THE EVER-EVOLVING LANDSCAPE OF PRIVACY AND SECURITY COMPLIANCE

2021 Managed Care Compliance Conference
February 1, 2021

Jonathan Friesen, JD, Chief Privacy Officer, Geisinger Health
Adam Greene, JD, MPH, Partner, Davis Wright Tremaine LLP

1

AGENDA

- Changes to Health Information Privacy Laws
- Interoperability
- Top Enforcement Areas
- Third Party Risk Assessment
- COVID-19 Impact

2

CHANGES TO HEALTH INFORMATION PRIVACY LAWS

3

HIPAA Proposed Rule – Right of Access

- Shorter time period for right of access (30+30 days → 15+15 days)
- Conform right of access to *Ciox Health decision*
  - Right to have PHI sent to third party limited to e-copy of EHR (therefore, limited to health care providers)
  - Clarifies fee for third-party directives (*Ciox* court indicated notice and comment required to extent fee limit to third-party directives)
- Clarification of right to inspect (e.g., right to take photographs, etc.)
- Fees for access must be posted on covered entity website
- Right of access includes through personal health application without fee

4

HIPAA Proposed Rule - Other

- Care coordination
  - Disclosures to social services agency, community-based organization, home and community based services provider, or similar health and human services organizations
- New content requirements for notice of privacy practices
- "Serious and imminent harm" → "serious and reasonably foreseeable harm"
- Changes "professional judgment" standard to "good faith"
  - Disclosing to parent who is not personal representative
  - Disclosing to persons involved in care or payment when individual is not present
  - Verification of identity

5

42 C.F.R. Part 2

- Governs confidentiality of substance use disorder ("SUD") records from certain "programs"
- 2017 – included changes to consent to promote health information exchange (but requiring naming of specific individuals) and allows shorter redisclosure notice
- 2018 – included changes to permit "lawful holders" (e.g., health plan) to disclose to contractors if appropriate contractual language is in place
- 2020
  - Greater ability for non-part 2 providers to integrate SUD information into records
  - Revised consent requirements to no longer require naming of specific individual recipient
  - Add care coordination and case management to disclosures that lawful holder can make to a contractor

6

42 C.F.R. Part 2

- CARES Act 3221
  - Patient can consent to all future uses of part 2 records for treatment, payment, and health care operations
  - Once disclosed for treatment, payment, or health care operations, HIPAA covered entity or business associate can treat the information like other protected health information
  - Applies HIPAA penalties to 42 C.F.R. part 2
  - Applies HIPAA Breach Notification Rule to confidentiality breaches of 42 C.F.R. part 2
  - Awaiting regulations

7

California Consumer Privacy Act ("CCPA")

- 2018
  - CCPA excludes PHI of covered entities and medical information of health care providers; a health care provider is exempt "to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section"
  - Amendment adds exemption for PHI of business associates
  - Governed HIPAA de-identified information that did not meet CCPA definition of "deidentified"
  - Does not apply to non-profits, except that those share branding with a qualifying for-profit

8

California Consumer Privacy Act ("CCPA")

- 2020
  - Added exemption for business associate "to the extent that the business associate maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1)."

9

California Consumer Privacy Act ("CCPA")

- 2020
  - Exempts HIPAA de-identified information except:
    - Website notice requirement for sale or disclosure of HIPAA de-identified information, which must identify whether "HIPAA Expert Determination" method or "HIPAA Safe Harbor" method of de-identification is used.
    - Requires contracts involving sale or licensing of HIPAA de-identified information, if a party is doing business in CA, to include:
      1. A statement that the deidentified information being sold or licensed includes deidentified patient information.
      2. A statement that reidentification, and attempted reidentification, of the deidentified information by the purchaser or licensee of the information is prohibited pursuant to this section.
      3. A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

10

21ST CENTURY CURES ACT: INTEROPERABILITY AND INFORMATION BLOCKING

"Lack of seamless data exchange in healthcare has historically detracted from patient care, leading to poor health outcomes, and higher costs. The CMS Interoperability and Patient Access final rule establishes policies that break down barriers in the nation's health system to enable better patient access to their health information, improve interoperability and unleash innovation, while reducing burden on payers and providers. Patients and their healthcare providers will have the opportunity to be more informed, which can lead to better care and improved patient outcomes, while at the same time reducing burden. In a future where data flows freely and securely between payers, providers, and patients, we can achieve truly coordinated care, improved health outcomes, and reduced costs."

– CMS Fact Sheet

11

BASIC REQUIREMENTS (CMS RULES)

The CMS (and ONC) Rules realize the promise to expand access and portability of health information that began with HIPAA

- **Patient Access API** (applicable January 1, 2021; enforced after July 1, 2021)
- **Provider Directory API** (applicable January 1, 2021; enforced after July 1, 2021)
- **Payer-to-Payer Data Exchange** (applicable January 1, 2022)
- **Improving the Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges** (applicable April 1, 2022)
- **Public Reporting and Information Blocking** (targeted for late 2020/early 2021)
- **Digital Contact Information** (targeted for end of the first quarter of 2021)
- **Admission, Discharge, and Transfer Event Notifications** (applicable April 30, 2021)

12

UNDERSTANDING CMS AND ONC RULES

- CMS Rules govern Payers, explicitly
  - However, some Payers may be liable under the ONC Rules
  - Organizations need to assess whether pieces of their businesses might be considered "Actors" under the ONC Rules
- What is an API?
  - Application Programming Interface: Defines interactions between different software intermediaries
  - (Simply put, it creates a common language that allows different systems to talk to each other)
- What is an "Actor" under the ONC?
  - Providers
  - Health Information Exchanges and Health Information Networks
  - Developers of Certified Health IT

13

CMS RULES: API REQUIREMENTS

Patient Access API*:** CMS-regulated payers, specifically MA organizations, Medicaid Fee-for-Service (FFS) programs, Medicaid managed care plans, CHIP FFS programs, CHIP managed care entities, and QHP issuers on the FFEs,…are required to implement and maintain a secure, standards-based (HL7 FHIR Release 4.0.1) API ***that allows patients to easily access their claims and encounter information, including cost, as well as a defined sub-set of their clinical information through third-party applications of their choice. (Patient Access API must meet the technical standards finalized in the ONC Final Regulation, which currently includes HL7® FHIR® Release 4.) **01/01/2021 and 07/01/2021**

Provider Directory API: CMS-regulated payers noted above (except QHP issuers on the FFEs) are required by this rule to make provider directory information publicly available via a standards-based API. Making this information broadly available in this way will encourage innovation by allowing third-party application developers to access information so they can create services that help patients find providers for care and treatment, as well as help clinicians find other providers for care coordination, in the most user-friendly and intuitive ways possible. Making this information more widely accessible is also a driver for improving the quality, accuracy, and timeliness of this information. **01/01/2021 and 07/01/2021**

***Payer-to-Payer Data Exchange*:** CMS-regulated payers are required to exchange certain patient clinical data (specifically the U.S. Core Data for Interoperability (USCDI) version 1 data set) at the patient's request, allowing the patient to take their information with them as they move from payer to payer over time to help create a cumulative health record with their current payer. Having a patient's health information in one place will facilitate informed decision-making, efficient care, and ultimately can lead to better health outcomes. **01/01/2022**

Source: CMS.gov, Interoperability and Patient Access Fact Sheet (edited)

14

BUILDING A COMPLIANCE PROGRAM TO ADDRESS THE CMS AND ONC RULES

- Begin with the **7 Elements** of an Effective Compliance Program
- Perform an inventory of your business and understand whether the Rules apply to you and if so, which components are subject to the Rules
- Implement Policies and Procedures
- Develop and Implement Training
- Document decisions and efforts
- Steering Committees and Project Management
- Consult with experts

15

TOP ENFORCEMENT AREAS

16

OCR Enforcement - General

- As of January 12, 2021
  - OCR has brought 94 financial enforcement actions
    - Range of $3,500 to $16 million
    - Average of $1.4 million
  - OCR is bringing million dollar settlements for large providers and plans that experience significant breaches due to a perceived lack of safeguards.
  - Failure to perform an accurate and thorough risk analysis continues to be high risk.
  - Vast majority of OCR cases continue to be resolved through technical assistance or case closure after corrective action.

17

OCR Enforcement - Right of Access

- OCR has brought 14 financial enforcement actions related to the right of access since September 2019
  - Range of $3,500 to $160,000
  - Average of $65,000
- Complaints about lack of access to PHI are very high risk and may be fast-tracked.

18

State AGs – HIPAA Enforcement

- State Attorneys General HIPAA actions are pretty sporadic, with only one settlement in 2020 and three in 2019.
- Recent cases have involved multi-state settlements, including a $39 million settlement with Anthem involving 43 states and a $10 million settlement with Premera Blue Cross involving 30 states.
- Traditionally, the most active state attorneys general under HIPAA have been Massachusetts, New York, and New Jersey.

19

THIRD PARTY RISK ASSESSMENT

20

SOC 2: BASICS

SOC 2 was developed by the American Institute of CPAs (AICPA)

A SOC 2 audit reviews an organization's management of customer data based on five "trust service principles"

1) Security: Is the system protected against unauthorized access (i.e., HIPAA Safeguards)?

2) Availability: Is the system available for operation and use as reflected in policies and the agreement(s)?

3) Processing Integrity: Are the services provided in a complete, accurate, and timely, manner?

(Remember: Your third-party vendor is responsible for its own integrity and is not responsible for the quality of the data it is provided unless you are contracting for it to fix your data explicitly)

- **4) Confidentiality:** Is the information designated as confidential protected pursuant to policies and your agreement?
- **5) Privacy:** Is personal information collected, used, retained, disclosed, and destroyed in accordance with the third-party's privacy notice, policies, and the agreement?

21

SOC 2: BASICS

Type I: Describes systems and system design, and determines whether the design can meet the relevant trust principles

Type II: Assesses and details the operational effectiveness of the systems

Assess the SCOPE of the SOC 2

Like with any audit, to assess it, the reviewer must understand the scope to determine whether and to what degree it should be relied upon

SOC 2 Audits are useful, but are also only undertaken if a customer asks an auditor to assess

- Thus, the customer defines the scope so approach with caution

22

SOC 2 AND THIRD-PARTY RISK ASSESSMENT

SOC 2 ≠ HIPAA Compliance

- SOC 2 can be a useful tool but it is not a HIPAA or regulatory requirement
- SOC 2 is a great beginning to your due diligence, but you must understand the report and its scope to determine whether it is reliable
- It is not a replacement for a HIPAA enterprise risk analysis and is not a "golden ticket" to onboard a business associate
- Review whether HIPAA is part of the scope of the SOC 2
- If your entity chooses to have a SOC 2, ensure that HIPAA is included or tied-in to achieve the best return on your investment

23

PROVIDER, BUSINESS ASSOCIATE, OR SOMETHING ELSE?

- How to assess whether a provider may be a business associate
  - What "business function(s)" is the entity providing?
  - **Example:** If the provider or provider group is performing analytics functions related to cost control on behalf of your entity, it might be a business associate.
    - If you are providing business services on behalf of a provider, you might be a business associate.
  - Many provider groups and other businesses are getting creative and expanding their business portfolio.
- Is it a provider, business associate, or something else?
  - Example: Personally-tailored drug manufacturer
  - What do I do if the entity with which I am doing business is "something else?"
    - Understand the differences and uses of Business Associate Agreements, Non-Disclosure Agreements, and Privacy and Security Agreements

24

COVID-19 IMPACT

25

COVID-19 Areas of Guidance & Enforcement Discretion

- Telehealth (health care providers only)
- Contacting patients about blood and plasma donation opportunities (providers and plans)
- Community-based testing (providers)
- Business associate disclosures for public health and health oversight
- Disclosures to first responders and law enforcement
- Health information exchange and public health

- Overall, not much affected health plans.

26

Employee Privacy Challenges

- The line between employee information and PHI gets blurred, as employers need COVID-19 data to operate.
- COVID-19 creates a lot of potential for employee curiosity and snooping
- Vaccination data will be the next big challenge

27

Working Remotely

- PHI at home: reasonable safeguards
- ePHI from home: risk assessment, risk management, and evaluation of changes in environment
- Policies and Training
- Physical safeguards of home workstations
- Contingency planning, emergency operation mode

28

CONCLUSION

29

Conclusions

- Privacy and security continues to be a dynamic area
  - Constant changes to privacy laws
  - Ever increasing information security threats
- Interoperability adds new wrinkles, with the tension between the flow of PHI and confidentiality
- Right of access has clearly become a top OCR enforcement priority, although other areas continue to pose risk
- Vendors represent a potential weak link in the information security chain
- COVID-19 introduced new security risks and privacy challenges

30

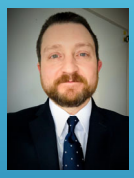
Questions?

31

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213



Jonathan R. Friesen, JD

Geisinger

jfriesen@geisinger.edu
570.214.2423

32