New Developments in Health Information Law, or How to Do Your Job and Not Get Arrested

MaHIMA Dot Wagg: November 3, 2017

Colin Zick, Esq., Foley Hoag LLP

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.

FOLEY HOAG LLP

The Issues

- By now, you have all seen the July 26, 2017 videotaped arrest of the head nurse at the University of Utah Hospital's burn unit, Alex Wubbels, by an over-reaching and over-zealous police officer (who has since been fired).
- Before seeing this, we might have assumed that not only hospital personnel, but law enforcement, understood the laws of informed consent and release of information. But we would be wrong.
- It's now over 20 years since HIPAA became law. Yet there is still vast ignorance or deliberate rejection of patient privacy rights, and those rights keep evolving just as the provision of care evolves.
- This raises the larger questions:
  - are we sure we know the law and how to apply it?
  - do we understand how to convey the law to others, even those who are supposed to know and enforce it?
  - what should be done when a dispute arises?

"Hi, I'm at the police station and they are asking for my phone."

- More and more information kept on phones.
- People don't want to have separate work phones.
- Information gets mixed together.
- What are the rules:
  - Emergency law enforcement access
  - Warrant
  - Can they keep the phone and for how long?
- How to prepare health care providers for this?
- What are the implications for your backups?

Rights Exercised by Personal Representatives

- Marianne Ajemian, v. Yahoo!, Mass. Supreme Judicial Court, October 16, 2017 addressed who can control a social media account of a decedent.
- "[A] personal representative may provide consent to the disclosure of a decedent's health information pursuant to the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § § 1320d et seq. (HIPAA). See 45 C.F.R. § 164.502. In like manner, a personal representative may provide consent on a decedent's behalf to a government search of a decedent's property. See United States v. Hunyady, 409 F.3d 297, 304 (6th Cir.), cert. denied, 546 U.S. 1067 (2005).
- Personal representative may waive decedent's patient-physician privilege)
- But how do we know who the personal representative is?

"Recalibrating Privacy Protections to Promote Patient Engagement"

- New England Journal of Medicine, October 26, 2017 discussing patient engagement, the "'blockbuster drug' of the 21st century"
- What are these new means of patient engagement?
  - Patient portals
  - Bluetooth biometric devices
  - Interactive voice response systems
  - Emails and text messages
- What does HIPAA fit in?
- How do state privacy laws fit in?

FOLEY HOAG LLP

All That Data!

- Therapies, diagnostics, and connected devices now gather huge amounts of data
- That data can be more valuable than the “thing” that is treated, diagnosing, or connecting, provided you have the legal ability to use that data, by:
  - Direct consent
  - Operation of law
  - Aggregation/anonymization

But There Are Risks….

- Journal of the American Medical Association, October 10, 2017, “Cybersecurity – A Serious Patient Care Concern”

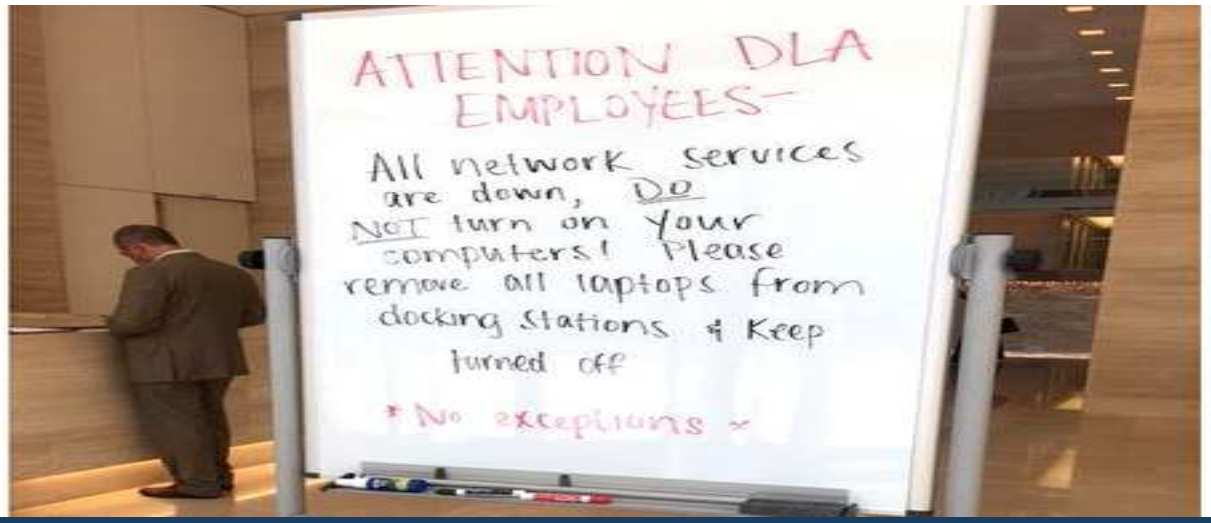
- **Average data breach costs:**
  - 2017: US $6.7 million
- **Lost business costs:**
  - US $3.91 million per breach
  - Loss of business/JVs/patients
  - Impairment of goodwill, reputation

JAMA: Cybersecurity Concerns and Medical Devices – Lessons from a Pacemaker Advisory, October 17, 2017

- Interesting viewpoints from this Journal of the American Medical Association article on FDA's August 2017 notice re: cyber security issues with certain pacemakers, including:
- "This first widespread cybersecurity advisory involving a permanent medical device implant provides some insight into the ways in which the public experience … might be improved."
- "Communications regarding widely used products for which multiple vendors exist in the marketplace should serve as opportunities to highlight current FDA and industry standards, and the degree to which similar products … may be subject to similar concerns."
- "[I]t could have been anticipated that popular media reports of a "pacemaker recall" would capture the attention of many patients living with unaffected devices…, who would wonder if their own device would be vulnerable to the same problem."
- "FDA might have leveraged the safety communication…."

The Worst Case: DLA Piper's Experience

- DLA was hit with a ransomware attack on June 27, 2017
- Attributed to "Petrwrap/Petya" ransomware
- Firm was "paralyzed": phones, computers and emails were down for nearly a week
- Lawyers were using cell phones and personal email accounts for firm business



FOLEY HOAG LLP

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.

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