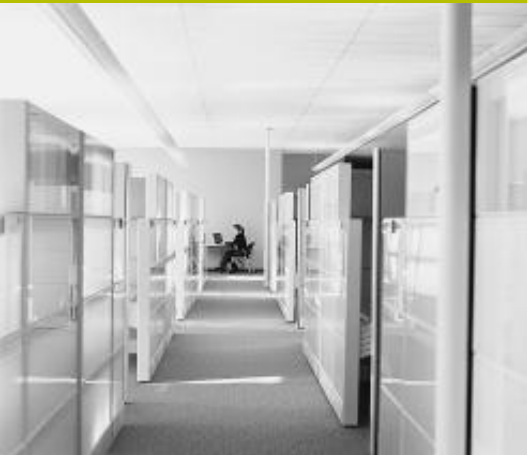




Release of Health Information Update



Massachusetts Health Information
Management Association
Dot Wagg Memorial Seminar

November 9, 2012

Colin J. Zick
Foley Hoag LLP
(617) 832-1275

czick@foleyhoag.com

www.foleyhoag.com

www.securityprivacyandthelaw.com

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

Release of Information Can Be Complicated!

What's the Difference? ROI Versus Photocopying

Release of protected health information (ROI) is characterized by high levels of complexity and risk that must be carefully balanced with the public's need for information. The numerous labor-intensive steps clearly demonstrate that ROI is far more complex than simply pressing "start" on a copy machine.

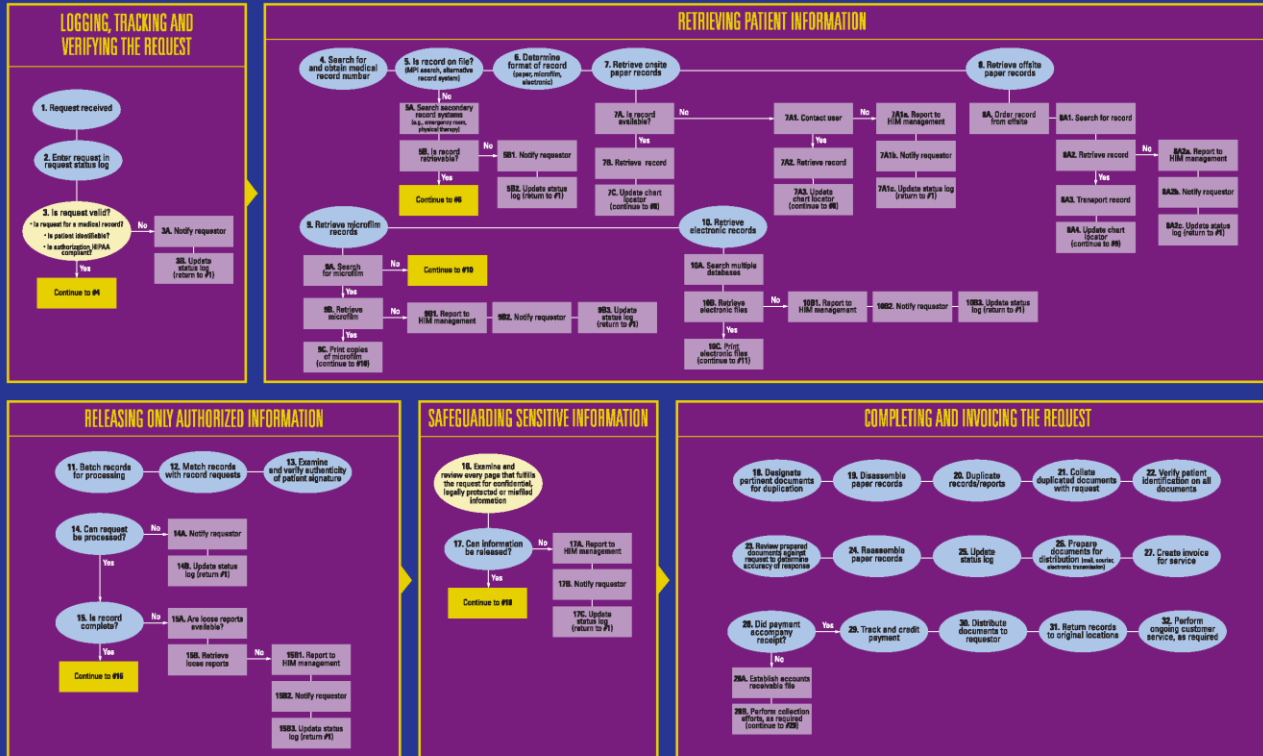
THE RETAIL PHOTOCOPYING PROCESS

1. Customer brings documents to copy center
2. Customer asks clerk to copy documents
3. Customer specifies copy instructions
4. Clerk follows instructions while copying
5. Clerk hands completed documents to customer
6. Customer leaves with documents

KEY

- 32 Primary Step
- 47 Secondary Step

The Release of Information (ROI) Process



The Benefits of Outsourcing

Faced with hundreds of requests per day, nearly 80 percent of hospital HIM departments choose to outsource some or all of the release of information (ROI) process to well-trained ROI specialists who know how to protect both the patient's confidentiality and the hospital's liability in information release. Outsourcing ROI can help HIM directors:

- Focus on core HIM responsibilities by off-loading labor-intensive ROI tasks
- Gain access to skilled personnel with special training and experience in ROI
- Ensure adherence to the latest HIPAA and other federal and state regulations that have an impact on patient privacy during information release
- Improve productivity, quality, efficiency and timeliness in fulfilling ROI requests
- Reduce the cost of personnel and equipment related to ROI
- Introduce best practices into HIM processes

"Since our hospital fully outsourced the release of information area, our turnaround time has improved tremendously, patients have been very satisfied with the timely receipt of information, and our other customers such as attorneys and insurance companies have been happy with the timeliness of information. We were able to focus our efforts on the core HIM responsibilities in the department."

- Anne Marrella, RHIT
Director, Medical Records
Tulsa State Medical Center

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?

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

What Matters for Release of Records:

- Look at the request and see what is being requested.
- Rarely will just “records” be requested (and almost never “designated record set”).
- “Correspondence” and other things that you would not consider part of the official “record” will likely be included in the request.

Common 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

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

Subpoena Basics (cont.):

- Rule 45 of the Federal and State Rules of Civil Procedure sets out the manner in which subpoenas are served and responded to.
- Both the federal and state rules generally make allowance for the party served with the subpoena to serve a written objection upon the party serving the subpoena and thereby forestall the necessity for producing documents. This may not be true for administrative subpoenas.

HIPAA, Subpoenas and Pre-emption

- 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).

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).

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)

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.

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.

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?

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](#).

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

Massachusetts State Actions Under the Data Security Law

- Briar Group LLC – 125,000 credit card numbers
 - \$110K penalty
- Belmont Savings Bank – 13,000 bank account numbers
 - \$7,500 penalty
- Maloney Properties – 600 customer Social Security numbers
 - \$15,000 penalty
- South Shore Hospital – 800,000 patients' data
 - \$750,000 penalty

SOURCE: MASSACHUSETTS OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION

Data Breach Notifications (Nov. 2007 – Nov. 2011)

- Total data breach notifications: 1,833
- Residents in Massachusetts affected: 3,166,031
- Residents protected by encryption: 11,367
- Residents protected *if* portable devices were encrypted: 1,490,308

SOURCE: MASSACHUSETTS OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION

Resources

- HHS OCR: <http://www.hhs.gov/ocr/privacy>
- Massachusetts Attorney General:
<http://www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/>
- Massachusetts Office of Consumer Affairs and Business Regulation
<http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf>
- Our blog: <http://www.securityprivacyandthelaw.com>

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 health care providers, as well as 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, and state and federal data privacy and security laws and blogs on them 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 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" since 2004.

Colin can be reached at (617) 832-1275, czick@foleyhoag.com.