FOLEY HOAG LLP

MaHIMA Webinar: "Alexa, What Medication Am I Taking?"

February 27, 2019

Colin Zick and Jeremy Meisinger, Esq.
Foley Hoag LLP

FOLEY HOAG 75 SINCE 1943

Colin J. Zick

Partner, Chair, Privacy and Data Security Practice

Boston | +1.617.832.1275 | czick@foleyhoag.com

- Counsels clients on issues involving regulatory compliance, and often involves the intersection of compliance with administrative proceedings or litigation. His work emphasizes compliance issues related to hospitals, physicians, provider organizations and insurers, as well as diagnostic testing companies, medical device and pharmaceutical manufacturers.

- Defends clients in disputes alleging kickbacks, overpayments, and billing and coding problems, and represents clients before state and federal health care licensing and regulatory entities. Has created comprehensive corporate compliance programs, successfully represented companies against alleged violations of state and federal anti-kickback statutes, securing OIG advisory opinions, and negotiating OIG corporate integrity agreements.

- Ranked as one of the Best Lawyers in America® for Healthcare since 2015, ranked by CHAMBERS USA as one of Massachusetts' leading health care lawyers since 2010. He also has served as the Chair of the Lex Mundi Health Care Industries Practice Group and as Co-Chair of the Boston Bar Association’s Health Law Section.

Jeremy W. Meisinger

Associate, Privacy and Data Security Practice

Boston | +1.617.832.3029 | jmeisinger@foleyhoag.com

- Answers client questions on regulatory compliance issues in healthcare and broader questions related to data privacy and security across multiple fields. His work focuses on compliance questions faced by providers, provider organizations, insurers, as well as diagnostic testing companies and pharmaceutical manufacturers.
- Represents clients before state and federal healthcare licensing and regulatory entities.
- Helps clients to develop internal data security and privacy policies, in both healthcare and non-healthcare contexts, as well as consumer-facing materials such as website privacy policies and terms of service.

About Foley Hoag LLP

- **280 attorney** firm founded in 1943 with offices in **Boston**, **New York, Paris** and **Washington DC**
- **150+ Health care and life sciences lawyers representing over 1,500 public and private clients** in a wide range of contexts
- Consistently recognized as leading law firm by:

IFLR1000 UNITED STATES
NYSE
IFLR1000
Chambers AND PARTNERS
The LEGAL 500
THE AMERICAN LAWYER
Best Lawyers BEST LAW FIRMS U.S.News
PRACTICAL LAW COMPANY
WTR World Trademark Review
Super Lawyers
CORPORATE counsel
iam
PatentBuddy Top Patent Prosecutors
Best Lawyers

FOLEY HOAG LLP

“Open the pod door, HAL”

- Commercial voice-activated intelligent personal assistants from Amazon, Apple, Google, and Microsoft, among others, are growing in popularity.
- A report from NPR and Edison Research states that 16% of the U.S. population—39 million Americans—currently owns a smart speaker that relies on a voice-activated personal assistant.
- Smart speakers will be installed in 55% of U.S. households by 2022—equaling 70 million households.
- As consumers become more accustomed to asking such devices for information, healthcare organizations will naturally become integrated into that behavior, and some already have.
- But are we ready for the response that HAL gave, or the other complications this technology brings?

Increasing Use of, and Scrutiny of, Voice-Activated Devices

- Arkansas police in 2017 obtained a search warrant to obtain recordings from Alexa, where a consumer's device may have recorded information relevant to a murder case.
- Amazon was ordered to hand over multiple days of Echo recordings in 2018 related to a double murder in New Hampshire.
- An Echo owner in 2018 reported to a local news media outlet in Seattle that she had inadvertently caused her Echo to send a recording of her conversation to a contact in her contact list.

Can Siri Stay After Visiting Hours?

- From mobile apps for monitoring medications to virtual appointments with specialists, telehealth services are creating new levels of convenience for providers and patients.
- As companies digitize more pieces of the health care puzzle, this will mean navigating complicated state regulations, evolving payer relationships, and issues around data and patient privacy.
- Hospitals have been using voice assistants for non-clinical applications, such as ordering lunch.
- Now they are moving to clinical applications, so that patients can check on their medications and contact their providers.
- In the future, we will have devices monitoring doctor-patient interactions, suggesting treatment approaches, or even alerting caregivers to voice changes that could be a sign of a health issue.

Examples of the Technological Change

- Slack claims it is “HIPAA Compliant” and is encouraging providers to share PHI on its platform
- In New York, Northwell Health is preparing to put Alexa in private rooms next month to allow patients to tap into their medical records.
- Mayo Clinic is using voice to deliver wound care instructions to some surgical patients and is studying the ability to diagnose cardiovascular disease and other conditions from patient’s voices.
- A large number of startups are developing voice technology to use in senior care, patient-provider communications, physician notes, and diagnostics.

VEVA, But in Nashville, Not Las Vegas

- Vanderbilt University Medical Center has developed a voice assistant for Electronic Health Records that can give verbal summaries back to providers using natural language processing.
- With VEVA, the Vanderbilt EHR voice assistant, the health system is using it help interpret voice requests, and pull pertinent data and provide relevant summaries.
- VEVA also may have some medication ordering functionality in future releases.

FOLEY HOAG LLP

The Legal Issues

- Technology has advanced dramatically, but the rules remains the same.
- The federal rules regarding patient communications are, at best, from 1996 and 2001. State rules are older than that.
- This results in a misalignment of rules and practice, with resulting confusion among providers, as well as risks that are growing. As a result, health privacy law may pose some obstacles to widespread adoption of these technologies.
- We cannot solve this issue today, but we can understand it better and develop some tools for dealing with requests and requesting parties.

FOLEY HOAG LLP

Some Basic and As Yet Unanswered Questions

- How does the device know it's the health care provider's voice?
- How does the device know it's the patient's voice?
- How does voice-guided care work in semi-private rooms?
- How does voice-guided care work when the patient doesn't want visitors to know his/her condition?
- Are conversations being recorded?
  - If is, when?
  - Can recording be turned off?
  - Who knows when the device is recording or not?

The Massachusetts Rules: Doctor-Patient Confidentiality

- There is no specific state confidentiality law that applies to physicians.
- However, Massachusetts courts have recognized a duty of confidentiality that all doctors in the Commonwealth owe to their patients.
- Physicians generally must not disclose a patient's health information without the patient's written consent, subject to limited exceptions (such as to meet a serious danger to the patient or to others or pursuant to a court order). ***Alberts v. Devine, 395 Mass. 59, 68 (1985)***.

Massachusetts Rules: Right to Privacy

- The Massachusetts Right of Privacy Act guarantees individuals the right to be secure from "unreasonable, substantial, or serious interference" with their privacy (*MA Gen. Laws Ch. 214 Sec. 1B*).
- In determining whether an employer has violated the Privacy Act, courts balance the employer's legitimate business interest against the substantiality of the intrusion on the employee's privacy (*Gauthier v. Police Comm'r of Boston, 408 Mass. 335 (1990)*).
- State law also prohibits the use of a person's "name, portrait, or picture" for purposes of trade without the person's written consent (*MA Gen. Laws Ch. 214 Sec. 3A*).

The Massachusetts Rules: Eavesdropping

- In Massachusetts it is illegal to willfully intercept, attempt to intercept or have someone else intercept on one's behalf any wire or oral communication. To intercept is "to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication."
- Punishment is a fine of up to $10,000, up to five years in state prison or both, or two and a half years in a jail or house of correction.

HIPAA

- The basic elements of HIPAA apply to any new technology.
- Go back to basics: What is "Protected Health Information"? **45 CFR 160.103:** Protected health information means individually identifiable health information … that is:
  (i) Transmitted by electronic media;
  (ii) Maintained in electronic media; or
  (iii) Transmitted or maintained in any other form or medium.
- Unanswered questions:
  - What about patient consent?
  - Are Amazon/Google/etc. going to be HIPAA business associates?
  - How do you do the necessary risk analysis?

HIPAA: Some Suggestions

- These systems must have the appropriate technical, physical, and administrative safeguards in place to protect the confidentiality, integrity, and availability of the ePHI involved.
  - Who is going to determine this?
- Until the BAA issue can be resolved, HIPAA-covered entities shouldn't consider using digital assistants for any functions or commands that will involve PHI.
- Even with a BAA, consider screening patients (e.g., avoid mental health and substance abuse settings)
- Consider whether/when to obtain patient consent.

HHS OCR Guidance

Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

Answer:

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.
- In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

https://www.hhs.gov/hipaa/for-professionals/faq/196/can-health-care-providers-have-confidential-conversations/index.html

HHS OCR Guidance

Does the Security Rule apply to written and oral communications?

Answer:

No. The standards and specifications of the Security Rule are specific to electronic protected health information (e-PHI). It should be noted however that e-PHI also includes telephone voice response and fax back systems because they can be used as input and output devices for electronic information systems. E-PHI does not include paper-to-paper faxes or video teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission. In contrast, the requirements of the Privacy Rule apply to all forms of PHI, including written and oral.

https://www.hhs.gov/hipaa/for-professionals/faq/2010/does-the-security-rule-apply-to-written-and-oral-communications/index.html

HHS OCR Guidance

Does the HIPAA Privacy Rule permit a doctor, laboratory, or other health care provider to share patient health information for treatment purposes by fax, e-mail, or over the phone?

Answer:

Yes. The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise.

For example:

- A laboratory may fax, or communicate over the phone, a patient's medical test results to a physician.
- A physician may mail or fax a copy of a patient's medical record to a specialist who intends to treat the patient.
- A hospital may fax a patient's health care instructions to a nursing home to which the patient is to be transferred.
- A doctor may discuss a patient's condition over the phone with an emergency room physician who is providing the patient with emergency care.
- A doctor may orally discuss a patient's treatment regimen with a nurse who will be involved in the patient's care.
- A physician may consult with another physician by e-mail about a patient's condition.
- A hospital may share an organ donor's medical information with another hospital treating the organ recipient.
- The Privacy Rule requires that covered health care providers apply reasonable safeguards when making these communications to protect the information from inappropriate use or disclosure. These safeguards may vary depending on the mode of communication used. For example, when faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard may involve a provider first confirming the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information. When discussing patient health information orally with another provider in proximity of others, a doctor may be able to reasonably safeguard the information by lowering his or her voice.

Date Created: 11/03/2003 https://www.hhs.gov/hipaa/for-professionals/faq/482/does-hipaa-permit-a-doctor-to-share-patient-information-for-treatment-over-the-phone/index.html

FOLEY HOAG LLP

Questions?

Thank you.

Colin Zick

Partner, *Co-Chair, Health Care Practice and Privacy & Data Security Practice*
Foley Hoag LLP

czick@foleyhoag.com | 617.832.1275

Jeremy Meisinger

Associate, Health Care Practice and Privacy & Data Security Practice
Foley Hoag LLP

jmeisinger@foleyhoag.com | 617.832.3029