Modernizing HIPAA: Assessing the Proposed Modifications to the HIPAA Privacy Rule and Implications for Stakeholders

This deep-dive discussion focused on the proposed modifications to the HIPAA rule and heard from physicians, hospitals and patients on the implications of the proposed rule. Panelists raised concerns regarding several proposals including to expand the individual Right of Access, allowing third-party sharing, requiring response to oral requests, and others. Panelists also discussed the need for Congress to enact federal privacy legislation to better align the current patchwork of privacy protections.

Speakers:

- **Laura Hoffman**, Assistant Director, Federal Affairs, American Medical Association
- **Deven McGraw**, Chief Regulatory Officer, Ciitizen Corporation, Former Deputy Director, Health Information Privacy, HHS Office for Civil Rights
- **Peg Schmidt**, Chief Privacy Officer, Advocate Aurora Health

Key Takeaways from Questions:

Individual Right of Access

- **Kristen McGovern:** The proposed rule is intended to provide individuals with easier access to their health records. Can you describe the current Privacy Rule's Right of Access, and talk through what the proposed rule seeks to modify?
    - **Deven McGraw:** In the omnibus rule, OCR had originally interpreted the provision around allowing patients to send information directly to the third-party of their choice to apply across the board with the HIPAA Right of Access; whether it's paper, or electronic, the patient has the right to get the information for themselves and send that information directly to a third-party such as another doctor or a family member. Then, there was a case that went to court where the court said that the right of the patient to send information to a third-party only pertains to information from the electronic health record (EHR). OCR has addressed this in the new proposals, including what it means to direct information to a third-party and what it means for services that a patient might hire to allow the patient to manage and control the records themselves. There is a new Right to Inspect, which allows patients to take a look at their record and use their own tools to take a picture at the time of service. OCR has also proposed shortening the timeframe from 30 days to 15 days, with an extension of up to 15 days from 30 days.
- **Kristen McGovern:** What is the difference between a patient authorization and the patient right of access? What are the different protections for data accessed through either pathway?
    - **Peg Schmidt:** There is a primary difference between the two methods, one is a required disclosure and one is a permitted disclosure. 1) Authorization (permissive): Covered entities (CE) are not required to act on that; 2) Disclosures under the Right of Access is a requirement. Authorizations require a number of specific elements in order to be valid, for instance, it must be signed by the individual and give clear direction on who the recipient is. Authorizations have no time requirement to respond; current Right of Access requires a response within 30 days. Both require reasonable safeguards for sending protected health information (PHI). There are more controls when patients are making a request under the Right of Access, they may be more in control because they are initiating it and can control the number of

disclosures being made. In an authorization, the patient doesn't necessarily have control over disclosures, and an authorization can continue to be used until it has expired or revoked. Under Right of Access a patient has a bit more recourse when making a complaint. There are tradeoffs to consider, however, with verification requirements and requirements to only disclose within the scope of the authorization, covered entities are still working in the interest of the patient to protect PHI. Some of these differences will be changed in the proposed rule.

Third-Party Access

- **Kristen McGovern:** HHS proposes to create a new pathway for patients to obtain their health information through a personal health application (PHA). While this could encourage individuals to use apps like Apple Health, it may also have privacy risks given that third party apps are generally not covered by HIPAA. Do you believe there are privacy risks with giving broad access to third party apps? Are there any examples of challenges occurring today that could indicate future issues? The definition of a PHA in the rule is broad – in some cases it's not just necessarily an app on your phone.
    - **Laura Hoffman:** Part of this proposal was to address some of the lack of clarity around whether a request to use a smartphone app is an individual requesting their own access or whether it's going to a third-party. OCR's guidance previously had indicated that an app is a third-party. When someone is requesting their information go to a smartphone app, they are exercising their individual Right of Access but directing it to be received by a third-party. Typically, that requires some sort of "clear and conspicuous" direction to the CE to ensure they are sending it to the correct party. This proposal is saying a third-party can be a personal health application (PHA) and that it is handled within the Right of Access. We support patient's ability to access their health information, however, you are exposing health care information to tech platforms, developers and others. Pew's survey found that people are supportive of using health apps – only a third of patients expressed concern about privacy. However, that number doubled when patients realized that HIPAA did not protect that information. Apps collect your information and share it with data brokers. The data brokers compile it into a profile about people. When these profiles are created, it creates a gating opportunity where certain people are given advantages and others are not. We've seen this happen in housing – the federal housing agency has looked into practices from Facebook where some were not able to see opportunities for housing based on the profiles that were created. It benefits the whole industry to be thinking about this and how to bake trust into the use of PHA or other apps. From a physician perspective, we are concerned about protecting that physician-patient relationship. We can come up with all the innovative technology in the world, but when you don't have trust baked in from the beginning and privacy by design, we wind up not being able to take advantage of the innovation and ultimately, the individual and public health suffer. <u>We are looking for federal privacy legislation that will put strict guardrails around how data brokers and platforms can use data.</u>
    - **Deven McGraw:** <u>We need federal legislation.</u> States are stepping up to act, but that creates a patchwork of protection. We need to make sure the definition of a PHA is a tool designed for the consumer' use – because otherwise it becomes a trap door by which any entity that wants data can get it. Our comments are going to ask for greater clarity – like did the individual choose to establish this account, do they have full control of the information, can they close the account and take their data with them and have their information deleted. Ideally there

would also be requirements around privacy policies and transparency and attestations around that. Unclear whether OCR thinks they can extend that far.

Oral Request

- **Kristen McGovern:** HHS proposes to require covered health care providers to respond to an individual's "clear, conspicuous, and specific" request to direct their electronic health information to a third party, including if the request is orally made. What implications do you see from this part of the rule? Second, although this would make it easier for individuals to direct access to their health information, what implications (burden or resources) might this have for providers and patients?
    - **Peg Schmidt:** Currently, requests have to be in writing signed by the individual that tell us specifics. That requirement works well because it supports accuracy and verification requirements. There are so many things that could go wrong with an oral request and we are concerned that oral requests could lead to impermissible disclosures. If a request is given orally via the phone, someone on the other end will have to document that request themselves because they are not likely to be the one to carry out the request, meaning there could be opportunity to misinterpret the request. Also, a written request will document the starting request date. Could envision a situation where a complaint is made, but we don't have an original request from the patient that documents the initiation date. Also concern about what happens if a patient makes an oral request elsewhere in the organization other than the department in which the request will be processed. There are many things that could go wrong with oral requests.
    - **Deven McGraw:** I see so much potential for abuse with oral requests. Why require an institution to respond to an oral request, versus making an option not to require writing. If a person is standing right there maybe they shouldn't be forced to fill out an oral request. But if directing information to a third-party, would want that request to be documented. Also, I am particularly concerned about the new part of the rule where the ultimate recipient of the information can call and say their patient wants information sent. How do we know for a fact that the patient is requesting information?

Other Proposals – SUD/SMI Disclosures, IB Rules, Right to Inspect

- **Kristen McGovern:** What other proposals in the rule do you think will have the biggest impact on patients? Or on the way in which health care data is exchanged or shared with others, such as with family members?
    - **Laura Hoffman:** There is a proposal on disclosures of PHI related to substance use disorder (SUD), serious mental illness (SMI) and emergencies. The idea is to make it easier to share information related to those conditions including with family members. There is this widespread perception that HIPAA prevents clinicians from sharing PHI including about SMI with family members, caregivers, and close friends; that's not true. Clinicians can already share that information, however, there is significant misunderstanding with what HIPAA allows and requires. We keep trying to legislate around misunderstanding. Two key issues with proposal: 1) NPRM is seeking to change the standard when entities can share information about SUD or mental illness. Right now, it is up to a clinician's professional judgment about whether they want to share that information with someone who is asking. OCR and the Department of Justice (DOJ) have never brought any enforcement action on clinicians. Via the

NPRM, OCR wants to try to make it easier and give assurance to CE that they can share this information without fear. OCR has proposed to replace the "professional judgment" standard with a "good faith belief." The presumption is if you share information, OCR is going to presume you did the right thing, unless you did it maliciously or with bad faith. The "Good faith belief" is not limited to clinicians. Front desk staff, medical assistants or others in the facility can be asked for information and if they think it is in good faith, they would be permitted to share information. This presents some concerns, and could actually lead to harm. 2) Would allow CE to disclose PHI to avert a threat to health or safety when harm is "serious and reasonably foreseeable." The current standard is "a serious and imminent threat to health and safety." When we think about historically marginalized populations who are already disproportionate targets of law enforcement, what starts happening when the health care system says we can disclose PHI as long as there is a reasonably foreseeable threat. Not comfortable supporting a relaxed standard when there is rampant racisms and bias. Patients will hear this as "if I look like a threat, they will share my information" OCR needs to give more thought about the equity aspects of this proposal. 3) OCR asked whether there are non-emergency circumstances in which a CE would be permitted to disclose PHI. A lot of these proposals by OCR are well intentioned – but we have to make sure we aren't swinging the pendulum too far in the other direction.

- **Deven McGraw:** Will have to reassess comments regarding the emergency situation made by Laura because we hadn't thought of that before. OCR has not held it up its requirements under the 21st Century Cures Act to clarify how the business associate agreements (BAA) mesh with information blocking (IB) rules. If a BAA is what controls whether information can go to a patient, for example, then you have entities covered by IB who voluntarily contract themselves out of sharing in certain circumstances. We have asked OCR to acknowledge that it needs to respond to IB expectations so there aren't two offices' policies in conflict with each other.
- **Peg Schmidt:** See some operational impacts from allowing patients to take notes, images, photographs. OCR included "at the point of care" which I am interpreting as during your appointment. Support option to inspect PHI and oftentimes taking photographs are no issue. I am concerned about operationalizing that in a manner that will minimize the provider burden and maintain patient privacy. Concerned that requests made during the point of care will result in workflow disruption. Providers are there for responding to the clinical treatment of the patient; can't see how responding to access requests fits into their time and clinical workflow. Would also need clarity if a provider is objecting to being included a video for example.

Federal Legislation

- **Kristen McGovern:** For years, Congress has considered creating new privacy protections, but has not yet enacted new policies. What are the current policy levers to ensure that health data that moves outside of HIPAA remains protected?
    - **Deven McGraw:** There are not many policy levers. At the federal level you have the Federal Trade Commission (FTC). States can also weigh in. That's why we see voluntary codes of conduct that entities can attest to such as the CARIN Alliance Code of Conduct, the AMA has

developed best practices, CTA, CDT/EHI have also developed codes of conduct. This allows differentiation in the marketplace, but it's not as good as a law.

- **Kristen McGovern:** Once a patient says they want to share information with someone, it would be governed by the FTC or voluntary codes of conduct or state law if it applies. This is where Congress could step in with federal legislation.
- **Laura Hoffman:** Even further, FTC's authority is limited to unfair and deceptive trade practices. The FTC authority is fragile and has been weakened even more recently. The FTC is paying attention to these issues, but they are under-resourced. There are very few levers that exist in federal law currently.