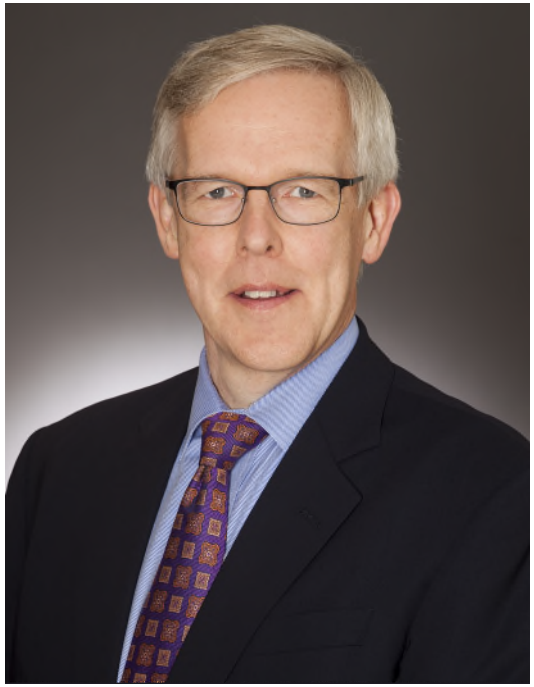
FOLEY HOAG LLP

New Developments in HIPAA and Related Issues in Health Information Law

MaHIMA Dot Wagg Memorial Legislative Seminar
October 28, 2020

Colin J. Zick, Esq.
Foley Hoag LLP



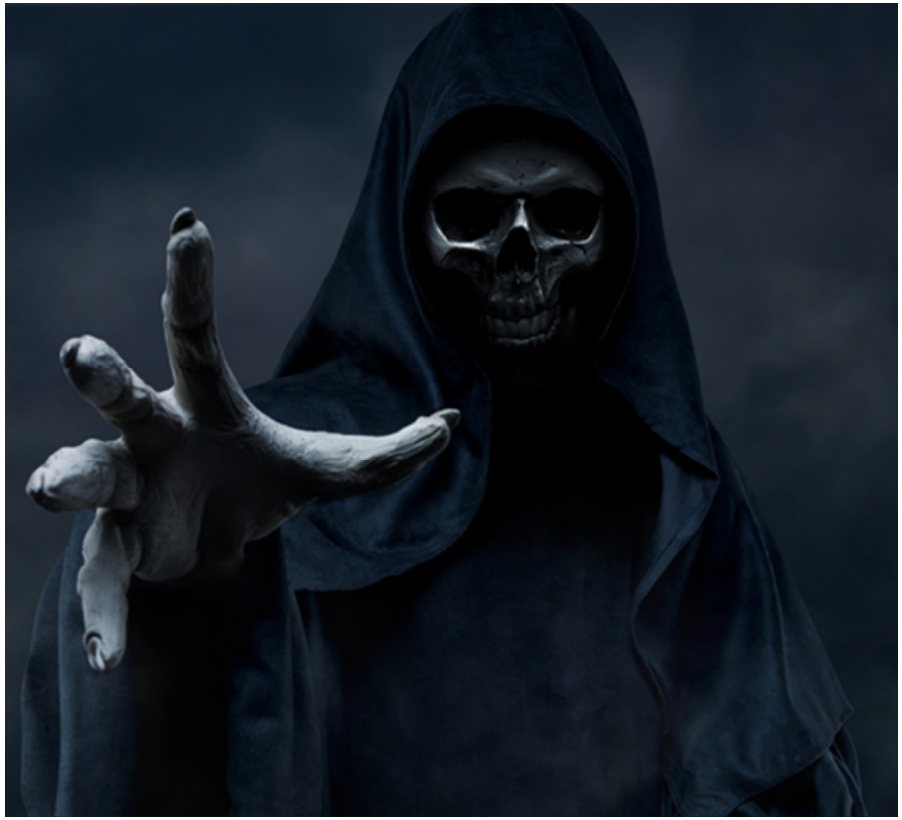
Colin J. Zick

Partner, Chair, Privacy and Data Security Practice,
and Co-Chair, Health Care Practice

Boston | +1.617.832.1275 | czick@foleyhoag.com

- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.
- Selected by his peers for inclusion in THE BEST LAWYERS IN AMERICA in the fields of Healthcare Law (2015-present) and Privacy and Data Security (2018-present)
- Ranked by CHAMBERS USA: AMERICA'S LEADING LAWYERS FOR BUSINESS as one of Massachusetts' leading Healthcare attorneys (2010-present)

Halloween or HIPAA: Which is Scarier?



HIPAA and the Pandemic

- Telehealth:
  - On Friday, March 20, 2020, OCR announced it will "exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."
  - Someday, there will be no public health emergency. What then?
- COVID testing:
  - Disclosures when HIPAA applies: On March 24, 2020, OCR issued guidance on how HIPAA covered entities may disclose PHI about an individual who has been infected with or exposed to COVID-19 to law enforcement, paramedics, other first responders, and public health authorities in compliance with HIPAA.
  - Lots of screening testing in which HIPAA does not apply and results are not being reported. But states are pushing back on this lack of disclosure.

HIPAA and the Pandemic (cont.)

- OCR Issues Guidance on How Health Care Providers Can Contact Former COVID-19 Patients About Blood and Plasma Donation Opportunities - June 12, 2020
- OCR Issues Guidance on Covered Health Care Providers and Restrictions on Media Access to Protected Health Information about Individuals in Their Facilities - May 5, 2020
- OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency - April 9, 2020
- OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency - April 2, 2020
- OCR Issues Bulletin on Civil Rights Laws and HIPAA Flexibilities That Apply During the COVID-19 Emergency - March 28, 2020

HIPAA and the Pandemic (cont.)

- OCR Issues Guidance to Help Ensure First Responders and Others Receive Protected Health Information about Individuals Exposed to COVID-19 - March 24, 2020
- OCR Issues Guidance on Telehealth Remote Communications Following Its Notification of Enforcement Discretion - March 20, 2020
- OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency - March 17, 2020
- OCR COVID-19 & HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency - March 17, 2020
- OCR BULLETIN: HIPAA Privacy and Novel Coronavirus – February 2020

HIPAA Enforcement Trends

- Since the compliance date of the Privacy Rule in April 2003, OCR has received over 245,393 HIPAA complaints and has initiated over 1,028 compliance reviews. We have resolved ninety-eight percent of these cases (241,570).
- From the compliance date to the present, the compliance issues most often alleged in complaints are, compiled cumulatively, in order of frequency:
  - Impermissible uses and disclosures of PHI;
  - Lack of safeguards of PHI;
  - Lack of patient access to their PHI;
  - Lack of administrative safeguards of electronic PHI; and
  - Use or disclosure of more than the minimum necessary PHI.

HIPAA Right of Access Penalties: 2020

- In 2019, OCR announced its “right to access” initiative.
- In 2020, OCR got serious about enforcement, settling nine cases in the last two months.
  - On October 9, 2020, it was announced that “OCR Settles Ninth Investigation in HIPAA Right of Access Initiative”
  - NY Spine Medicine agreed to take corrective actions and pay $100,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard.
  - In July 2019, OCR received a complaint from an individual alleging that beginning in June 2019, she made multiple requests to NY Spine for a copy of her medical records. NY Spine provided some of the records, but did not provide the diagnostic films that the individual specifically requested.
  - In addition to the monetary settlement, NY Spine will undertake a corrective action plan that includes two years of monitoring.

HIPAA Settlements: 2020

- Health Insurer Pays $6.85 Million to Settle Data Breach Affecting Over 10.4 Million People - September 25, 2020
- HIPAA Business Associate Pays $2.3 Million to Settle Breach Affecting Protected Health Information of Over 6 million Individual - September 23, 2020
- Orthopedic Clinic Pays $1.5 Million to Settle Systemic Noncompliance with HIPAA Rules - September 21, 2020
- Lifespan Pays $1M to OCR to Settle Unencrypted Stolen Laptop Breach - July 27, 2020
- Small Health Care Provider Fails to Implement Multiple HIPAA Security Rule Requirements, Fined $25,000 - July 23, 2020
- Health Care Provider Pays $100,000 Settlement to OCR for Failing to Implement HIPAA Security Rule Requirements - March 3, 2020

The FTC Wants to Get into the Breach Notification Act

- FTC Seeks Comment as Part of Review of Health Breach Notification Rule
  - The Federal Trade Commission is seeking comment on whether proposed changes should be made to a decade-old rule that requires certain companies that provide or service personal health records to notify consumers and the Commission of a data breach.
  - The Health Breach Notification Rule, which went into effective in 2009, requires vendors of personal health records and related entities that are not covered by the Health Insurance Portability and Accountability Act (HIPPA [sic]) to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data.
  - Currently, the Rule requires such entities to provide notifications within 60 days after discovery of the breach. If more than 500 individuals are affected by a breach, however, entities must notify the FTC within 10 business days.

Interoperability/Patient Access Rule

- On May 1, 2020 CMS published in the Federal Register the Interoperability & Patient Access Final Rule. The comprehensive interoperability regulation adopts a number of significant reforms:
  1. Establishes requirements for a new **Patient Access API** and a new **Provider Director API** for CMS-regulated payers
  2. Creates a **Payer-to-Payer Data Exchange**, to allow patients to "take" their data as they switch between health plans
  3. Creates new public reporting for providers that engage in **information blocking** or who fail to list or update contact information with **NPPES**
  4. Modifies the Medicare Conditions of Participation to require hospitals, including psychiatric hospitals and critical access hospitals, to send electronic patient event notifications of a patient's **admission, discharge, and/or transfer (ADT)** to another healthcare facility or to another community provider or practitioner

New Patient Notification Requirement

HOSPITALS

Post-Acute Care (PAC) Providers & Suppliers

PCPs and Physician Groups

As part of the Conditions of Participation, **all hospitals with an electronic medical record system** capable of sending ADT messages (including critical access hospital and psych) must send notifications in **near real time** to **PCPs, physician groups and post-acute providers** when a patient:

✓ **Registers** at the ED
✓ Is **admitted or transferred** to **Inpatient**
✓ Is **admitted or transferred** to **Observation**
✓ Is **discharged** from any of the above

New Patient Notification Requirement

Minimum information to be included in notification

- Patient name
- Treating practitioner name
- Sending institution name
- Patient diagnosis when permitted by law (***not required***)

Compliance Details

- Must have an established care relationship with the patient
  - PCP
  - Previous PAC provider or one where the patient is being transferred or referred
  - Any physician identified by the patient as a primary care
- Make a "reasonable effort" to send to all providers
- Include out-of-network providers
- No specific standard (e.g., HL7, FHIR, CCDA) required to deliver notification
- Does not need to measure "receipt"

Compliance Effective May 1, 2021

FAQs on Compliance

- **Q:** My hospital does not have an EHR system capable of sending ADT notifications. Do I need to comply?
  - **A:** No. CMS is defining a system with this capacity as one that utilizes the ADT messaging standard, Health Level Seven (HL7®) Messaging Standard Version 2.5.1 (HL7 2.5.1)). If your medical record or EHR system does not have this technical capacity, you need not comply.

- **Q:** My EHR system is capable of meeting the ADT messaging standard, but we rely on direct messaging for these types of communications. Am I required to utilize the ADT messaging standard (HL7) to send patient event notifications?
  - **A:** No. CMS is adopting the ADT standard solely to determine whether a hospital is subject to the Conditions of Participation. CMS is not specifying a standard for the content, format, or delivery of the patient event notifications.

FAQs on Compliance (cont.)

- **Q**: Is it possible I may need to send multiple notifications for a patient during a single stay?
  - **A:** Yes. By way of an example, consider a patient presenting at the ED that is later admitted as an inpatient. The hospital would be expected to send:
    - ✓**One notification upon registration in the ED**
    - ✓**One notification upon admission as an inpatient**
    - ✓**One notification upon discharge from the hospital**

- **Q:** What providers do I need to notify?
  - **A:** Pursuant to the updated Conditions of Participation, you must make reasonable efforts to notify:
    1. **All applicable post-acute care services providers and supplies; and**
    2. **The patient's established primary care practitioner; or**
    3. **The patient's established primary care practice group; or**
    4. **Other practitioners responsible for the patient's care**

FAQs on Compliance (cont.)

- **Q**: How do I identify "applicable" PAC providers?
  - **A:** Notifications should be sent to those PAC providers with whom the patient **(1)** has an **established care relationship immediately preceding** the hospital registration or admission and/or **(2)** to those providers to whom the patient is **being transferred or referred**.

- **Q**: Who is an "established" primary care provider?
  - **A:** In the preamble, CMS makes clear the focus should be on a patient's primary care practitioner or group identified by the patient (or through the medical record) as primarily responsible for his or her care. The emphasis is on those providers that ***need*** *to receive notification of the patient's status for treatment, care coordination, or quality improvement purposes.*

FAQs on Compliance (cont.)

- **Q:** What is a “reasonable effort” for purposes of sending notifications?
  - **A:** CMS states that the focus is on those circumstances within the hospital’s control. Thus, if a provider is not capable of receiving a notification within a hospital system’s capabilities, a provider has still made a reasonable effort.

- **Q:** Why is CMS amending the Conditions of Participation? What are the implications?
  - **A:** This was arguably the most controversial piece of this policy, as failure to comply with applicable Conditions of Participation can result in termination from the Medicare program. Still, CMS reinforced its belief that “patient event notifications should be a fundamental feature of hospital medical record systems to support effective care transitions and promote patient safety during transitions.”

FAQs on Compliance (cont.)

- **Q:** How will CMS ensure compliance with this new requirement?
  - **A:** CMS will develop updated policies and procedures for its surveyors who will likely:
    - (1) interview hospital and medical records staff;
    - (2) review active and closed medical records for evidence of patient event notifications;
    - (3) review patient event notification policies and procedures; and
    - (4) conduct observational interviews to determine if requirements are being met.
- **Q:** May I rely on an intermediary to transmit this patient event notification data on my behalf?
  - **A:** Yes. The final rule explicitly recognizes the ability of an third-party or intermediary to facilitate the patient event notifications so long as the intermediary does not impose restrictions on which recipients are able to receive notifications. CMS notes: "*We agree that the use of intermediaries to deliver patient notifications can reduce burden on hospitals and support effective notification systems.*"

Changes to 42 C.F.R. Part 2

- SAMHSA has revised part 2, to facilitate better coordination of care for substance use disorders which will also enhance care for opioid use disorder (OUD).
- **What Changed Under the New Part 2 Rule:** The new rule modifies several sections of Part 2, as follows:

Provision	What Changed?	Why Was This Changed?
Applicability and Re-Disclosure	Treatment records created by non-Part 2 providers based on their own patient encounter(s) are explicitly not covered by Part 2, unless any SUD records previously received from a Part 2 program are incorporated into such records. Segmentation or holding a part of any Part 2 patient record previously received can be used to ensure that new records created by non-Part 2 providers will not become subject to Part 2.	To facilitate coordination of care activities by non-part-2 providers.
Disposition of Records	When an SUD patient sends an incidental message to the personal device of an employee of a Part 2 program, the employee will be able to fulfill the Part 2 requirement for "sanitizing" the device by deleting that message.	To ensure that the personal devices of employees will not need to be confiscated or destroyed, in order to sanitize in compliance with Part 2.
Consent Requirements	An SUD patient may consent to disclosure of the patient's Part 2 treatment records to an entity (e.g., the Social Security Administration), without naming a specific person as the recipient for the disclosure.	To allow patients to apply for benefits and resources more easily, for example, when using online applications that do not identify a specific person as the recipient for a disclosure of Part 2 records.

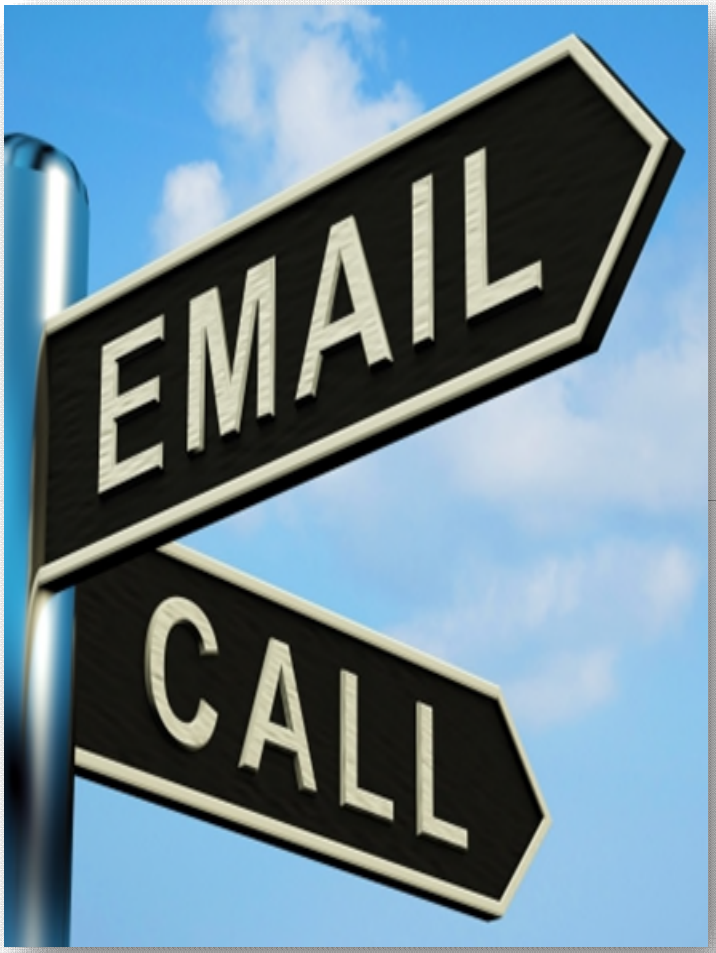
More 42 C.F.R. Part 2 Changes

Disclosures to Central Registries and PDMPs	Non-OTP (opioid treatment program) and non-central registry treating providers are now eligible to query a central registry, in order to determine whether their patients are already receiving opioid treatment through a member program. OTPs are permitted to enroll in a state prescription drug monitoring program (PDMP), and permitted to report data into the PDMP when prescribing or dispensing medications on Schedules II to V, consistent with applicable state law.	To prevent duplicative enrollments in SUD care, duplicative prescriptions for SUD treatment, and adverse drug events related to SUD treatment.
Medical Emergencies	Declared emergencies resulting from natural disasters (e.g., hurricanes) that disrupt treatment facilities and services are considered a "bona fide medical emergency," for the purpose of disclosing SUD records without patient consent under Part 2.	To ensure clinically appropriate communications and access to SUD care, in the context of declared emergencies resulting from natural disasters.
Research	Disclosures for research under Part 2 are permitted by a HIPAA-covered entity or business associate to individuals and organizations who are neither HIPAA covered entities, nor subject to the Common Rule (re: Research on Human Subjects).	To facilitate appropriate disclosures for research, by streamlining overlapping requirements under Part 2, the HIPAA Privacy Rule and the Common Rule.
Audit and Evaluation	Clarifies specific situations that fall within the scope of permissible disclosures for audits and/or program evaluation purposes.	To resolve current ambiguity under Part 2 about what activities are covered by the audit and evaluation provision.
Undercover Agents and Informants	Court-ordered placement of an undercover agent or informant within a Part 2 program is extended to a period of 12 months, and courts are authorized to further extend the period of placement through a new court order.	To address law enforcement concerns that the current policy is overly restrictive to some ongoing investigations of Part 2 programs.

California Consumer Privacy Act and HIPAA

- CCPA went into effect January 1, 2020; it regulates the privacy of health information of California residents, but exempts:
  - Protected Health Information (PHI)
  - Personal information that HIPAA-covered entities handle like PHI
- Most likely to benefit from this exemption
  - Health care providers
  - Health insurers
- These companies collect personal information that is <u>not</u> exempt:
  - Employment information
  - Electronic network activity information (e.g., cookies)
  - Labs doing return to work COVID screening (not diagnostic testing)

Thank you!



Colin Zick

Partner,
Co-Chair, Health Care Practice, and
Privacy & Data Security Practice

Foley Hoag LLP

czick@foleyhoag.com | 617.832.1275

Thanks to my colleague, Ross Margulies, for his contributions to the part of this presentation addressing interoperability.