hope our shift to the imposition of corrective actions and settlements under our Right of Access Initiative will finally wake up healthcare providers to their obligations under the law," said Roger Severino, OCR Director
- Don’t be a sleepy bureaucrat, no slow walking requests for copies from patients!

HIPAA Enforcement 

Ambulance Company Pays $65,000 to Settle Allegations of Longstanding HIPAA Noncompliance

- OCR's investigation uncovered long-standing noncompliance with the HIPAA Rules, including failures to conduct a risk analysis, provide a security awareness and training program, and implement HIPAA Security Rule policies and procedures
- Despite OCR's investigation and technical assistance, the CE did not take meaningful steps to address their systemic failures

OCR Imposes a $2.15 Million Civil Money Penalty against a Hospital for HIPAA Violations - October 23, 2019 - Note: This is an example of no settlement, agreement to pay full fine and to not have a CAP

- OCR's investigation revealed that CE failed to provide timely and accurate breach notification to the Secretary of HHS, conduct enterprise-wide risk analyses, manage identified risks to a reasonable and appropriate level, regularly review information system activity records, and restrict authorization of its workforce members' access to patient ePHI to the minimum necessary to accomplish their job duties

HIPAA Enforcement

- 11/27/19 – (breach in April 2017) - OCR Secures $2.175 Million HIPAA Settlement after Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information plus a 2-year Corrective Action Plan (CAP)
  - **Note:** This CE refused to change their position *after* being advised by OCR they were incorrect

- HHS OCR) received a complaint alleging that a CE hospital had sent a bill to an individual containing another patient's PHI
  - OCR's investigation determined that this CE mailed 577 patients' PHI to wrong addresses that included patient names, account numbers, and dates of services
  - The CE reported this incident as a breach affecting 8 individuals, because CE concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred

- The CE persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR

- OCR also determined that the CE failed to have a business associate agreement in place with an entity that performed business associate services for the CE

Conclusion

- The future of privacy and security regulation seemingly tightening up, in response to a wild marketplace and a law and order administration
- As for regulatory compliance, keep doing what you are doing for privacy and security and assume nothing changes, then watch for updates from regulators and the press
- Maintain vigilance for newly arising security threats and vulnerabilities, respond and document your response in real time
- Patient Access request issues continue to evolve and is a very important topic to understand completely and apply correctly
- Stay tuned: For more 'Hot Topics' and other Advanced HIPAA Training webinars and programs

Questions?

Harmony Healthcare
Exceptional People. Exceptional Results.

RRS MEDICAL
Secure PHI Transfer Technology and Solutions

CompliancePro SOLUTIONS