Grab Bag: Electronic Health Records and What Should Keep You Up at Night

Briar Andresen, Katie Ilten & Jim Platt

February 2015

Fredrikson & BYRON, P.A.

Overview

- Surveys
- CoPs and Privacy and Security
- Interoperability
- Meaningful Use payments
- Malpractice
- Scribes
- EHR contracting
- Ownership of info
- Passwords
- Patient portals
- Departing practitioners
- Questions

EHR and Surveys

- Review CMS 2009 memo: “Surveying Facilities That Use Electronic Health Records”
- http://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/downloads/SCLetter09_53.pdf

Provider/Supplier Responsibilities

"[A] provider must grant access to any medical record, including access to EHRs, when requested by the surveyor. If access to an EHR is requested by the surveyor, the facility will (a) **provide the surveyor with a tutorial** on how to use its particular electronic system and (b) **designate an individual who will**, when requested by the surveyor, access the system, **respond to any questions or assist the surveyor** as needed in accessing electronic information in a timely fashion. . . .

Provider/Supplier Responsibilities

. . . . **If the facility is unable to provide direct print capability** to the surveyor, the **provider must make available a printout of any record** or part of a record upon request in a timeframe that does not impede the survey process. . . . Whenever possible, the facility must provide surveyors electronic access to records in a **read-only format** or other secure format to avoid any inadvertent changes to the record. . . .

Surveyor's Responsibilities

. . . . **Electronic access to records will not eliminate the need for a surveyor to print a paper copy** or to request a paper copy of certain parts of certain records. However, the surveyor shall make reasonable efforts to avoid, where possible, the printing of entire records. The surveyor should print or request a paper copy of only those parts of records that are needed to support findings of noncompliance. . . .

Other issues and tips

- What does the EHR include?
- Shortcuts
- Printed versus “live” view
- Keep a copy of printed records provided
- Quality review and incident reports
- Outsider’s view of alerts and terminology

Privacy and Security

Surveyors are not responsible for assessing compliance with the HIPAA Privacy and Security Rules. . . . **Surveyors instead are to focus on how the EHR system is being used in the facility, and whether that use is consistent with the Medicare CoPs or CfCs**.

Privacy and Security

For example, are **computer screens** showing clinical record information **left unattended** and readily observable or accessible by other patients/residents or visitors? Are there documents **publicly posting passwords**, which would be evidence of noncompliance with both confidentiality and medical record authentication requirements? Is there evidence to support a complaint allegation that facility **staff shared information obtained from an EHR with unauthorized individuals**?

Privacy and Security

Likewise, when an SA has concerns that a provider or supplier EHR system may not be in compliance with the HIPAA Security Rule, the **SA has the discretion to file a complaint with the CMS Office of eHealth Standards and Services** or OCR**.**

What's this about interoperability?

- Office of the National Coordinator for Health IT
- Draft report released with 2017 deadline by which "a majority of individuals and providers across the care continuum" should be able "to send, receive, find and use a common set of electronic clinical information."

Meaningful Use Payments

- Payment is made to the eligible professional.
  - 42 CFR 495.10(f)(3) “Each EP may reassign the entire amount of the incentive payment to only one employer or entity.”
  - Specific to Meaningful Use, or does general assignment language work?

CMS commentary

"CMS views the assignment process as primarily a contractual issue between the employer and employee. . . . [I]f the EP wishes to reassign his or her incentive payment to the employer or entity with which the EP has a contractual arrangement, the parties should review their existing contract(s) to determine whether the contract(s) currently provides for reassignment of the incentive payment or if the contract(s) needs to be revised." 75 Fed. Reg. 44446 (July 28, 2010)

Departing practitioners

- EP moves to another practice after a reporting year.
- EP splits a reporting year between two practices.
- EPs must maintain documentation for six years. 42 C.F.R. 495.8(c)(2)
  - Preamble says 10 years from the date of registration.

EHRs and Malpractice

- Cut and paste
- Password sharing
- Alerts
- No physician signature
- Printed copies
- Corrections

Use of Medical Scribes

- Increasingly popular
- Common uses
- Legal issues
  - Patient privacy and HIPAA
  - Joint Commission requirements
  - CMS requirements

CMS Requirements

- 42 CFR 482.24(c)(1) (Conditions of Participation for Hospitals)
    - "(1) All patient medical record entries must be legible, complete, dated, timed, and authenticated in written or electronic form by the person responsible for providing or evaluating the service provided, consistent with hospital policies and procedures."
- Similar requirements for other providers (e.g., hospice, home health)

CMS Requirements –Cont'd

- Social Security Act 1862(a)(1)(A):
  - All billed services must be based only on activities that are reasonable and necessary for the diagnosis or treatment of illness or injury.
- Program Integrity Manual, Chapter 3, Section 3.4.1.2:
  - CMS can request records for review to make a prepayment or postpayment claim review determination.
- Change Request 6698 - - Signature Requirements for Medical Review Purposes

Examples of Electronic Signatures

- 'Electronically signed by' with provider's name
- 'Released by' with provider's name
- 'Signed by' with provider's name
- 'Signed: John Smith, M.D.' with provider's name
- •Digitized signature: Handwritten and scanned into the computer
- •'This is an electronically verified report by John Smith, M.D.'
- •'Authenticated by John Smith, M.D'
- •'Closed by' with provider's name
- •'Finalized by' with provider's name
- •'Electronically approved by' with provider's name
- •'Signature Derived from Controlled Access Password'

Medical Scribes and Electronic Signatures

- Records that are dictated and/or transcribed, but do not include valid signatures 'finalizing and approving' the documents will result in denial of claims.
- If the signature requirements are not met, carrier will contact the person or organization that submitted the claim(s) and ask him/her to submit an attestation statement or signature log.
- Attestation statements may not be signed by someone other than the author of the medical record entry in question (even in cases where two individuals are in the same group, one should not sign for the other in medical record entries or attestation statements)

Medical Scribes and Electronic Signatures – Cont'd

- Opening the patient record: under whose name and password?
- Physician dictates the encounter to the scribe who enters it in the record; identifiable as being entered by the scribe?
- At the close of the encounter, does the physician review and electronically sign?

Other Pitfalls to Consider

- Who can make minor corrections to the EHR (e.g., typos)? Does the EHR provide a trail?
- Do you allow others to close an encounter for a physician who is absent (e.g., on vacation)?
- What about corrections made by the billing office? Or can they “view only?”
- Communicating with patients on patient portals?
- Internal communications with scribes that contain PHI on secure email?

Medical Scribe Policy

- Some elements to include:
  - Who can serve as a scribe?
  - Training
  - Patient privacy
  - Use of passwords, i.d. numbers
- Employ your own or contract with others?
  - Indemnification clauses
  - HR, tax and benefit considerations

Selecting a vendor

- Selection committee
- What are your functional requirements?
- What are your technical requirements?
- Pricing
- Cloud-based vs. installed software
- Security
- Will you use a bidding or RFP process?
- Select at least 2 finalists

Elements of an IT contract

- Quote/Proposal with pricing, modules and schedule
- Software license or service terms and conditions
- Maintenance and support terms and conditions
- Statement of work outlining implementation, conversion, customizations, training, etc.
- Service Level Agreement
- Business Associate Agreement

EHR contracting—on the front end

- Defining the “Product” or “Software”—what are you buying?
  - Functionality promises made in the sales process should be reflected in the agreement
  - Incorporate RFP responses, key sales materials, demonstration materials or other vendor responses (“Documentation”)
  - Vendor will maintain the software so that it has the functionality to establish/maintain “meaningful use”

EHR contracting issues

- Warranties
  - Perform per “Documentation”
  - Comply with laws and regulations
  - Non-infringement
  - Services will be provided in a professional and workmanlike manner
  - Vendor will diligently work with third party database vendors

EHR contracting issues

Payment

- Tie upfront payments to milestones and hold a portion until after Go Live
- Annual/monthly fees start on Go Live, not contract signing
- Cap the annual increases to maintenance or subscription
- How are fees calculated? Pay attention to definition of “user,” “transaction,” “claims,” etc.
- Ask about future pricing for additional users, new locations, new modules

EHR contracting issues

- Termination
- Security/BAA
- Indemnification/limits on liability
  - Make mutual!

Key provisions in health IT contracts

- Support and maintenance
  - Meaningful Use updates and other enhancements included in support fees
- Service levels
  - System up-time and response time
  - Support response and resolution time
  - Credits for failure
  - Ability to terminate for repeated SLA failures

EHR contracting issues

- During the contract period
  - Document issues/problems
  - If there hasn't been a breach, what are other termination options?
  - Transition of system

Medical record issues

- Who “owns” information (in a shared system)?
- How will “ownership” be tracked?
- Which party (in a shared system) is responsible for making disclosures and complying with requests?
  - Breach of one organization’s info by another organization with access—who reports? Who notifies?

SplashData's "Worst Passwords of 2014":

1 123456
2 password
3 12345
4 12345678
5 qwerty
6 123456789)
7 1234
8 baseball
9 dragon
10 football
11 1234567
12 monkey
13 letmein
14 abc123
15 111111
16 mustang
17 access
18 shadow
19 master
20 michael
21 superman
22 696969
23 123123
24 batman
25 trustno1

Passwords

- Sharing them—generally a bad idea*
- Changing them—generally a good idea
- Other password issues passwords
  - Vendors?
  - Payors?
  - Do they really need access?
    - Minimum necessary!

Patient portals

- One study said that patient online access to EHRs went from 25% in 2011 to 50% in 2014.
- Patients want to
  - Email health care professionals
  - Review treatment plans
  - See doctors' notes and test results
  - Schedule appointments
  - Submit refill requests

Patient portals

- Is this the same as HIPAA access?
- May the patient portal include access to records other than the health care organization providing the portal?

Patient portals and minors

- A sticky wicket with parental access
- State laws require privacy with certain types of medical information of minors
  - Sex, pregnancy, drug and alcohol issues
- Options
  - Age limits for parental access—patients above X age get own passwords?
  - Don't put restricted info on portal—but what does that include?

When providers leave

- Closing their charts
  - Report to NPDB?
  - “a failure to complete medical records is related to a physician’s professional competence or conduct and almost always has the potential to adversely affect a patient’s health or welfare.”
  - Not all suspensions reportable, but repeated offenses and/or lengthy time lapses.

Questions?

Briar Andresen
612.492.7057
bandresen@fredlaw.com

Jim Platt
612.492.7047
jplatt@fredlaw.com

Katie Ilten
612.482.7428
kilten@fredlaw.com