New Developments in HIPAA and Related Issues in Health Information Law

MaHIMA Dot Wagg Memorial Legislative Seminar
November 1, 2019

Colin J. Zick, Esq.
Foley Hoag LLP

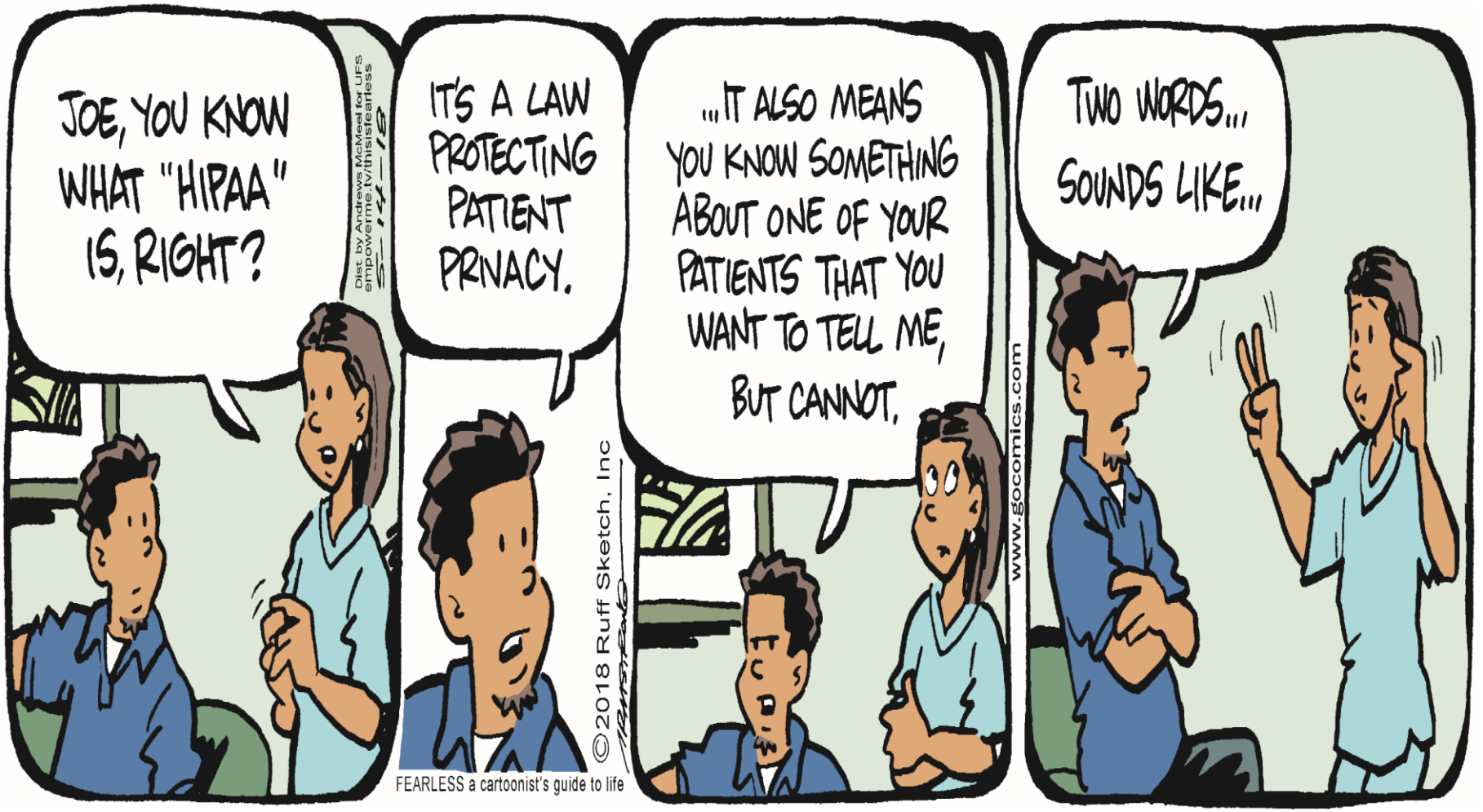
Colin J. Zick

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)

Charades



Physicians Talking With Their Domestic Partners About Patients

- Health care institutions often require that physicians and medical students click through annual online modules or attend lectures about HIPAA.
  - But do these tutorials help a physician know what to say to a partner after making a mistake with a patient?
  - How to talk about a patient death?
  - How to share their lives at work with the ones they love?
- Physicians may benefit from accessing spaces independent of their partners, such as process groups with colleagues or counseling sessions with mental health professionals where they can speak in confidence, potentially taking some of the burden off their partners and themselves.
- Even these spaces, however, may create issues with respect to HIPAA, making the need for clarification on the boundaries of disclosure all the more important.
- See JAMA, October 15, 2019

Health & Fitness Apps and HIPAA

- Fitness, wellness and health-tracking apps may be convenient and easy to use, but apps should be forthright about data collection and use and that have security measures like data encoding.
- Wall Street Journal, February 24, 2019, "Popular Apps Cease Sharing Data With Facebook"
  - Flo Period & Ovulation Tracker
  - Azumio's Instant Heart Rate
  - Fit Now's Lose It!
- Washington Post, April 10, 2019, "Is your pregnancy app sharing intimate data with your boss?"
  - Some companies were sharing intentionally
  - But some were sharing accidentally
  - This is only going to be come a bigger issue, as more apps are integrated into patient care, e.g.:
    - Diabetes (Livongo, Onduo)
    - Mental health (Pear)

HIPAA FAQs on Right of Access: Health Apps and APIs

- On June 17, 2019, OCR released frequently asked questions about the HIPAA right of access related to apps designated by the individual and application programming interfaces (APIs) used by the provider's electronic health record system. These FAQs addressed:
  - Liability for such transfers? It depends.
    - Once health information is received from a covered entity, at the individual's direction, by an app that is neither a covered entity nor a business associate under HIPAA, the information is no longer subject to the protections of the HIPAA Rules.
  - Does the provider need a BAA with the app provider? It depends.

HIPAA FAQs on Right of Access: $$$

- **May a covered entity charge individuals a fee for providing the individuals with a copy of their PHI?**
  - Yes, but only within specific limits. The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee to provide the individual (or the individual's personal representative) with a copy of the individual's PHI, or to direct the copy to a designated third party. The fee may include only the cost of certain labor, supplies, and postage:
- **Is $6.50 the maximum amount that can be charged to provide individuals with a copy of their PHI?**
  - No. For any request from an individual, a covered entity (or business associate operating on its behalf) may calculate the allowable fees for providing individuals with copies of their PHI: (1) by calculating actual allowable costs to fulfill each request; or (2) by using a schedule of costs based on average allowable labor costs to fulfill standard requests. Alternatively, in the case of requests for an electronic copy of PHI maintained electronically, covered entities may: (3) charge a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and postage). Charging a flat fee not to exceed $6.50 per request is therefore an option available to entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically.

CMS/ONC Proposed Interoperability Regulations

- The CMS Interoperability and Patient Access Proposed Rule introduces new policies that will expand access to health information and improve the seamless exchange of data in healthcare.
  - This will enable better care coordination, better patient outcomes and reduced costs.
  - The proposals will help to break down existing barriers to interoperability and empower patients by giving them access to their health information.
- The policies in this proposed rule touch on all aspects of healthcare, from patients to providers to payers and researchers.

Potential Changes to 42 C.F.R. Part 2

- SAMHSA is currently proposing to revise part 2, to facilitate better coordination of care for substance use disorders which will also enhance care for opioid use disorder (OUD).
- **What Is Changing Under the New Part 2 Rule:** The proposed rule will modify several sections of Part 2, as follows:

Provision	What Is the Proposed Change?	Why Is This Being Changed?
Applicability and Re-Disclosure	Treatment records created by non-part 2 providers based on their own patient encounter(s) will not be covered by part 2, unless any SUD records previously received from a part 2 program are incorporated into such records. Segmentation or holding apart 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 per part 2.
Consent Requirements	An SUD patient may consent to disclosure of his 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.
Disclosures Permitted w/ Written Consent	Disclosures for the purpose of "payment and health care operations" are permitted with written consent, in connection with an illustrative list of 17 example activities.	In order to resolve lingering confusion under part 2 about what activities count as "payment and health care operations," the list of examples will be moved into the reg text from the preamble.

HIPAA Enforcement Trends

OCR Concludes All-Time Record Year for HIPAA Enforcement

- OCR Imposes a $2.15 Million Civil Money Penalty against Jackson Health System for HIPAA Violations - October 23, 2019
- Dental Practice Pays $10,000 to Settle Social Media Disclosures of Patients' Protected Health Information - October 2, 2019
- OCR Settles First Case in HIPAA Right of Access Initiative - September 9, 2019
- Indiana Medical Records Service Pays $100,000 to Settle HIPAA Breach - May 23, 2019
- Tennessee Diagnostic Medical Imaging Services Company Pays $3,000,000 to Settle Breach Exposing Over 300,000 Patients' Protected Health Information - May 6, 2019
- Cottage Health Settles Potential Violations of HIPAA Rules for $3 Million - February 7, 2019
- Colorado hospital failed to terminate former employee's access to electronic protected health information - December 11, 2018
- Florida contractor physicians' group shares protected health information with unknown vendor without a business associate agreement - December 4, 2018

HIPAA and Massachusetts Law: Unfair Business Practices

- Pennington-Matte v. Steward Health Care System and Sharecare Health Data Services, LLC (f/k/a Bactes Imaging Solutions), Mass. Appeals Court
- Between 2013 and 2017, Pennington-Matte was a patient at various hospitals and healthcare facilities operated by Steward. On numerous occasions during that time period, Pennington-Matte requested electronic copies of her medical records.
- Pennington-Matte alleged that Sharecare did not provide the records she requested and some of records were not timely produced.
- She further alleged that she was consistently overcharged for the copies Sharecare sent to her or to her attorney. The court agreed:
  - "In order to obtain complete copies of her records and determine the proper amount she owed for the copies, Pennington-Matte hired an attorney to contact the defendants and intervene on her behalf. Assuming these allegations to be true, Pennington-Matte was defending against improper claims for payment and vindicating her rights under HIPAA and G. L. c. 111, § 70E, not vindicating her rights under G. L. c. 93A."

Proposed AKS Safe Harbors

- In tandem with the creation of a new Stark exception by CMS, OIG is proposing a new safe harbor to protect donations of certain cybersecurity technology.
  - (1) The donated technology must primarily serve to protect information by preventing, detecting, and responding to cyberattacks. As highlighted by OIG, this includes but is not limited to, “software that provides malware prevention, data protection and encryption, etc. The proposed cybersecurity safe harbor aims to protect a broad range of services including:
  - (2) Donation of technology may not be conditioned on future referrals.
  - (3) As mentioned above, the donation of technology may not be conditioned upon recipients conducting future or current business with the donor.
  - (4) The donor and recipient must enter into a written agreement.
  - (5) Donors are prohibited from shifting costs of any cybersecurity donations to federal health care programs.

California Consumer Privacy Act and HIPAA

- CCPA goes 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)

Mass. Digital Health Council: The DDN

- The Massachusetts Digital Health Council recommended the creation of a Distributed Digital Network ("DDN") to allow for the sharing of key electronic health records across Massachusetts.
- The DDN would serve the primary purpose of enabling providers' real time access to historical records and diagnoses to improve care and facilitate patients' access to their healthcare data.
- The DDN will require a legal framework that standardizes policies and processes for protected health information exchange.
- Foley Hoag was engaged by MassTech to advise on how best to implement the DDN under today's laws and regulations. The legal options for implementation are as follows:

OPTION A	OPTION B	OPTION C
Leveraging existing business associate agreement structure, an "Operational Virtual Entity" would be created and would contract with each covered entity ("CE") in the Commonwealth. The entity would be deemed a business associate of each CE to facilitate data flow in to the entity. The entity would then contract with Stewards to enable outbound data flow.	A separate entity would be created to serve as a health care clearinghouse under HIPAA. The mandate would require CEs to push data to the clearinghouse, which would then provide data to stewards. Note: Clearinghouse is a virtual entity and not a physical data clearinghouse.	All covered entities in the Commonwealth and certified stewards would form an "organized healthcare arrangement" allowing them to transfer data between each other with few legal constraints.

Thank you!

Colin Zick

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

Foley Hoag LLP

czick@foleyhoag.com | 617.832.1275