HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

OCR May Alter HIPAA Rules to Ease Compliance, Care Coordination

The healthcare industry has complained about the difficulty of complying with HIPAA since the law was enacted. Now, the HHS Office for Civil Rights (OCR) is asking for suggestions on how to make HIPAA more manageable. What changes might actually happen remains uncertain.

OCR issued a Request for Information (RFI) seeking public input about how the HIPAA Privacy Rule could be changed to promote value-based and better coordinated care. *(Editor's Note: The RFI is available at: https://bit.ly/2iVERG4.)* OCR's effort to resolve frustrations with HIPAA is long overdue, says **Joseph A. Dickinson**, JD, partner with Smith Anderson in Raleigh, NC.

"HIPAA, as it has evolved, has gone too far. It is inhibiting the sharing of information for purposes of healthcare treatment," he argues. "We see it every day with doctors including fears of HIPAA liability in their healthcare process, sometimes not fully sharing information with other healthcare professionals that might actually be pertinent and needed to provide the best care."

Meanwhile, there is a serious problem in the industry with data breaches and healthcare organizations not taking their obligations seriously, Dickinson says. OCR's challenge will be to change the law in ways that ease the unreasonable burden without letting organizations off the hook if they do not make reasonable efforts to comply.

"I think OCR is going to cut back on the fundamental obligations to protect patient privacy up front, but making some changes on the other end so that once they have that protected data they can share it with other providers to get the best care for the patient," Dickinson says.

The OCR's RFI focuses on how HIPAA rules can be revised to facilitate coordination of patient care among and between providers, explains **Eric D. Fader**, JD, an attorney with the Rivkin Radler in New York. Although HIPAA became law in 1996, Fader says not everyone understands certain aspects of the rules. Thus, some healthcare providers, particularly their clerical employees, sometimes find it easier not to cooperate promptly with a patient's or another care provider's request for records while using HIPAA as an excuse.

The Treatment, Payment, and Healthcare Operations (TPO) exception to the Privacy Rule continues to be difficult to grasp for some, Fader says. The TPO exception permits (but does not require) the sharing of patients' protected health information (PHI) for purposes of care coordination. Fader says requests for PHI from one unrelated provider to another often are not handled with the same degree of urgency.

"The OCR has surely heard anecdotally of many instances where requests for information for treatment purposes were either not complied with at all, whether through a misunderstanding of what HIPAA allows or for workload reasons, or due to an unwillingness to cooperate with the requesting party," Fader says. "It appears that the OCR is considering how to make sharing PHI for purposes of treatment ... more mandatory than permissive, a goal with which I agree."

The other sections of the RFI are mostly variations on the same theme, Fader says. They include consideration of shifting some provisions of HIPAA from "disclosure of PHI is permissible if ..." to "disclosure is required under these circumstances."

Fader predicts care coordination, case management, quality assurance, and other activities will be easier if healthcare providers understand that they do not need to be concerned about disclosing PHI to another party that is subject to HIPAA already while also recognizing the need to handle requests promptly.

"Just as the OCR continues its enforcement activities when healthcare providers inexplicably still fail to comply with HIPAA after all these years, and just as they continue to put out press releases regarding settlements that are clearly intended to be educational for the provider community, the OCR has clearly recognized that more education is necessary to improve

sharing of patient information so that the system will work better overall," Fader says. "[OCR] seems to be prepared to make this a priority in 2019."

HHS started an initiative to enhance care coordination, but HIPAA has proven to be an obstacle, says **Richard Trembowicz**, JD, associate principal with ECG Management Consultants in Boston. Healthcare providers are hindered by cumbersome documentation of authorization to share and fear of extensive liability if information is inappropriately shared with third parties, he says.

"Simply put, the cost of documentation of authorization of access and delivery of PHI and risk of error in information management both increase if more individuals are authorized to have access to PHI, especially if the rules have lots of exceptions or nonstandard processes," Trembowicz explains. "CMS is also concerned that the time period within which a provider must respond to an individual's request for the sharing of PHI is too long, making the information value stale by the time it is shared."

HHS has posed 54 subjects for public comment to obtain insight on how changes to the rule could affect all involved in the care delivery process. Trembowicz notes that several questions seek feedback on the additional provider burden should HHS require providers to respond to individual requests for PHI faster than current law and regulations require. This will necessitate providers to devote additional resources to searching for, copying, and delivering the requested information to the individual, he says.

"It also begs the question of whether format of delivery, such as electronic, will be required, and whether the provider has a responsibility to deliver the information to other third parties as directed or requested by the individual," Trembowicz says. "All of this will cost money, and HHS provides no guidance on whether it will compensate providers for the additional costs." In addition, HHS is seeking feedback on the authorization process to release information, various exceptions, and effects on business associates with which the provider conducts business, including the security practices and documentation of authorizations to release information.

"The greatest concern of providers is that HHS will issue new unfunded mandates that increase the cost of medical care without compensation," Trembowicz says.

Several proposals for which OCR seeks feedback deserve special mention, according to **Kristen Rosati**, JD, an attorney with the law firm of Coppersmith Brockelman in Phoenix. First, she says the focus on including nontraditional providers and social service agencies in data sharing is important to managing care. There is an increasing recognition that the social determinants of health, such as the availability of food, counseling, and secure housing, significantly influence an individual's ability to manage a chronic condition or to improve after an acute health episode.

"Second, the industry should support OCR's focus on sharing information with family members and caregivers to address the opioid crisis and serious mental health issues," Rosati offers. "Family members and caregivers play an essential role in getting people with additional problems to treatment and in helping them manage their care. They often are as important to the treatment team as the physicians and nurses."

However, Rosati notes that OCR also solicits feedback on a proposal that would increase obstacles to data sharing. OCR has asked for comment on requiring HIPAA-covered entities to include information in an "accounting" about disclosures from electronic health records that are made for treatment, payment, and operations purposes. An accounting is a list that covered entities must provide to an individual on request, which includes information about disclosures of that individual's health information for purposes other than treatment, payment, and operations, Rosati explains.

"It's incredibly burdensome even under the current scope of the rule. Adding to that requirement creates more burden without much benefit. It also is not technically feasible to do automatically, as electronic health record systems do not capture the information that would be required in an accounting," she says. "We hope the industry pushes back on this proposal."

It is always difficult to predict how HIPAA regulations might change, says **Roy Wyman**, JD, partner with Nelson Mullins in Nashville, TN. Agencies like HHS generally avoid making changes to regulations, as such edits require lengthy administrative and public review and can end up causing as much damage as good, Wyman says.

However, the Trump administration emphasizes reducing the burdens of regulations. For example, the 21st Century Cures Act requires HHS to develop a plan to reduce regulatory and administrative burdens on the use of health IT and electronic health records. The Cures Act mostly targeted areas outside HIPAA, but the draft strategy for the Cures Act includes criteria that also could be used in any HIPAA simplification, Wyman explains.

The draft strategy says changes should be achievable within the near-to-medium term (a roughly three- to five-year window). It also says HHS should be able to either implement these strategies through existing or easily expanded authority or should have significant ability to influence the implementation of these strategies.

HHS may be reticent to take any actions perceived as watering down privacy protections, but some provisions may be ripe for change because they are not related to individuals' rights, Wyman explains.

"For example, the rules for when a hospital or provider can disclose information are complex and often require professional judgment," Wyman says. "More common sense and bright-line rules would simplify the process for sharing information with relatives and friends of patients and understanding when another individual or estate can act on behalf of the individual."

Other areas are largely invisible to individuals and privacy advocates but are complex. Such areas can cause unintentional violations. Some examples include sharing health information for "healthcare operations," public health, and research purposes.

"The ability to disclose information for these purposes is more complex and limited than sharing information for treatment or payment purposes," Wyman explains. "A simple guideline allowing entities to share information for operations of the sender or the receiver or for public health and research purposes, subject to the other rules of HIPAA, is a relatively simple fix that might receive relatively narrow complaints from privacy advocates. Such simplification also might promote the quality and efficiency of patient care."

Similarly, Wyman notes that the rules and definitions for Affiliated Covered Entities, Organized Health Care Arrangements, and hybrid entities create a legal tangle. These rules permit various types of arrangements and entities to comply with HIPAA, yet they can create administrative and training burdens. "Simplifying these rules could largely eliminate these definitions while permitting covered entities and business associates to be joined and divided in ways that seem most appropriate to the entity so long as those receiving health information comply with HIPAA and maintain the security of the information," he says.

Wyman believes the Security Rules also need a significant overhaul. "Many of the requirements overlap, contain confusing terms, and are mostly useful to assure consultants remain in business. The regulations could use a good review to reduce and consolidate many of the requirements, make sure that the requirements are understandable to the technologically naïve, and are more user-friendly," Wyman offers. "For example, the Security Rules include three different sections that address access control. Some sections of the regulations are deemed 'required,' and others are 'addressable,' yet all of them must be considered. A clearer description of what is required would eliminate a huge amount of confusion."

While technically outside of HIPAA, Wyman says rules about the protection of information held by mental health and substance abuse providers have created enormous burdens. The "Part 2" rules (42 C.F.R. Part 2) originally predated HIPAA as well as the internet. Although these rules were updated recently, they remain burdensome, according to Wyman.

"Unfortunately, the increased burden on these providers has made it very difficult for them to share information with other providers, participate in health information exchanges, or generally function in a data-intensive world," he laments. "A wholesale annexation of Part 2 into HIPAA seems unlikely, but the two sets of regulations could be better harmonized. For example, Part 2 could create an exemption that would allow sharing of data with a covered entity or business associate of a covered entity under HIPAA based either on a written agreement or particular requirements on the receiving entity written into the regulations. The requirements on the receiving entity might be similar to how covered entities treat psychotherapy notes under HIPAA."

OCR is asking the public for ways to modify the HIPAA regulations specifically to drive cost savings and value, which are most commonly expected to come from the development of coordinated care platforms, says **Jeff Drummond**, JD, an attorney with Jackson Walker in Dallas. HIPAA is naturally obstructive to care coordination. Any efforts at care coordination naturally assume ready exchange of patient information among providers, payers, and others involved in the care of the patient (or the patient population). Meanwhile, HIPAA's focus on privacy and security generally limits information sharing, according to Drummond. HIPAA allows for such sharing of patient medical records, but Drummond believes too many people in the healthcare industry do not understand HIPAA and are afraid of it. Thus, they refuse to share information even though HIPAA would allow it.

"Another major problem is that given the combination of the Facebook and other social media platform privacy issues all over the news, as well as the daily reports of major breaches of personal and medical information, many people are too afraid that their medical record privacy will be abused," he explains. "People fear for their privacy, so they don't want their information released, even though releasing the information in an appropriate manner would actually improve their healthcare and the overall cost of healthcare."

Drummond says these problems cannot be fixed by changing HIPAA because as currently structured, HIPAA would work to allow appropriate information exchange for care coordination and value-based healthcare. "Thus, I do not see any major changes being made to HIPAA," Drummond says. "However, given the push for regulatory change, and the need to be seen as doing something, I would expect some tinkering around the edges." Here is how Drummond expects to see OCR change HIPAA:

• Minor tweaks to the definition of "healthcare operations" to clarify and

possibly expand the ability to share PHI for population health, emergencies, and value-based care initiatives;

• Minor clarifications regarding "personal representatives" and when parents are (or are not) treated as such;

• Specific language (more likely guidance than changes to the actual text of the regulations) addressing uses and disclosures in the mental health and substance abuse arena;

• Revisions to the "accounting of disclosures" requirements to streamline the process by eliminating much of the requirement;

• Finalization of the rule allowing individuals to share in the fines levied by OCR for a HIPAA breach;

• Specific language addressing when a ransomware attack (or similar technology-driven incident) is a reportable breach.

Drummond says some commentators will ask for removal of the requirement that directs patients sign an acknowledgement receipt regarding the Notice of Privacy Practices when they first go to their doctor. However, he does not think that will occur. "It would definitely remove a noticeable burden on both providers who have to print out notices, ask for signatures, and keep track of them. Ultimately, that's a small burden to make sure that providers actually provide the notice," he says. Patients have an opportunity to think about how their information is going to be used and disclosed. Ultimately, I think [OCR will] leave it in place as is." The biggest effect from any changes may involve the increasing use of technology in the transmission of patient data from one healthcare provider to another, says **Patrick Pilch**, managing director and national leader for BDO Healthcare Advisory's Center for Healthcare Excellence & Innovation. "We're seeing more care being directed over smartphones, for example, so OCR may change the requirements for providers who have not been connected electronically in the past," he offers.

"That could have a big impact and would change HIPAA in a way that acknowledges how healthcare delivery has changed in the past 20 years. It's that kind of thing that frustrates people who are trying to comply with HIPAA but the law doesn't seem to fit with how things are done in the real world." ■

HIPAA Requires Security for Printers, Just Like Other Servers and Endpoints

HIPAA security requires protection for servers and various endpoint devices. However, many healthcare organizations do not realize printers need the same attention.

Most covered entities and business associates do not appreciate how printers have evolved from "dummy copiers" to today's complex business machines that include multiple servers built directly into them, explains **Jim LaRoe**, CEO of Symphion, a software and services company in Dallas. The competition among printer manufacturers has driven the inclusion of web servers, file transfer protocol servers, fax servers, huge hard drives, and many other advanced capabilities, he notes. Yet, printers, unlike standalone servers, are maintained outside of data centers without the physical and technical safeguards that are common to data centers.

"They are also managed by nonsecurity, non-IT professionals, not the heavily credentialed system administrators like in data centers, and are not included in IT policies and procedures," LaRoe adds. "Moreover, printers, like laptops, are mobile throughout the enterprise. They are often on wheels."

HIPAA's general mandates require covered entities to ensure the confidentiality, integrity, and availability of PHI the business creates, receives, maintains, or transmits. HIPAA also requires covered entities to protect against any reasonably anticipated threats or hazards to the security or integrity of information. "Printers in hospitals clearly 'create, receive, maintain, and/or transmit' electronic PHI," LaRoe notes. "Moreover, even the most cursory examination of reasonably anticipated threats and hazards to the security and integrity of that ePHI trigger the HIPAA mandates to protect printers."

Specifically, HIPAA requires covered entities and business associates to assess current security and risks for ePHI in the entire enterprise. That includes the risks presented by the printers and implementation of a security plan, policies and procedures, and controls that address vulnerabilities and risks. The entity must monitor, record, and evaluate implemented security settings to ensure the security plan and controls are maintained vigilantly, according to LaRoe.

"Neither hospitals nor enterprises are dealing with network printers correctly. That makes them one of the biggest security threats for 2019, especially considering that breaches are getting more costly," LaRoe warns. "Since every printer on a print fleet can provide hundreds of vulnerabilities, and many hospitals can have thousands of printers, the message is clear. Even though printers have been here for years, they ... must be protected like the servers that they are, with automated IT asset life cycle management and continuous cyber hardening." ■