Updates from the Legislative and Regulatory Front

Kelly McLeodon, RHIA, CHPS
Managing Director
CompliancePro Solutions

Agenda

- HIPAA Privacy and Security Rule Expected Updates
- Substance Abuse Rule NPR
- Expansion of Enforcement
- Patient Access FAQ
- 2016 OCR Phase 2 Audits
- Phase 2 Audit Protocols
- Security Risk Analysis & Stage 3 Meaningful Use
- Hot Cases

OCR’s New Website

- OCR FAQs by topic, various sections of FAQs are being updated
- Easy to find enforcement actions too
- Part of new website, easier to navigate
- Section or Individuals and Professionals
HIPAA Privacy and Security Rule
Expected Updates

- New Accounting of Disclosure rules (with or without Access Reports)
- Financial penalties splitting with persons reporting for breach

HIPAA Privacy and Security Rule
Expected Updates

- Penalty (Fines) Sharing
  - (c) Distribution of Certain Civil Monetary Penalties Collected
    - (2) Within 18 months and then 3 years from enactment a person damaged by a violation can receive a % of the penalties.
    - HITECH in 2009 called for splitting penalties (fines) with the complainants
    - I believe these rules are being promulgated and expect to see them in 2015
    - If so, this is a game changer, the amount of HIPAA complaints may escalate dramatically and with that the requirements for documentation and potentials for missing something and having a violation increases

Substance Abuse Rule NPR
Confidentiality of Substance Use Disorder Patient Records – New NPR

- New Proposed Rule from SAMHSA
- Vetted for comments by AHIMA
- Need updates since last one was 1987
- SAMHSA wants to ensure that patients with substance use disorders have the ability to participate in, and benefit from new integrated health care models without fear of putting themselves at risk of adverse consequences
- SAMHSA strives to facilitate information exchange within new health care models while addressing the legitimate privacy concerns of patients seeking treatment for a substance use disorder. These concerns include: the potential for loss of employment, loss of housing, loss of child custody discrimination by medical professionals and insurers, arrest, prosecution, and incarceration

- Requires violations for methadone programs to be reported to FDA not SAMHSA
- Definitions reworded, consolidated, etc
- Applicability to whom the rule applies seems to widen and become more specific, but are not just ‘medical facilities’ they can be practices or any other program receiving Federal assistance for substance abuse treatment
- Patients who have included a general designation in the “To Whom” section of their consent form (see §2.31) must be provided a list of entities to which their information has been disclosed pursuant to the general designation
- Have in place formal policies and procedures addressing security, including sanitization of associated media, for both paper and electronic records

- 60 day comment period closed April 9, 2016
- Applicable 180 days after Final Rule publication Unsure of that date at this point
- This proposed rule would revise 42 CFR part 2, Confidentiality of Alcohol and Drug Abuse Patient Records regulations which protects the confidentiality of the identity, diagnosis, prognosis, or treatment of any patient records which are maintained in connection with the performance of any federally assisted program or activity relating to substance abuse education, prevention, training, treatment, rehabilitation, or research

- 6/8/2016
Confidentiality of Substance Use Disorder Patient Records – New NPR

- Consent and notice form changes
- Prohibition on Re-disclosure (§2.32), we propose to clarify that the prohibition on re-disclosure only applies to information that would identify, directly or indirectly, an individual as having been diagnosed, treated, or referred for treatment for a substance use disorder, such as indicated through standard medical codes, descriptive language, or both, and allows other health-related information shared by the part 2 program to be re-disclosed if permissible under other applicable laws
- Permit audits and evaluations using CMS guidelines

Expansion of Enforcement

OCR Resolution Agreements and CMPs

OCR website detailing penalties and resolution agreements
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/

March 16, 2016
$1.55 million settlement underscores the importance of executing HIPAA business associate agreements

North Memorial Health Care of Minnesota has agreed to pay $1,550,000 … failing to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information
HIPAA Fines and Penalties

Lot’s of CMP and settlement actions:

• $239,800 about employees taking ePHI home with inadequate safeguards
• $2,200,000 for allowing filming of PHI for a TV show without permission
• $750,000 for no BAA agreement that opened vulnerabilities
• $3,900,000,000 for having insufficient and incomplete security, no policies for authorizing access, receipt and removal of laptops, restricting access to unauthorized users by a Research organization
• 1,550,000 for no BAA or risk analysis.

All Quiet on the FIPA Front?

• So far not much news from FIPA
• Anyone heard anything?
• Are you all submitting FIPA Breach notifications in addition to HIPAA?

FTC and FCC step up to Regulate in Addition to HIPAA

• The FTC (Federal Trade Commission) has begun enforcement of general industry privacy and security, but also some in healthcare
• Appeals court did uphold FTC jurisdiction over some breaches
• FCC says don’t forget about us too!
• ONC has also released a privacy and security guide
• This trend is sure to increase as privacy and security are universally supported by patients and consumers and their politicians
• This represents a vast expansion of enforcement power that is much wider in scope than HIPAA
• Part of an overlapping strategy to increase privacy / security across all sectors, not just healthcare
HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

- How Security Rule and other Cyber programs work together — OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework
- In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity providing a voluntary, risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to understand, communicate, and manage cybersecurity risks
- This crosswalk document identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule which healthcare CE's and BA's must comply with
- Good for assessing gaps in HIPAA Security based compliance programs
- The NIST Framework offers depth to security protocols as it is more expansive and more technically prescriptive than the HIPAA Security Rule

Patient Access FAQ

- Guidance released at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/#newlyreleasedfaqs on the very hot topic for OCR, patient right of access to their own PHI
- This topic has become much more complex and great care must be taken to be compliant. Here are some tips from a privacy professional:
- A ROI (Release of Information) otherwise known as an "Authorization" is for the disclosure of PHI to organizations or individuals for information that falls outside permissible disclosures of treatment, payment, operations (TPO)
- Right to Access, is an individuals right to have "access" to his or her PHI.
- Requiring an individual to sign an "Authorization" is violation of an individuals civil rights
- However organizations will often request that an individual wanting access to his/her record submit a written request
- The written request is not the same thing as an Authorization, so don't be confused
Patient Access FAQ

- A written request for access is typically conducted or required by an organization to:
  1. Verify the identity of the individual
  2. To evaluate if the request for access will have the potential to cause harm to the individual if the information contained within the record is released. An organization has the right to deny the request for access if they feel the information contained within the record will cause harm to the individual

Patient Access FAQ

- In the case of an authorization, the individual is giving his/her “permission” for the organization to disclose the information to a third party. An authorization must have certain elements, content, and language within the document in order for it to be considered a valid authorization under HIPAA
- A request by a patient or their representative for access or copies of their PHI must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI
- Only very limited reasons to deny access, due to records not being in DRS (Designated Record Set), psychotherapy notes or if the release would endanger
- Prompt access is encouraged, but 30 days to fulfill the request

Patient Access FAQ

- BA’s have to abide by these rules if they maintain DRS records
- FAQ has depth on record copy fees allowed for patient access copies
- Patient’s must be advised of any fees in advance (remember only HIPAA fees, not state laws apply, unless state law says ‘free’)
- CE’s cannot pass along changes from ROI (or any other BA) vendor to provide patient’s own copies
- Patient’s can tell CE where to send their PHI
- ’Readily producible electronic formats’ required
- CE must put in safeguards to verify the identity of the patient / individual making the request, part of written request for access or copies
- Electronic signatures are ok, but again verification of the requestor is required
### Patient Access Request Details

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient requests to access (typically 'view the record live')</td>
<td>Typically a simple form that has easy to understand language explaining the forms purpose. No legalese necessary.فاءر validation of who signed the form is required so there may be an area for this. As well as where copies should be sent.</td>
</tr>
<tr>
<td>Patient requests copy for themselves</td>
<td>For these types of requests only HIPAA fees are allowed. No other information should be asked for in these forms per OCR guidance these forms are to be kept easy to understand.</td>
</tr>
<tr>
<td>Patient directs copies of their information sent to designated others</td>
<td>1. Patient requests to access (typically 'view the record live')</td>
</tr>
<tr>
<td>Note attorney's requesting PHI themselves claiming to represent the patient are NOT subject to HIPAA fees, regular state based RFS fees apply.</td>
<td></td>
</tr>
</tbody>
</table>

### Patient Consent Details

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending medical record copies to other providers for treatment purposes</td>
<td>1. Sending medical record copies to other providers for treatment purposes. Typically this is done without authorization since HIPAA allows TPO to be used without consent or authorization.</td>
</tr>
<tr>
<td>Using patient information for billing purposes with clearinghouses, insurance companies, etc.</td>
<td>2. Using patient information for billing purposes with clearinghouses, insurance companies, etc.</td>
</tr>
<tr>
<td>Making projections about expanding services of the organization that provided treatment or using the information in reports that are required to be filed with some overseeing agency, e.g. births for vital statistics.</td>
<td>3. Making projections about expanding services of the organization that provided treatment or using the information in reports that are required to be filed with some overseeing agency, e.g. births for vital statistics.</td>
</tr>
</tbody>
</table>

### Patient Authorization Details

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An attorney requests medical record</td>
<td>1. Attorneys require medical record</td>
</tr>
<tr>
<td>Attorney's correspondence to patient is returned with copies of the patient's medical record.</td>
<td>2. Attorneys' correspondence to patient is returned with copies of the patient's medical record.</td>
</tr>
<tr>
<td>Family members of patient are interested in pursuing a course of action that is not fully provided for by the patient's own medical record.</td>
<td>3. Family members of patient are interested in pursuing a course of action that is not fully provided for by the patient's own medical record.</td>
</tr>
<tr>
<td>Patient'srif for recording data that is not part of the medical record.</td>
<td>4. Patient's request for recording data that is not part of the medical record.</td>
</tr>
<tr>
<td>Patient's request to have medical record copied to another entity.</td>
<td>5. Patient's request to have medical record copied to another entity.</td>
</tr>
<tr>
<td>Copies of the medical record are sent to another entity.</td>
<td>6. Copies of the medical record are sent to another entity.</td>
</tr>
</tbody>
</table>
Attorney Request vs Patient Access

- Attorneys are not entitled to patient request record copy fees Per DWT Law Blog and Adam Green:
  

Attorney's Claim

- An attorney is bringing an action on behalf of a former patient that requires evidence of injury or other medical information.
- The attorney sends a letter to a health care provider requesting a copy of the former patient's medical records. The attorney's request will include a HIPAA-compliant authorization, signed by the patient (or the patient's personal representative).
- The attorney often will claim entitlement to the fee limitation at 45 C.F.R. § 164.524(c)(4), which limits a health care provider's charges to a patient for access to medical records to a "reasonable, cost-based fee.
- Attorneys have claimed that, because they are acting on behalf of the patient, they are entitled to the HIPAA rate for patient requests.

OCR responds March 25, 2015

- OCR distinguishes between an individual's (or their personal representative's) right to access their protected health information, versus an attorney requesting copies of medical records with a signed Authorization by the patient.
- OCR states that "If the rights under the individual access provisions at 45 C.F.R. § 164.524(a)(1) apply only to individuals (or their personal representatives under 45 C.F.R. § 164.502(g)) who request access to their medical records... Since there was no request made directly by the individual and the attorney does not constitute a personal representative for purposes of 45 C.F.R. § 164.502(g), the requirements under 45 C.F.R. § 164.524(a)(1) do not apply here.
- With respect to the cases where a provider gives the medical records to the attorney, because the copy of the medical record is being provided under the authority of 45 C.F.R. § 164.530(a)(1)(i), there is no applicable HIPAA restriction on the fees that the covered entity or business associate may charge in connection with such disclosures. In the absence of any HIPAA restriction on the fees, state law restrictions may apply.
- Therefore attorney's requesting records for patient's even with a signed authorization can be charged State record copy fees, not the lower cost based fee from the HIPAA Privacy Rule.
2016 OCR Phase 2 Audits

Audit Program Link

- [http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when](http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when)

The Letter You Don’t Want to Get From OCR...Pre-Audit Contact Questions
New Phase 2 Audit Program Released

Phase 2 started 03/21/16
• The first step is the letter verification to ensure they have the right addresses going out on this date
• The second step will be questionnaire which will ensure they have the right leadership within the organization involved and correct contact info
• Will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules.
• These audits will primarily be desktop audits, although some on-site audits will be conducted
• Onsite will start later this year. Just because you got a desktop audit does not mean you will get an onsite audit.

New Phase 2 Audit Program Released

• The 2016 audit process begins with verification of an entity's address and contact information. An email is being sent to covered entities and business associates requesting that contact information be provided to OCR in a timely manner
• OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees; this data will be used with other information to create potential audit subject pools
• If an entity does not respond to OCR's request to verify its contact information or pre-audit questionnaire, OCR will use publically available information about the entity to create its audit subject pool. Therefore an entity that does not respond to OCR may still be selected for an audit or subject to a compliance review
• The OCR website indicates the email address communication will come from OSOCR Audit @ hhs.gov
• Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity's spam filtering and virus protection are automatically enabled, we expect entities to check their junk or spam email folder for emails from OCR

Number of Phase 2 Audit Protocols

• Privacy = 89
• Security = 72
• Breach = 19
• Total = 180 protocols
• What does this tell us about the importance of Privacy?
• Security is a bear however, huge amount of documentation required
• Breach is covered from end to end
Phase 2 Audit Program Overview

• Surveysed sites will produce a list of their BAs, which probably becomes the pool for BA audits
• A geographically representative sample of those covered entities will then be selected for audit
• The audits will be conducted on a broad range of covered entities, including healthcare providers, health plans, healthcare clearinghouses, and business associates of covered entities, including large organizations and smaller practices
• The audits will involve 200 desktop audits and 10 to 25 full scale audits
• OCR will use a contractor (FCi Federal) to perform part of the audits
• OCR has been building out web infrastructure to facilitate the audits

Phase 2 Audit Program Overview

• Fines and penalties could be raised if a surveyed site is out of compliance, but this is not the real intent of the audits
• The real intent is to focus on areas that must be compliance in a teaching and learning environment...
• Still fines could be levied

FAQ – Paraphrased and Edited

What is the General Timeline for an Audit?

• In the coming months, OCR will notify the selected covered entities in writing through email about their selection for a desk audit. The OCR notification letter will introduce the audit team, explain the audit process and discuss OCR’s expectations in more detail. In addition, the letter will include initial requests for documentation. OCR expects covered entities that are the subject of an audit to submit requested information via OCR’s secure portal within 10 business days of the date on the information request. All documents are to be in digital form and submitted electronically via the secure online portal.
• After these documents are received, the auditor will review the information submitted and provide the auditee with draft findings. Auditees will have 10 business days to review and return written comments, if any, to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee’s response. OCR will share a copy of the final report with the audited entity.
FAQ – Paraphrased and Edited

What is the General Timeline for an Audit?

• While conducting desk audits of covered entities, OCR will replicate the notification and document request process for initiating desk audits of selected business associates. OCR will share a copy of the final report with the audited business associate.

• Similarly, entities will be notified via email of their selection for an onsite audit. The auditors will schedule an entrance conference and provide more information about the onsite audit process and expectations for the audit. Each onsite audit will be conducted over three to five days onsite, depending on the size of the entity. Onsite audits will be more comprehensive than desk audits and cover a wider range of requirements from the HIPAA Rules.

Phase 2 2016 OCR Audit Protocols

Layout of Protocol Table

• Item Number
• Audit Type – Privacy, Security or Breach
• Section – Statute Number
• Key Activity – Important field of the major topic areas addressed
• Established Performance Criteria
• Audit Inquiry – Main statutory language and definitions if applicable
• Required/Addressable – For security protocols only, HIPAA security rule
Privacy Audit Inquiries Change

There are changes to the criteria and inquiries from 2012 and there are slightly different numbers for each category (privacy, security, breach)

2012 Protocol for Deceased Individuals

- Inquire of management as to whether requirements with respect to PHI of a deceased person are met. Obtain and review the process and evaluate the content relative to the specified criteria used to ensure compliance with the requirements of PHI with ...

2016 Protocol for Deceased Individuals

- Do the covered entity’s policies and procedures protect the deceased individual’s PHI consistent with the established performance criteria? Inquire of management. Obtain and review policies and procedures regarding use and disclosure of deceased individuals’ PHI. Evaluate whether the policies and procedures are consistent with the established performance criterion.

Privacy Right to Access

Established Performance Criteria

- Determined whether the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access. (ii) If an individual requests a copy of the protected health information, or for use in, a civil, criminal, or administrative action or proceeding.

Item Number 65 Right to Access

Audit Inquiry

- How does the covered entity enable the access rights of an individual? Inquire of management.

- Obtain and review policies and procedures in place for individuals to request and obtain access to PHI and to determine whether they comply with the mandated criteria. Determine whether policies and procedures adequately address circumstances in which an access request is made for PHI that is not maintained by the covered entity, per 164.524(d)(3).

- Obtain and review the notice of privacy practices. Identify whether an individual’s right to access in a timely manner is correctly described in the notice.
Privacy Right to Access
Audit Inquiry

Item Number 65 Right to Access

• Obtain and review access requests which were granted (and documentation of fulfillment, if any) and access requests which were denied.
• Verify that access was provided consistent with the policies and procedures.
• Verify that requests for access were fulfilled in the form and format requested by the individual if the covered entity can readily produce the PHI in the requested form and format, including electronic format.
• Determine whether response was made in a timely manner (e.g., within 30 days of request receipt, unless extension provided consistent with 164.524(b)(2)(ii)).

Privacy Right to Access
Audit Inquiry

Item Number 65 Right to Access

• Determine whether fee charged meets the reasonable cost based fee requirement of 164.524(c)(4).
• If the entity denied access to certain PHI, determine whether it provided access to other PHI requested by the individual that was not excluded, per §164.524(d)(1).
• For cases for which access was denied, assess whether the denials, and any reviews made pursuant to individual request, were consistent with the policies and procedures.
• Inquire of management whether the covered entity has used a standard template or form letter for requesting access to protected health information. If the covered entity has used a standard template or form letter for access, obtain and review the document and determine whether it includes the requirements.

DWT Recommendations for Audit Prep

• Check your email and spam folders for OCR’s emails, and set OCR as an approved sender.
• Respond.
• Round up all the OCR inquiries.
• Have an audit response plan in place.
• Conduct a Pre-Audit Review.
• Respond timely to all OCR requests.
• Know your business associates.
• Be current, but not too current, maybe not documents created after the data request.
How to Prepare for 2016 OCR Audits?

1. Perform the privacy and security risk analysis you already are required to complete to be in compliance!
2. Be careful to understand the depth of an audit, very detailed and requires pulling up information as documentation to be provided
3. Your privacy and security risk analysis may or may not be at an ‘audit’ depth. That is up to you and your available resources
4. Create full set of Privacy and Security Policies, with procedures and forms
5. Ensure adequate workforce HIPAA training

Security Risk Analysis & Stage 3 Meaningful Use

Meaningful Use Stage 3 Final Rule

- MU Final Rule released on October 6, 2015 effective December 6, 2015
- This Final Rule is intended to be the final stage of the MU program and simplifies and reduces the number of measures
- Reduces the number of mandatory items
- Paves the way for MIPS (Merit Based Incentive Payment) from CMS which will incorporate MU in the future
- MU Stage 3 to provide flexibility to meet MIPS
- MIPS NPR (Notice Proposed Rule) targeted for Mid-2016 MIPS more focused on quality and care delivery than MU which was really more technology focused
- Payment adjustments under MU for failure to adopt EHR will be carried into MIPS around 2019
Meaningful Use Stage 3 Final Rule

- Stage 3 represents simplification of program requirements
- Introduction of flexibility within certain objectives
- Option to participate in Stage 3 in 2017, but required in 2018
- Overall focus on interoperability
- Encryption is just mentioned in passing, no requirements beyond HIPAA requirements (yes for transmission of PHI, not mandated for data at rest)
- Must conduct SRA once per reporting period, but ONC/CMS recognize this is an on-going not discrete process
- SRA for MU just covers certified EHR PHI, but they recommend to widen the scope to all PHI to meet HIPAA too

OIG Audits MU Recipients for Security (HIPAA Security Rule)

Security of certified electronic health record technology under meaningful use
HHS-OIG Work Plan | FY 2015

- We will perform audits of various covered entities receiving EHR incentive payments from CMS and their business associates, such as EHR cloud service providers, to determine whether they adequately protect electronic health information created or maintained by certified EHR technology
- A core meaningful-use objective for eligible providers and hospitals is to protect electronic health information created or maintained by certified EHR technology by implementing appropriate technical capabilities
- To meet and measure this objective, eligible hospitals, including critical access hospitals, must conduct a security risk analysis of certified EHR technology as defined in Federal regulations and use the capabilities and standards of Certified Electronic Health Record Technology. (45 CFR § 164.308(a)(1) and 45 CFR §§ 170.314(d)(1) – (d)(9).)

OIG Audits MU Recipients for Security (HIPAA Security Rule)

- Differs from CMS Figliozzi MU audits which focused on a copy of a SRA (Security Risk Analysis) not the adequacy of the analysis
- OIG goes deeper into security including
  - BA’s with access to the EHR
  - Focus on Cloud service providers and EHR vendors
  - Onsite 2-3 weeks w/ Interviews
  - What happens if fail? Fraud?
  - Supposedly not punitive to individual hospitals and Eps. But no one is sure, are they collecting data for a larger study?
Conclusion

- The OCR 2016 Audit Program is Phase 2 is here, be prepared, even if not audited a OCR compliant and investigation could cause you to answer the same questions and face liability
- Enforcement always expands, never will it contract for privacy and security
- HIPAA Privacy and Security demands for data are constantly increasing and must be well organized, automation becoming reality
- Remember Business Associates have the same rules to comply by performing both privacy and security risk analysis as a part of their Privacy and Security Compliance Programs

Resources and References

- Office for Civil Rights (OCR) website both privacy and security
- HIPAA Security Final Rule 2003
- HIPAA Privacy Rules Updated for Omnibus
- NIST 800-66 Introductory Resource for HIPAA Security Rule
- NIST 800-19 Risk Management Guide for IT Systems
- ONC Published free tools
- OCR published FAQs and on-line guidance
- DAS Audit for Security and the EHROIG - Davis Schoolcraft - dschoolcraft@omwlaw.com
- Carlyn Choate - SR Policy and Privacy Coordinator – AHIMA Confidentiality Blog

For Questions, Comments and Requests, please contact:

Kelly McLendon, RHIA, CHPS

E-mail: kmclendon@complianceprosolutions.com
Web: www.complianceprosolutions.com
Phone: 321-268-0320