CT AAP HIPAA/HITECH Follow Up To Training Sessions September 24, 2013

Presentation by:

Jennifer L. Cox, J.D.

Cox & Osowiecki, LLC

Hartford, Connecticut

Today's Program

- Housekeeping about the manual:
  - Amending the manual
  - Best practice for keeping manual current
  - **Clarifying patient directed release versus authorization form**
  - **CT AAP is working on having the NOPP translated into Spanish**
- New guidance from OCR on specific topics
- Review questions from attendees, covering a variety of topics

Manual Use and Details

- Word document format on the flash drive. You should be able to revise the policies and forms to put your logo or information on them, or customize as you wish
  - Jen Cox made spelling errors on NOPP, meaning and content not affected, but you may want to revise
- Authorization form is substantially similar to old form, you can use your old authorization if you wish

Manual Use and Details

- The policy manual should be kept in a location where workforce are allowed to review it, but not patients. You can keep it electronically if you choose.
  - It is your documentation for compliance
  - You must keep prior policies on file for at least 6 years (administrative materials)
- If there is ever a HIPAA investigation or audit, OCR always asks for ALL HIPAA policies and materials, including proof of employees' HIPAA training, be sent within 10 days

Patient Directed Release Versus Authorization For Release

Manual contains two different policies about patient agreeing to release records:

- *Authorization for the Use/Disclosure of PHI Determination – When Required*
  - Appendix D form, Authorization for Release goes with this policy, follows **Privacy Rule Section 164.508**
- *Access to Records and PHI & Patient Access to Electronic Copies*
  - Appendix G form, Patient Directed Release of Records Directly to Patient or to a Designated Person, goes with this policy, follows **Privacy Rule Section 164.524**

Patient Directed Requests

- HIPAA has never required a patient to sign for release of records to himself/herself, but best practice is to have some sort of documentation
- Providers historically used "authorization" form (164.508)
- **New e-copy rules:** OCR states that there is a gap between 164.58 and 164.524, and the result is you cannot use regular authorization when patient directs you to send an electronic copy to a third person (must follow 164.524)
  - Appendix G form solves this gap
  - **You may continue to use the Appendix D authorization for anything other than patient requesting e-copy be sent to a designated person**
  - **You may also use any written form you devise to effect patient directed transfer of records as long as it contains the patient's signature, and clearly identifies the person designated by the patient to receive the PHI, and where to send it**
- **Caution – e-copy rights and the copy fee restriction applies to all patient directed access, as discusses in the Access policy!!!**

OCR Updates and Keeping the Manual Current

- Need to check the OCR HIPAA web site frequently www.hhs.gov/ocr/privacy/
- OCR is starting to issue more guidance (really late, but perhaps better than not at all)
- Five (5) new pieces of guidance since September 13th
- For the balance of 2013, check at least once a week

Health Information Privacy

HIPAA
- Understanding HIPAA Privacy
- HIPAA Administrative Simplification Statute and Rules
- Enforcement Activities & Results
- How to File a Complaint
- News Archive
- Frequently Asked Questions

PSQIA
- Understanding PSQIA Confidentiality
- PSQIA Statute & Rule
- Enforcement Activities & Results
- How to File a Complaint

Health Information Privacy

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules

Learn about the Rules' protection of individually identifiable health information, the rights granted to individuals, breach notification requirements, OCR's enforcement activities, and how to file a complaint with OCR.

The Patient Safety and Quality Improvement Act of 2005 (PSQIA) Patient Safety Rule

Learn about the Patient Safety Rule's protection of confidential patient safety work product, the permitted disclosures of patient safety work product, OCR's enforcement activities, and how to file a complaint

What's New

- NPP Enforcement Delay for CLIA Labs - 9/19/13
- New Guidance on Marketing: Refill Reminders - 9/19/13
- New Guidance on Decedents - 9/19/13
- New Guidance on Student Immunizations - 9/19/13
- HHS Issues Model Notices of Privacy Practices - 9/13/13
- Patient Safety Inflation Adjustment Notice - 9/10/13
- Unofficial Combined Regulation Text - 6/11/13
- Conference on *Safeguarding Health Information: Building Assurance through HIPAA Security*, May 21st & 22nd, 2013 - 2/26/13
- Sample Business Associate Agreement – 1/25/13
- Omnibus HIPAA Rulemaking – 1/17/13
- HHS issues letter to providers on disclosures to avert threats to health or safety – 1/15/13

News

- HHS Settles with Health Plan in Photocopier Breach Case
- WellPoint Settles HIPAA Security Case for $1,700,000
- Shasta Regional Medical

Added Guidance Since September 13th

- NPP Enforcement Delay for CLIA Labs - 9/19/13
- New Guidance on Marketing: Refill Reminders - 9/19/13
- New Guidance on Decedents - 9/19/13
- New Guidance on Student Immunizations - 9/19/13
- HHS Issues Model Notices of Privacy Practices - 9/13/13

Submitted Questions

- Excellent Follow Up Questions Received!!

Type of Questions Covered In This Webinar

- School nurse and immunization records
- Acknowledgment and Notice of Privacy Practices
- General Questions, including:
  - What is new in HIPAA, faxing, documenting training, voicemail and answering machines, mailing certified or regular post, patient copy fees, and rights to copy,
  - Technology, smart phones, cell phones and encryption
- Breach Rule compliance
- Business Associates and BAAs
- Out-of-Pocket, Restriction of Info to Payers

School Nurses & Immunizations

- Since 2003, HIPAA Privacy has prohibited a provider/practice from disclosing immunization info directly to school nurse without WRITTEN parental permission
  - Parental permission could be 164.508 authorization
  - Blue form could work, if in date and signed
- "Feels illogical because immunization is disclosed to the DPH system, why not school nurse…" the system falls under a different HIPAA rule!!
- New rule relaxes the old rule, now the parental permission can be verbal (must come directly from the parent)
- Practice must still document the permission

Q: Where is this discussed in the manual?

A: In the *Authorization for the Use/Disclosure of PHI Determination – When Required* policy

Acknowledgment of Patient Being Offered NOPP

- Upon first visit, patient must be presented with the NOPP and the acknowledgment process completed
- Never needs to be redone, even if you revise (you must start using the new version for wall posting and website link)
- Manual, Appendix B contains a form to capture the required "acknowledgment"
  - Discussed in policy *Acknowledgment of Notice of Privacy Practices*
- This process has to be done *exactly* to meet the rule – which is how the form and policy are designed

45 CFR 164.520: Acknowledgment Process

Provider must (except in medical emergencies):

> "…make a good faith effort to obtain a written **acknowledgment** of receipt of the [NOPP]…and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained…"

- Q: Should I make a checkbox for the patient to say he/she declined the copy? Can it be on the intake/registration form.
- A: The patient should not be asked to sign off on the refusal. The mandated rule is to either obtain the patient's signature for receipt of the NOPP – or, if the patient fails or refuses to sign, the practice documents it (as in the manual form). If you want to put the entire acknowledgment process on your intake form you could (not recommended, because office use part has to work, but permitted)

Acknowledgment & NOPP Rule Continued

Q: If I post a summary – is that enough?

A: No. If you post the summary (and not full version), the full version must be available for the taking – without the patient having to ask for it, even if patient has already been through the acknowledgment process.

Q: Where can I find summary version?

A: OCR website has a short version you can use as the summary – but it must be customized per the instruction on their website. Not in the manual (on purpose because it creates risk).

General Questions

Q: What is actually "NEW" for 2013?

A: Everything on the slideshow from training.

- (Manual has been updated for better compliance overall. But the minimum required changes are as described in the training slides.)

Q: Do I need to change fax cover sheets?

A: No. Paper faxing rules have not changed.

Q: Where do I document employee training?

A: You must document employee HIPAA training (not a new rule) and you can keep it anyplace. The manual provides space at Appendix **I**, but you can use any format you wish.

General Questions

Q: Can we leave voicemail/answering machine messages?

A: Yes, but you need to be careful to leave only limited information, such as contact info requesting call back or appointment time (not test or clinical results). If you intend to leave more detailed information, obtain written agreement from patient.

Q: When mailing records to another provider, do you need to send certified mail – and who pays for the copy?
A: No. There are no specific requirements on proving receipt when mailing records. The copy fee is the patient's responsibility, unless you have an agreement with the other practice.

General Questions - Copies

Q: Copy fees – do we really have to give patient copy of record w/in 30 days of request, even if they refuse to pay the fee?

A: Yes. If they owe the fee (e.g., private pay, not Medicaid patient), then you can put the copy charges in collection if they refuse to pay. But you must still provide the records (as many times as they ask).

- Applies to your entire record – regardless of who created the record (consultants, hospital, prior provider… if you keep the record, you have to produce copy, subject to release for HIV, mental health, substance abuse)
- Also see Manual, Access to Records and PHI & Patient Access to Electronic Copies for a discussion of cap on copy fees for e-copies

General Questions: Technology

Q: Cell phone has email or text data. Does that create an issue?

A: Yes, there is an issue. If an unencrypted device is stolen or lost, the failure to encrypt is a breach rule violation. Password protection is not sufficient to meet the encryption rules.

Q: What if the only info on the cell phone is ten digit phone number?

A: If the patient's phone number or email or contact info is there, the encryption rule applies. If it is just sending a call back number to the office or service – the rule would not apply.

- But note: the transmission of the call back number needs to be sent in a secure fashion. The phone knows who it dialed, emailed, or texted..

General Questions: Technology

Q: New phone system going in – what to consider?

A: Need to consider the same Privacy Rule and Security Rule issues for any digital media or system that will contain PHI

- Passwords
- Access and user rights
- Voicemail conversion to email

General Question: Returned Mail

Q: During training sessions, “bad mail” addresses and returned mail were mentioned. Please explain why this is important.

A: Two unrelated mail issues were referenced:

- (1) Returned mail after actual breach notice is mailed out, if you get 10+ bad ones back, you can work to get the number to 9 to avoid “substitute notice”
- (2) If the post office (or FedEx, etc.) loses your records in transit – you have to make a breach notification UNLESS they (USPS or the carrier) can explain why the PHI was destroyed, and could not have been seen by anyone (e.g., “eaten by the post office machines and totally destroyed”)
  - But if it is just gone or missing – you are responsible for the breach notification, **follow the breach investigation planning materials in the manual, Appendix E**

Breach Rule Baseline

A breach occurs upon acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule

Breach Related Questions – "Misfiled"

- Q: Practice is migrating from paper to EMR – scanned many records. Some errors in scanning, including Patient A's file erroneously contains parts of Patient B's file. Does a breach occur when practice discloses the Patient B materials to Patient A?
- A: Yes, that is subject to the breach notification rule. Use the Breach Investigation and Response Plan form to process.
  - Variation: Records sent to Patient A on disc, or in paper format, or over secure internet. Same answer.
  - Variation: portal access, but record was copied wrong, so patient logging in saw his records – but others as well. Same answer.
- Once you learn of this, you need to correct the records ASAP

Business Associate Changes

Changes are drastic

Business Associate Agreements

- New template, *Sample Business Associate Agreement Provisions* on OCR website:
- http://www.hhs.gov/ocr/privacy/

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Subcontractors

Q: Does practice have to ensure subcontractors sign a BAA with my BA?

A: No. The rule does not require a practice to check up on whether BA has a subcontractor BAA in place. Your ONLY obligation is to require, in the text of your BAA, that a BA pass on the obligations to its subcontractors.

Q: Camera store is a BA – but they send out some of the work – do they need to have a BAA with their subcontractors who receive the outsourced work?

A: If PHI is involved in the subcontractor's work, yes. The camera store needs a subcontractor BAA with its outsourced entities. If the work is done by another part of the same company, nothing additional is required.

Unwilling BAs

Q: What is best strategy for large vendors (Gateway, Amazon, McKesson) that insists on using their own BAA form?

A: You can use any BAA form as long as it contains the minimally required elements found in the new rule, chief among these the BA must follow the security rule (subpart C of part 164), the breach rule (164.410 and subpart D of part 164) and must pass-through its BA obligations to its subcontractors, in writing.

Q: What if the vendor insists that no new BAA is needed?

A: **Ask for their reasoning in writing (they could be right, but putting it in writing makes it more real).** Unfortunately, you might need a lawyer to intercede because there are many variables, and it can be hard to sort through.

Out-of-Pocket Restriction

Winner of the “rule least likely to succeed” contest

New Information From Medicaid

- DSS has informed CT AAP that the restriction **DOES NOT** apply to, and should not be extended to, Connecticut Medicaid patients
- DSS has also said, for Medicaid program patients:
  - No copy charges
  - No missed appt charges
  - This leaves questions
  - Bottom line: if you charge Medicaid patient any out of pocket fees, there is a risk that DSS believes it is not permitted

How to Process These Requests

Q: Are there examples of workflow to implement this rule?

A: It may be necessary to flag the entire patient chart if the restriction is requested/granted

- Too many variables (including insurance company audit) to have a one size fits all approach
- For EHR/EMR – seems impossible to do any way other than by flagging that person and the record for all time, and giving the patient special attention each visit
- Note: rule applies to Medicare patients, but Medicare might still require info for "audit" and program evaluation

Q&A

Happy to answer more