FOLEY HOAG LLP

Driving Business Advantage

Protecting Health Information: Health Data Security Training

How to secure patient information and manage your obligations under HIPAA, the HITECH Act and other federal and state data privacy and security laws

October 25, 2012

Colin J. Zick
Foley Hoag LLP
(617) 832-1275
czick@foleyhoag.com
www.securityprivacyandthelaw.com

FOLEY HOAG LLP
Driving Business Advantage

Health Information Privacy and Security: Why Should It Be a Priority?

- **More federal and state laws, increasing penalties**
- **Theft of consumer information increasing, resulting in:**
  - Attorney General investigations and settlements;
  - private consumer litigation;
  - harm to patients; and
  - harm to businesses and their reputations.
- **Recent enforcement actions of note:**
  - South Shore Hospital by the Massachusetts Attorney General's Office; and
  - MEEI by HHS Office of Civil Rights.

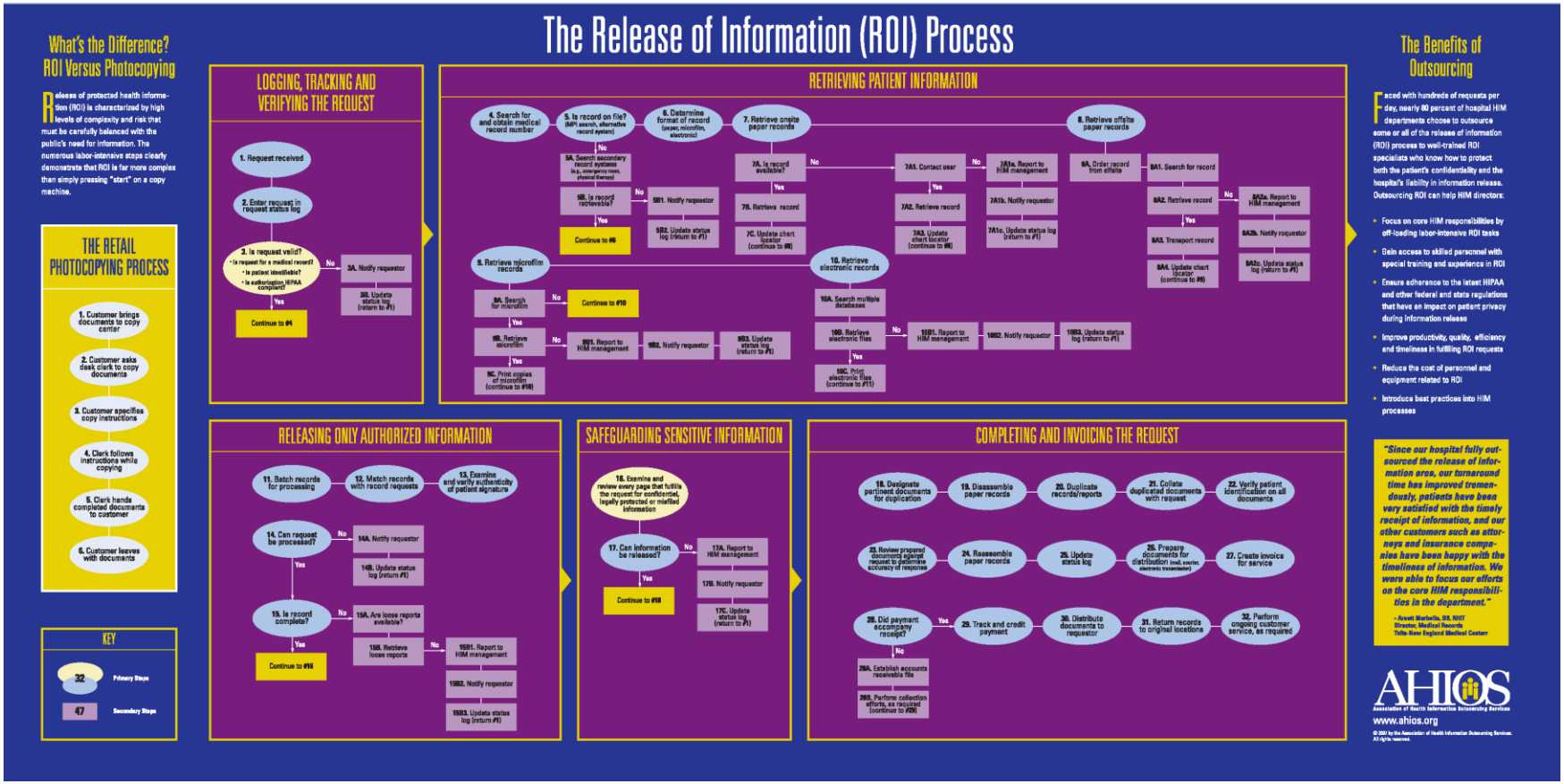
FOLEY HOAG LLP
Driving Business Advantage

Overview: What are the issues?

- Changing regulatory and technological environment
- Old issues:
  - –Subpoenas
  - –Patient requests for information
- New Technologies and Issues:
  - –EHRs
  - –Mobile devices
  - –Cloud computing
  - –Government audits and enforcement actions

FOLEY HOAG LLP
Driving Business Advantage

Release of Information Can Be Complicated!



FOLEY HOAG LLP
Driving Business Advantage

Basic Questions:

- What is the “patient record”?
- Who owns/controls the “patient record”?
  - Does it matter it is paper or EHR
- When do you have to consider releasing or providing access to the patient record?
- What parts of the record should you release?
  - What requires higher level authorization to release?
- Who should you tell before you release the record?
- Where can the record go?
- How should it get there?

FOLEY HOAG LLP
Driving Business Advantage

What is the "Record"?

- "Medical record" is poorly or not defined under state law (*e.g.*, correspondence, films, etc.)
- "Designated record set" includes the following information regarding care decisions:
  - Medical records
  - Billing records
  - Claims information
- These may be kept in different places, on different media.

FOLEY HOAG LLP
Driving Business Advantage

Categories of Record Requests

- Civil *versus* criminal requests for information:
  - Subpoenas versus Summonses
    - Attorney-issued versus Court-issued
    - Constitutional rights of the accused versus privacy rights.
  - Requests for production of documents
  - Requests with patient authorization
  - Civil investigative demands
- In all of these types of requests:
  - HIPAA applies
  - State confidentiality and privilege rules apply
  - Read the request and provide only what is requested.

FOLEY HOAG LLP
Driving Business Advantage

Subpoena Basics:

- Subpoenas come in many shapes and sizes.
- The response analysis changes based upon the type of subpoena:
  - Federal/State
  - Civil/Criminal
  - Investigative/Administrative
- HIPAA is a set of minimum privacy standards. As such, it generally pre-empts state law and state subpoena rules.
- However, where state law privacy protections for health information are "more stringent" than a HIPAA protection, the state protection should still govern. 45 C.F.R. § 160.203(b).

FOLEY HOAG LLP
Driving Business Advantage

What Else Does HIPAA Say About Subpoenas?

- HIPAA permits disclosure without patient authorization:
  - pursuant to a "subpoena, discovery request, or other lawful process" *provided* the covered entity receives certain "satisfactory assurances" from the requesting party (either that efforts have been made to notify the subject individual or to obtain a protective order meeting certain criteria); or
  - on the order of court or administrative tribunal, provided that the covered entity discloses only the PHI expressly authorized by such order. 45 C.F.R. § 164.512(e).

FOLEY HOAG LLP
Driving Business Advantage

The New World: EHRs

- Increase of amount of access exponentially and therefore the risk of improper access.
  - You and your staff have more access to other records; and
  - Others have access to your records.
- Look for/impose levels of access tied to job responsibilities
- Maintain audit trails and periodic reviews of use.
- Do not share/loan passwords
- Change passwords frequently
- Use strong passwords (and don't write them down where they are easily found)

FOLEY HOAG LLP
Driving Business Advantage

The New World: Mobile Devices and Laptops

- Increase ease of access, but also risk of loss.
  - Familiarity breeds contempt.
- Need to know what's on what and in what form.
- Need to know who has what and that use is authorized.
- Protect the devices against loss or improper access:
  - password protected;
  - data encrypted; and
  - "Lojack" or other means of retrieval/securing if lost or stolen.

FOLEY HOAG LLP
Driving Business Advantage

The New World: The Cloud

- What do we mean by “the Cloud”?
- Elements of cloud computing:
  - Cheap storage
  - Easy access
    - Too easy?
  - Security: the cloud could itself is relatively secure
    - The issue is how you use it and for what.
  - It is not for most practices to do-it-yourself with health information.
- Contracts are complicated, can be difficult to negotiate.

FOLEY HOAG LLP
Driving Business Advantage

Practices in Transition

- A generation of physicians is retiring and practices are consolidating.
  - Their records are primarily paper records.
- Professional obligations require that physicians find a home for some of their records, others can be destroyed.
  - No one wants to pay for this.
  - Need to plan now for this eventuality.
- Some practices are willing to take records as a means of securing new patients.
  - This creates transition issues, as acquiring practices often have EHRs;
  - Who pays the cost of bringing paper records into the EHR?

FOLEY HOAG LLP
Driving Business Advantage

The Number and Size of Breaches Continues to Rise

- OCR posts on its website a list of HIPAA "covered entities" that have reported breaches of unsecured health information affecting more than 500 individuals. OCR's posting showed 500 health data breaches that impacted over millions of individuals.
- This posting by OCR was required by the August 2009 Interim Final Rule, which was issued pursuant to the HITECH Act. In particular, § 164.408 of this breach notification interim final rule implements § 13402(e)(3) of the HITECH Act. The rule became effective September 23, 2009.
- Under this rule, breaches that affected 500 or more individuals must be reported to OCR within 60 days, via an OCR online notification form. Training materials and related guidance on breach notification can be found on the OCR web site.

FOLEY HOAG LLP
Driving Business Advantage

Common Data Breach Scenarios

- Unintentional Breaches
- Faithless Employee/Ex-Employee
- Hackers & Thieves / Organized Crime
- Competitive Espionage

FOLEY HOAG LLP
Driving Business Advantage

Preparing for and Responding to a Breach

- Compliance / developing information security programs
- Incident response and investigation
- Breach notification and resolution
- Litigation
- Government Investigation

FOLEY HOAG LLP
Driving Business Advantage

Federal HIPAA Settlements and Penalties

- Resolution Agreement with Providence Health & Services--July 16, 2008: $100,000
- Resolution Agreement with CVS Pharmacy, Inc.--January 16, 2009: $2.25 million
- Resolution Agreement with Rite Aid Corporation--July 27, 2010: $1 million
- Resolution Agreement with Management Services Organization Washington, Inc.--December 13, 2010: $35,000
- Civil Money Penalty issued to Cignet Health of Prince George's County, MD--February 4, 2011: $4.3 million
- Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, Inc.--February 14, 2011: $1 million
- Resolution Agreement with Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc.—October 2012: $1.5 million

FOLEY HOAG LLP
Driving Business Advantage

Colin J. Zick is a partner in Foley Hoag LLP's Administrative and Litigation practice groups. His work has had a particular emphasis on compliance issues related to pharmaceutical and medical device companies. This compliance work includes helping clients establish and maintain effective compliance programs. He counsels clients on issues involving information privacy and security including HIPAA, state and federal data security laws, and the FTC Red Flag Rules and blogs on these issues at www.securityprivacyandthelaw.com.

Colin also defends clients in disputes alleging kickbacks, overpayments, and billing and coding problems, and represents clients before various state health care licensing and regulatory entities. Colin serves as the North America Regional Vice-Chair of the Lex Mundi Health Care Industries Practice Group and Co-Chair of the Boston Bar Association's Health Law Section. He has been ranked by CHAMBERS USA as one of Massachusetts' leading health care lawyers and selected by his peers as a Massachusetts "Super Lawyer" from 2004 through 2012. He can be reached at (617) 832-1275, czick@foleyhoag.com.