FOLEY HOAG LLP

# New Developments in Health Information Law

*MaHIMA Dot Wagg Legislative Seminar*
*November 9, 2018*

Colin J. Zick, Esq., Foley Hoag LLP

## Colin J. Zick

*Partner, Chair, Privacy and Data Security Practice*

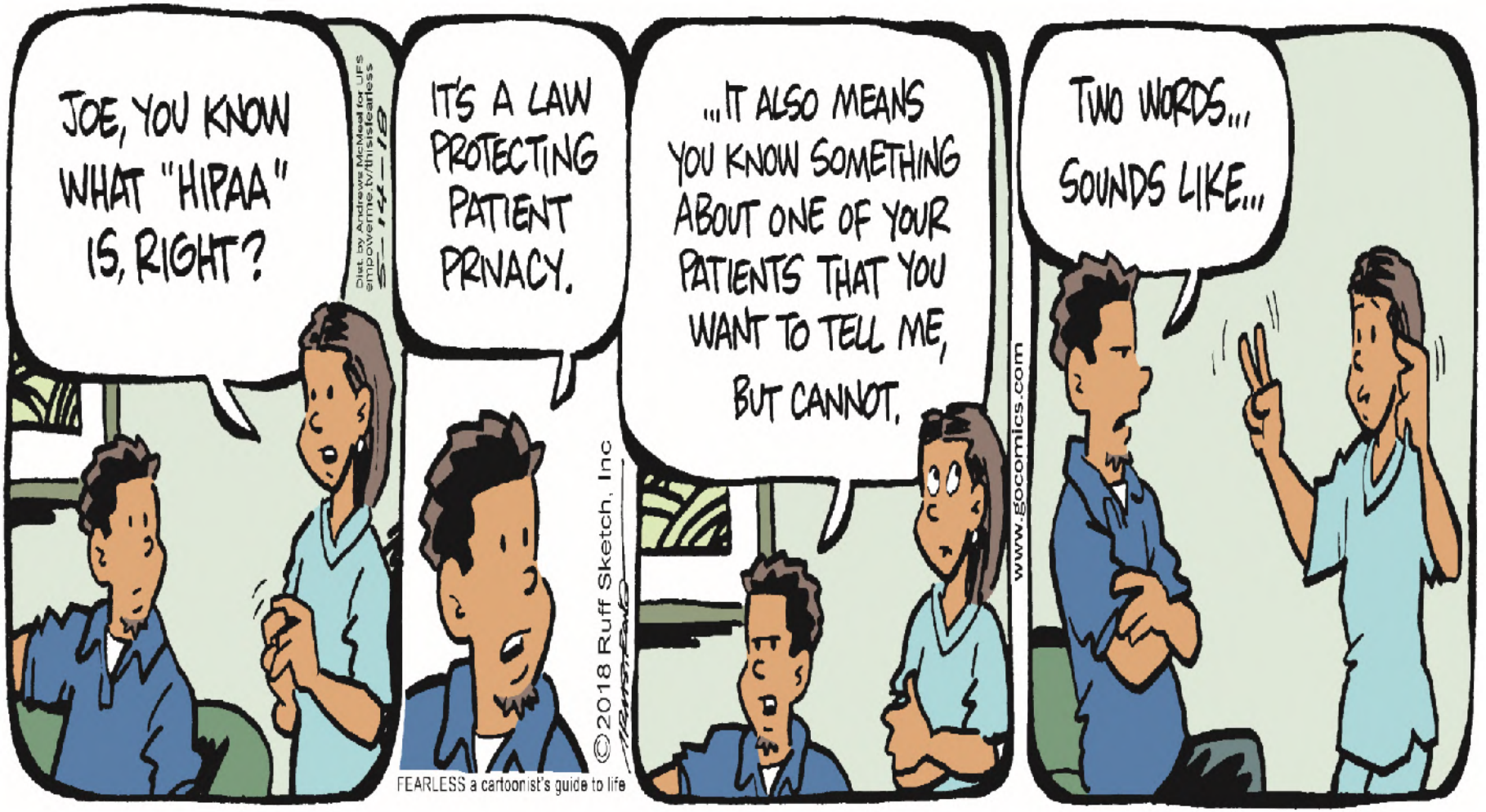
Boston | +1.617.832.1275 | czick@foleyhoag.com

- 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.

- Advises on issues involving the transfer of data between jurisdictions, including EU-US Privacy Shield, and other relevant data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.

- Co-founded the firm's Privacy and Data Security Group (which he currently chairs) and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com, and was recognized by JD Supra's 2017 Readers Choice Awards. Serves as outside counsel to the Advanced Cyber Security Center, and is a member of Law360's Privacy & Consumer Protection editorial advisory board.

# Charades




JUMP START © Robb Armstrong. Reprinted with permission of ANDREWS MCMEEL SYNDICATION. All rights reserved.

# One More Joke

"Knock, knock."

"Who's there?"

"HIPAA."

"HIPAA, who?"

"I'm sorry, but I cannot disclose that."

# 20+ Years Post-HIPAA ROI Still a Problem


JAMA Network | Open

Original Investigation | Health Informatics

**Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records**

Carolyn T. Lye, BA; Howard P. Forman, MD, MBA; Ruiyi Gao, BS; Jodi G. Daniel, JD, MPH; Allen L. Hsiao, MD; Marilyn K. Mann, JD; Dave deBronkart, BS; Hugo O. Campos; Harlan M. Krumholz, MD, SM

- Among the 83 top-ranked US hospitals representing 29 states, there was discordance between information provided on authorization forms and that obtained from the simulated patient telephone calls in terms of requestable information, formats of release, and costs.

# Texas cancer center pays $4.3 million for HIPAA violations

- MD Anderson Cancer Center had paid $4,348,000 in penalties to OCR, the fourth largest amount ever awarded for HIPAA violations.
- MD Anderson made three separate data breach reports in 2012 and 2013 involving the theft of an unencrypted laptop from the home of an employee and the loss of two unencrypted thumb drives containing the unencrypted ePHI of over 33,500 individuals.
- MD Anderson had written encryption policies and its own risk analyses found that the lack of device-level encryption posed a high risk to the security of ePHI.
- Even so, MD Anderson failed to encrypt its electronic devices.
- MD Anderson claimed that it was not obligated to encrypt its devices, and the ePHI at issue was for “research,” and thus was not subject to HIPAA’s nondisclosure requirements.

# 42 CFR Part 2 and HIPAA

- Applicability of 42 CFR Part 2 is fact-specific and hard to categorize, but consent requirements and exceptions & exclusions remain.
- 2018 Revision - Disclosures for Payment and Healthcare Operations ( § 2.33)
  - Additional disclosures of patient identifying information, with patient consent, to facilitate payment and healthcare operations such as claims management, quality assessment, and patient safety activities.
  - Lawful holders to disclose or re-disclose patient identifying information to their contractors, subcontractors and legal representatives for purposes of carrying out the lawful holder's payment and health care operations activities, when patient consents to disclosure for those activities.
- **ER staffs accessing medical record and communication about patient's health information:** ER is likely not holding itself out as providing substance use disorder diagnosis, treatment, or referral for treatment. Therefore, 42 CFR Part 2 would not apply to the ER. The Privacy Rule permits covered entities to use and disclose PHI for TPO. ER staff may provide directory information and general condition of patient to family member.
- **Hospitals receiving subpoena for "any and all records" within its possession for patient:** subpoena might not be compliant with both HIPAA and Part 2.

# Meanwhile, in Massachusetts….

- Chapter 63 of the Acts of 2018 (amending Chapter 176O, section 27), “An Act to Protect Confidentiality of Health Information”
- (a) The division shall develop a common summary of payments form to be used by all carriers in the commonwealth and provided to health care consumers with respect to provider claims submitted to a payer. [It] shall be written in an easily readable and understandable format … [and] may be exchanged securely through electronic means.…
- (b) Carriers shall issue common summary of payments forms at the member level for each insured member [and] may establish a standard method of delivery ….
- (e) Carriers shall not specify or describe sensitive health care services in [this] form. The division shall define sensitive health care services for the purposes of this section….

# Lawsuits About the Costs of Copies

- The plaintiff's tort/workers comp bar is very active in this space.
- Demands letters about ROI are common.
- Settlements are common.
- There's a key issue as yet unresolved (at least to these lawyers).

# Recent Court Decision on ROI Fees

- 11th Circuit (reviewing a case from Georgia) regarding ROI fees.
- Plaintiffs claimed that the overcharges (1) were in violation of the business associate agreement between defendant and the health care provider for plaintiffs, (2) the defendant was unjustly enriched by the payments.
- The court affirmed dismissal of the contract claim, noting that the business associate agreement (like most business associate agreements) specified that there are no third party beneficiaries to the agreement, and that under state law generally only parties to a contract may enforce it. The court also affirmed dismissal of the unjust enrichment claim, because under state law a plaintiff generally may not claim that a voluntary payment led to unjust enrichment.
- "Plaintiffs made payments to Defendant despite knowing that Defendant had likely charged more for the already provided medical records than was legally permitted," but paid anyway.

# Have Your Heard About GDPR?

- On May 25, 2018, the General Data Protection Regulation ("the GDPR") will apply in all Member States of the European Union ("EU") and will replace the Directive 95/46/CE ("the Directive").
- The purpose of the Directive was to protect the personal data of individuals to an extent that may seem surprising from a US point of view. The new regulation goes even further, since it is presented as "*an essential step to strengthen citizens' fundamental rights in the digital age*."
- The GDPR applies to the collecting and processing of personal data by all kinds of entities in all activities, including in the healthcare/life science sectors.
- **You Can't Ignore the GDPR.** The GDPR will apply to organizations established outside the EU that offer goods or services to individuals in the EU and/or monitor the behavior of data subjects within the EU (Article 3). In other words, even a US company will have to comply with the GDPR if it targets European consumers or monitors any personal data on European citizens.

# 21st Century Cures Act

- 12/13/2016 Signed by President and became law
- How does it impact HIM:
  - Sec. 4003. Interoperability.
  - Sec. 4004. Information blocking.
  - Sec. 4005. Leveraging electronic health records to improve patient care.
  - Sec. 4006. Empowering patients and improving patient access to their electronic health information.
  - Sec. 4012. Telehealth services in Medicare.

# 21st Century Cures Act: Section 4003

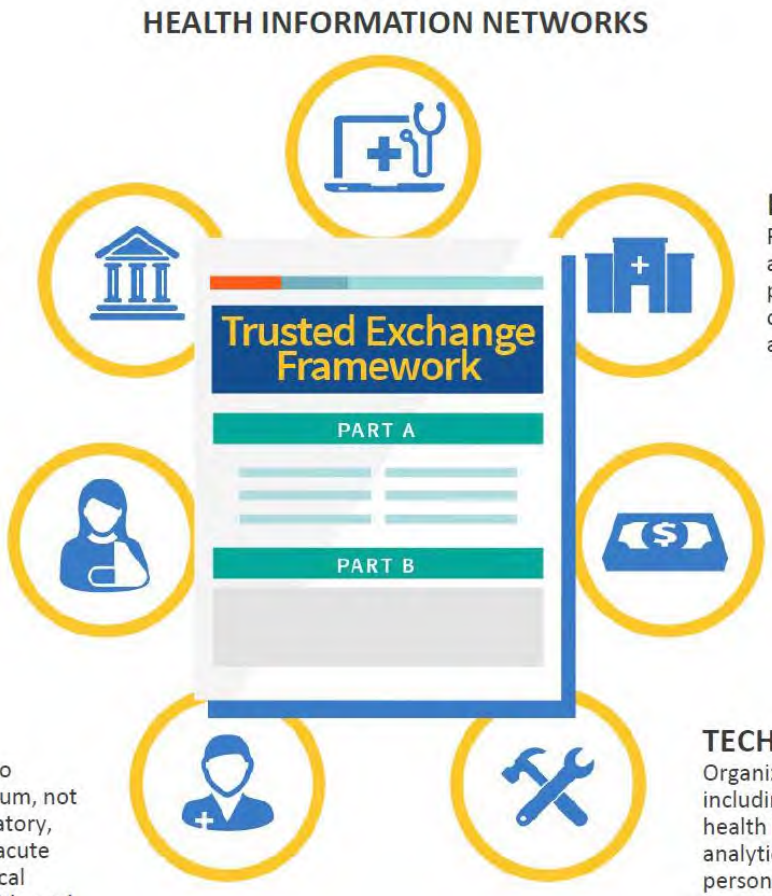
## Interoperability

- 4003(a) Defines Interoperability as:
  - The term ‘interoperability’, with respect to health information technology,
  - means such health information technology that—
    - A. enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;
    - B. allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
    - C. does not constitute information blocking as defined in section 3022(a) of the PHSA as amended.

# Trusted Exchange Framework and Common Agreement

- *"Not later than 6 months after the date of enactment of the 21st Century Cures Act, the National Coordinator*
- *shall convene appropriate public and private stakeholders to develop or support a trusted exchange*
- *framework for trust policies and practices and for a common agreement for exchange between health*
- *information networks. The common agreement may include—*
  - *(I) a common method for authenticating trusted health information network participants;*
  - *(II) a common set of rules for trusted exchange;*
  - *(III) organizational and operational policies to enable the exchange of health information among networks, including minimum conditions for such exchange to occur; and*
  - *(IV) a process for filing and adjudicating noncompliance with the terms of the common agreement."*

# Stakeholders who can use the Trusted Exchange Framework




**FEDERAL AGENCIES**
Federal, state, tribal, and local governments

**PUBLIC HEALTH**
Public and private organizations and agencies working collectively to prevent, promote and protect the health of communities by supporting efforts around essential public health services

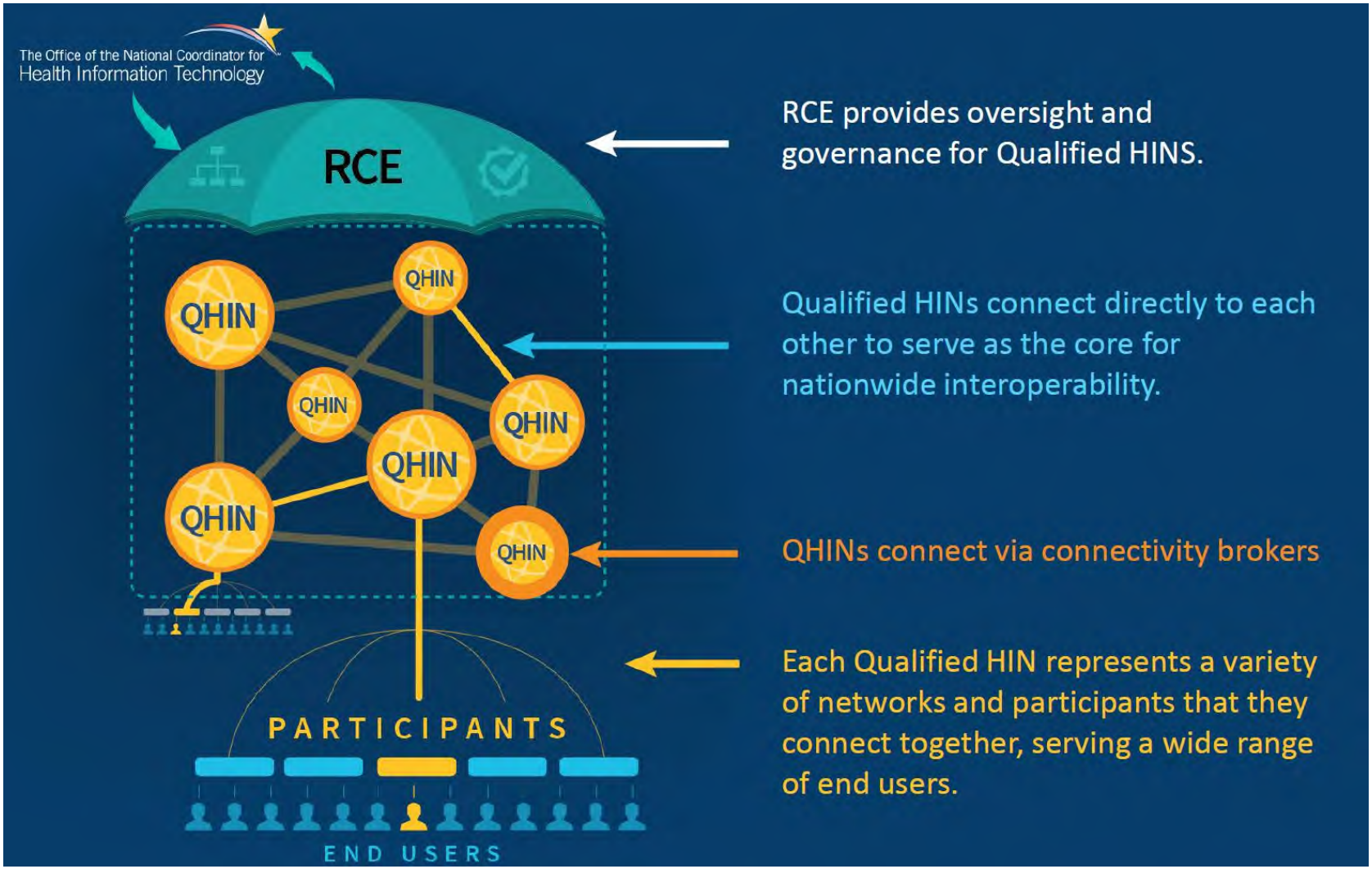
**INDIVIDUALS**
Patients, caregivers, authorized representatives, and family members serving in a non-professional role

**PAYERS**
Private payers, employers, and public payers that pay for programs like Medicare, Medicaid, and TRICARE

**PROVIDERS**
Professional care providers who deliver care across the continuum, not limited to but including ambulatory, inpatient, long-term and post-acute care (LTPAC), emergency medical services (EMS), behavioral health, and home and community based services

**TECHNOLOGY DEVELOPERS**
Organizations that provide health IT capabilities, including but not limited to electronic health records, health information exchange (HIE) technology, analytics products, laboratory information systems, personal health records, Qualified Clinical Data Registries (QCDRs), registries, pharmacy systems, mobile technology, and other technology that provides health IT capabilities and services

# How Will the Trusted Exchange Framework Work?



# Privacy/Security: Identity Proofing

**Identity proofing is the process of verifying a person is who they claim to be. The Trusted Exchange Framework requires identity proofing (referred to as the Identity Assurance Level (IAL) in SP 800-63A).**

**End Users and Participants** Each Qualified HIN shall require proof of identity for Participants and participating End Users at a minimum of IAL2 prior to issuance of credentials.

**Individuals** Each Qualified HIN shall require its End Users and Participants to proof the identity for Individuals at a minimum of IAL2 prior to issuance of credentials. Individuals must provide strong evidence of their identity.

| IAL 2 REQUIREMENT | DESCRIPTION |
|---|---|
| **Evidence** | • One (1) piece of SUPERIOR or STRONG evidence; OR<br>• Two (2) pieces of STRONG evidence; OR<br>• One (1) piece of STRONG evidence plus two (2) pieces of ADEQUATE evidence |
| **Validation** | • Each piece of evidence must be validated with a process able to achieve the same strength as the evidence presented.<br>• Validation against a third-party data service SHALL only be used for one piece of presented identity evidence. |
| **Address Confirmation** | • The Credential Service Provider (CSP) SHALL confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. |

# 21st Century Cures Act: Research

- Requires the Secretary of the Department of Health and Human Services (HHS) to issue "Guidance Related to Streamlining Authorization" under HIPAA for uses and disclosures of protected health information (PHI) for research.
- Authorizations for the use or disclosure of PHI for future research (or other purposes) must include a "description of each purpose of the requested use or disclosure. The statement 'at the request of the individual' is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose."
- Pursuant to sections 2063(b)(1)(B) and (C) of the Cures Act, OCR clarifies that an authorization for uses and disclosures of PHI for future research must contain "an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure." [8] When, as here, the authorization is for a use or disclosure of PHI for research, "including for the creation and maintenance of a research database or research repository," "the statement 'end of the research study,' 'none,' or similar language is

# 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