Recent Developments in Privacy and Confidentiality of Health Records

Briar Andresen

Marguerite Ahmann

April 12, 2017

Fredrikson & BYRON, P.A.

Overview

- Updated Part 2 Regulations
- Privacy Developments

Part 2

- 42 C.F.R. Part 2 (“Part 2”) implements federal drug and alcohol confidentiality law (42 U.S.C. § 290dd-2)
- Applies to federally assisted substance use disorder treatment programs (“Part 2 Programs”)
- First promulgated in 1975
- Last modification was in 1987

Part 2: The Basics

- Part 2 applies to:
  - patient identifying information (or “PII”);
  - that has been obtained from a Part 2 Program; and
  - indicates that the individual has a substance use disorder.

Part 2 Final Rule

- Effective Date:
  - Original: February 17, 2017
  - Delayed: March 21, 2017
- Modernizes Part 2 regulations in light of technological changes and enhances privacy and security protections

Part 2: Definitions

- Scope: Applicable to “Programs”:
  - (1) An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
  - (2) An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
  - (3) Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

Part 2: Definitions

- *Substance use disorder*
  - A cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal. For the purposes of the regulations in this part, this definition does not include tobacco or caffeine use.

"To Whom"

- Part 2 Programs must obtain written consent to share Part 2 information for most purposes, including TPO.
  - **Prior Part 2 Regulations:** Consent form required to specify the name or title of the individual/organization
  - **New Regulations:** Allows for general designation (e.g., "my treating providers") and disclosure to intermediaries

"To Whom"

- The intermediary must be able to track and generate a list of disclosures.
  - For up to the prior two years
  - More robust than an accounting of disclosures under HIPAA
  - Must be implemented in tandem with the general designation
  - SAMHSA *requests* that costs not be passed on to the patient

“From Whom”

- Consent Requirements (§ 2.31) – SAMHSA proposed:
  - Require the “From Whom” section to specifically name the Part 2 program or other lawful holder of patient identifying information making the disclosure

Re-Disclosure Prohibition

- Old: Broad prohibition on disclosing information to a third party without consent or regulatory exception.
- New: Prohibition is limited to data that directly or indirectly identifies a patient as suffering from a substance use disorder.
  - Note, this includes identifying the Part 2 program itself.

Medical Emergencies

- Aligning the language under the regulation to the language within the statute
- Gives providers more discretion to determine when a “bona fide medical emergency” exists
- SAMHSA plans to provide examples in sub-regulatory guidance

Qualified Service Organization (QSO)

- Allows for disclosure to third parties that provide services
- QSO Agreements
- Final rule revises scope of QSO arrangements:
  - Excludes care coordination
  - Excludes medication management
  - Added population health management

Research

- Permits Part 2 data to be disclosed to qualified personnel for scientific research
  - Must comply with HIPAA and Common Rule
  - No re-disclosure except back to its source
  - Must maintain and destroy Part 2 information per security rule

Discontinued Records

- Disposition of Records by Discontinued Programs § 2.19:
  - Addresses both paper and electronic records
  - Adds requirements for sanitizing associated media

(Lack of) Alignment with HIPAA

- SAMHSA noted its intention to align with HIPAA where possible:
  - Patient Identifying Information
  - Security for Records
- Intended to be more stringent than HIPAA

Patient Identifying Information

- Attempted to align with PHI under HIPAA
- Any information that could identify a patient as suffering from, or receiving treatment for, a substance use disorder would constitute patient identifying information

Security for Records § 2.16

- Final rule substantially revised security requirements:
  - Part 2 programs and other lawful holders of PII must have in place formal policies and procedures to reasonably protect against unauthorized uses and disclosures of PII and to protect against reasonably anticipated threats or hazards to the security of patient identifying information

Security: Required Policies and Procedures

– Policies must cover:

- Transferring, removing, and destroying paper and electronic records (including sanitizing the electronic and hard copy media);
- Rendering PII non-identifiable in a manner that creates a very low risk of re-identification;
- Creating, receiving, maintaining, and transmitting electronic records; and
- Physical security measures, including maintaining paper records in a secure space, using and accessing workstations, secure rooms, locked file cabinets, etc.

SNPRM

- § 2.32: Prohibition of Re-Disclosure
- § 2.33: Disclosures Permitted with Written Consent

Privacy developments

“Are we doing enough??”

- Probably not
- HIPAA audit results and settlements demonstrate that it’s hard to do “enough,” especially if you’re unlucky enough to have a major breach
- New hacking reports across multiple industries
- Difficult to keep up with changing environment and expectations

HIPAA—updates in last 12(ish) months

- HIPAA and the cloud
  - Guidance October 2016
- Blocking access to PHI by BA
  - FAQ, October 2016
- Negotiating EHR contract
  - Guidance September 2016
- Access/Fees for records
  - Jan./Feb. 2016, guidance and FAQ
- HIPAA and Ransomware
  - Guidance and Fact Sheet, July 2016
- Allowing film crews to record
  - FAQ (and settlement) April 2016
- Man in the Middle Attacks
  - OCR newsletter April 2017

HIPAA-And-The-Cloud¶

By-Briar-Andresen¶

HIPAA and the Cloud

- Guidance aimed at users of cloud computing (CEs and BAs)
- OCR recommends checking NIST resources, esp. “NIST Definition of Cloud Computing” to review options
- Have a BAA with your cloud service provider, understand how it works so risk analysis can be performed
- Pay attention to SLA

HIPAA and the Cloud

- CSP is a BA even if it doesn't have "access" to the ePHI that it maintains
  - True even for encrypted information
  - "No view services" has lowered risk, but still some risk—CSP is not exempt from HIPAA requirements; spell out who is responsible for what (including in BAA)
  - "A CSP is not responsible for the compliance failures that are attributable solely to the actions or inactions of the customer, as determined by the facts and circumstances of the particular case."

HIPAA and the Cloud

- Using as CSP without having a BAA in place first is a HIPAA violation
  - There was a $2.7m settlement related to a covered entity's use of a cloud-based server without a BAA
- "Security incidents" must be reported by the CSP
  - Includes "attempted" OR successful unauthorized access
  - But no specific requirements for when these reports must happen, or how much detail
- Mobile device use ok to access ePHI in the cloud
- Storing outside U.S. is ok, but…
- Not required to audit anyone, but…

Blocking access to PHI

- Can a BA block/terminate access to PHI?
  - NO!
- BA is not allowed to use PHI in a way that would violate the Privacy Rule
- BA is required by Security Rule to ensure availability of all ePHI
- BA must make PHI available to covered entity to satisfy access to PHI obligations of covered entity

Guidance for EHR contracts

- ONC, guidance September 2016
- Selecting EHR vendor, negotiating EHR contracts
- “EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print”
- Includes some sample contract terms

Guidance for EHR contracts

- Core service and performance obligations should be spelled out clearly
- Pick vendors willing to incorporate language that says who will be responsible for information security
- Try to get warranties and other guarantees

Access to PHI/Fees for records

- New FAQs and a “clarification”
- Generally, individuals have a right to access their own PHI
- OCR “clarified” that individuals may direct a third party to have access without signing an authorization
  - Request for access by third party must be in writing and signed, and clearly identify who will get the information

Access to PHI

- Must provide in the form/format requested (if readily producible in that form) or a readable hard copy form or as otherwise agreed with the individual
- If PHI is on paper, and individual wants it electronically, if readily producible (e.g., scanning), must do it
- Must be able to electronically product information maintained electronically

Access to PHI

- 30 day response is permitted, but OCR makes clear that's an outer limit
- If you have requested PHI immediately available, you should get it to the individual quickly

Fees for PHI

- "Reasonable, cost-based fee"
- ONLY labor, supplies, and postage
  - No retrieval fees, no fees for time spent searching for records
  - Labor is only for creating and delivering the copies
  - Supplies: paper, toner, USB drive, etc.
  - Can't require someone to purchase USB; information can be mailed or emailed.

Fees for PHI

- Others fees authorized under state law are not ok
- "Covered entities should provide …access … free of charge."
  - HIPAA does allow you to charge
- Can charge for a summary of the info if the person agrees in advance to both the summary and the fee

Fees for PHI

- Can charge for labor of photocopying or scanning into electronic format
- OCR expects these labor costs to be small
- Can’t charge to “view and download” from portal
- Notify individuals in advance of the approximate fee for copies

Fees for PHI

- Actual costs
  - Still must tell expected cost in advance
- Average cost
  - Schedule of costs for labor based on average labor cost
  - Can charge per page only where PHI is in paper form and person asks for a paper copy
- Flat fee
  - $6.50 maximum

Fees for PHI

- Fee limits apply to individuals own requests and requests to give PHI to a third party
- Requests by third parties based on patient's authorization are not subject to these fees (unless the third party is forwarding the patient's request)

HIPAA and Ransomware

- Thousands of daily ransomware attacks in 2016
- Bad actor gains access via malware to technical infrastructure to deny the organization access to its own data by encrypting the data
- Guidance describes prevention and recovery from healthcare perspective

HIPAA and Ransomware

- HIPAA preparedness can help!
  - Security management process/risk analysis to identify threats
  - Implement procedures to guard against and detect malicious software
  - Train staff on protecting themselves/the organization
  - Maintain frequent backups and make sure you can get data from backups
  - Have contingency/emergency plan/security incident procedures in place

HIPAA and Ransomware

- Guidance discusses how to detect whether your systems are infected with ransomware
- What to do if systems are infected
  - Security incident and response plan
  - NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide
- Is it a breach?
  - It depends—fact-specific analysis
  - If ePHI is encrypted as a result of an attack, OCR says it is a breach

Allowing film crews in…

- Generally, don’t
- NY hospital hit with settlement for allowing crews “unfettered access” to treatment areas without authorization
- If they’re going to be where there is PHI, they must have patients sign an authorization
- The case resulted in a new FAQ on filming

OCR Cyber Awareness Newsletters

- Reporting and Monitoring Cyber Threats (February 2017):
  - Encourages:
    - Reporting to United States Computer Emergency Readiness Team (US-CERT).
    - Monitoring of US-CERT website.
  - PHI may not be shared for unless the disclosure is otherwise permitted under the HIPAA Privacy Rule.

OCR Cyber Awareness Newsletters

- Man-in-the-Middle Attacks and “HTTPS Inspection Products” (April 2017).
- Understanding the Importance of Audit Controls (January 2017).

ONC Updated SAFER Guides

- March 2017 (revised version)
- Safety Assurance for Electronic Health Records Guides
  - The Guides
  - Nine guides for providers to “assess and remediate EHR vulnerabilities”
- First published in 2014
- Foundational guides, infrastructure guides, and clinical process guides
- Self-Assessment

ONC SAFER Guides

- High Priority Practices
- Organizational Responsibilities
- Contingency Planning
- System Configuration
- System Interfaces
- Patient Identification
- Computerized Provide Order Entry with Decision Support
- Test Results Reporting and Follow-Up
- Clinician Communication

HIPAA and OCR

- New kid on the block:

OCR’s new boss is Roger Severino

OCR and HIPAA

- 2016 was active year for OCR enforcement
  - 12 settlements, one CMP
- AGs also getting in on the action
  - MA and CT seeing more activity
- Average settlement amount nearly doubled
- Hacking is the cause of most *large* breaches

HIPAA Audits

- Toolbox of ensuring compliance—not done in pursuit of CMP
- OCR thinks of this as a “free consultation” with feedback in the draft report
  - You *can* move from audit to compliance review if you:
    - Don’t respond
    - Send documents that make it look like you have no idea what you’re doing
- Currently in Phase II of audit program—desk audits
- OCR not sure if on-site audits will be coming before end of 2017

HIPAA Audits

- Is your notice “prominent” enough on your website?
  - *“An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices.”*
  - Down at the bottom of the page isn’t good enough
- Do you have contact information for business associates?

HIPAA enforcement

- Investigations and compliance reviews are complaint-driven
  - Breach reports, news reports, information from other agencies
- Looking for “egregious” behavior in settlement corrective actions
- Insider threats (not ending employee access properly)
- Timeliness of breach notification

HIPAA settlements

- UMass paid $650,000
  - Less than they otherwise would have if they had been in better financial shape
- A malware situation, and a hybrid entity
- Failure to have appropriate firewalls and to ensure appropriate compliance as a hybrid entity
- Insufficient risk analysis

HIPAA settlements

- $5.5m for Memorial Healthcare System (FL)
  - February 2017 (happened in 2011/2012, breach report submitted April 2012!)
  - Name, DOB, SSN for 115,143 individuals
  - Ex-employee used password to access info on a daily basis for a year (80,000 individuals)
  - Didn’t implement procedures on terminating user right of access
  - Didn’t regularly review IS activity on applications even though it was identified on risk analysis for five years
  - May have been an issue with affiliate physician offices

HIPAA settlements

- First settlement related to failure to timely report a breach
- $475,000 for Presence St. Joseph Medical Center/Presence Health (IL)
- Discovery of breach October 22, 2013, report to OCR January 31, 2014 (and to individuals February 4, and media February 5).
- Problem was that it affected 800+ individuals

HIPAA CMP!!

- Children's Medical Center of Dallas (TX) (February 2017)
- Did not go to an ALJ before receiving CMP
- Failure to timely request a hearing
- Fine itself was due to "impermissible disclosure of unsecured electronic protected health information (ePHI) and non-compliance over many years with multiple standards of the HIPAA Security Rule"
- Self-report of lost unencrypted Blackberry in 2009 (reported in 2010), then separate report of laptop lost in 2013

OCR

- More to come on sharing information with caregivers and family members
- 21st Century Cures Act
  - HHS must clarify when HIPAA allows communications with caregivers of adults with serious mental illness to facilitate treatment.
  - Also requires guidance on communications when patient presents serious threat to self/others
  - Guidance by Dec. 13, 2017, and model training materials
  - Won't change the law/regulations—just makes HHS explain the existing rules

OCR

- Cyber security and cyberthreats remain a big deal
- They are proud of their guidance on ransomware
- Hire a person who knows about security
- Focus on risk analysis
- Mobile devices

FACTA

- Fair and Accurate Credit Transactions Act (2003)
  - Part of intent of law is to cut down on identity theft and consumer fraud
- Subway just settled for $30.9m
- Class action for having a receipt that showed **full expiration date** of debit card + last 4 digits

Doing as much as you can

- Risk analysis
  - Do it, update it, check back on it
- Document what you've done
  - Build your records for risk analysis, but also for training, breach reporting (or not reporting)
- When something goes wrong, address it as quickly and thoroughly as possible
  - Respond and remediate
- Bring in experts when you need to

Questions?

Briar Andresen
612.492.7057
bandresen@fredlaw.com

Marguerite Ahmann
612.492.7495
mahmann@fredlaw.com