ConnectedHealthInitiative

January 31, 2023

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue SW
Washington, District of Columbia 20201

RE: ***Connected Health Initiative Comments to the White House Office of Science and Technology Policy on Confidentiality of Substance Use Disorder (SUD) Patient Records [87 FR 74216]***

Dear Secretary Becerra:

The Connected Health Initiative (CHI) writes to provide input to the Department of Health and Human Services (HHS) on its proposal to modify its regulations to implement section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[1] HHS' steps to revise 42 C.F.R. Part 2 (Part 2) regulations comes at an important time, presenting the opportunity to improve and harmonize regulatory requirements over important information in a way that provides vital protections to patients while responsibly enhancing health data flows in the continuum of care.

CHI is the leading effort by stakeholders across the connected health ecosystem to responsibly encourage the use of digital health innovations and support an environment in which patients and consumers can see improvements in their health. We seek essential policy changes that will help all Americans benefit from an information and communications technology-enabled American healthcare system. CHI is a longtime active advocate for the increased use of new and innovative digital health tools in both the prevention and treatment of disease, specifically regarding clinical trials and investigations. For more information, see www.connectedhi.com.

Digital health technologies can, and must, play a key role in addressing the national opioid epidemic through substance use disorder (SUD) treatment. Data and clinical evidence from a variety of use cases continue to demonstrate how the connected health technologies available today improve patient care, prevent hospitalizations, reduce complications, and improve patient engagement, especially in the SUD context.[2]

---

[1] 87 FR 74216.

[2] Oesterle TS, Kolla B, Risma CJ, Breitinger SA, Rakocevic DB, Loukianova LL, Hall-Flavin DK, Gentry MT, Rummans TA, Chauhan M, Gold MS. Substance Use Disorders and Telehealth in the COVID-19 Pandemic Era: A New Outlook. Mayo Clin Proc. 2020 Dec;95(12):2709-2718. doi: 10.1016/j.mayocp.2020.10.011. Epub 2020 Oct 21. PMID: 33276843; PMCID: PMC7577694.

Digital and connected health tools, including wireless health products, mobile medical device data systems, telemonitoring-converged medical devices, and cloud-based patient portals, can fundamentally improve and transform American healthcare. By securely enabling the exchange of health information and incorporating patient-generated health data (PGHD) into the continuum of care, these tools can render meaningful and actionable outcomes.

Part 2 currently imposes different requirements for SUD treatment records than the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, Breach Notification, and Enforcement Rules, at times subjecting HIPAA Covered Entities and their Business Associates that maintain both PHI and Part 2 records to both rules. Notably, any disclosure of substance use disorder records protected by Part 2 would also, generally, require the consent of the individual who is the subject of such information. Unless and until the Part 2 regulations are revised to conform with the HIPAA Rules, in any case where a disclosure of such Part 2-protected information was necessary, healthcare providers and their Business Associate would risk violating Part 2 and be subjected to criminal penalties if they complied with a required disclosure under the HIPAA Rules. As such, it is likely that most health care providers or Business Associates put in the unenviable position of complying with either Part 2 or HIPAA would choose Part 2, given the criminal liability. In this vein, we strongly suggest that HHS review not only the HIPAA Rules as part of the effort to increase care coordination and continuity of care, but also the Part 2 regulations, which create significant burdens on such efforts. In practice, this regulatory regime often leaves providers lacking the necessary access to vital information when treating patients.

CHI strongly supports the revision of Part 2 regulations to ensure that healthcare providers can communicate effectively with each other and with the friends and family members of patients suffering from substance use disorders, thus allowing researchers to study the national problem of opioid abuse. Revisions made by HHS to Part 2 regulations should be made in light of the specific limitations on disclosure of protected health information (PHI) by the HIPAA Privacy Rule including to employers and law enforcement. Specific limitations that should be considered include (1) the requirements to implement administrative, physical, and technical safeguards to ensure the confidentiality, availability, and integrity of such information under the HIPAA Security Rule; (2) the requirements to notify individuals, HHS, and, in some cases, the media, of a breach of such information under the HIPAA Breach Notification Rule; and (3) the increased penalties for disclosures and other violations under the HIPAA Enforcement Rule. Because HIPAA sets the baseline for protection, such a baseline should apply to substance use disorder treatment information as well. Fortunately, the inclusion of Section 3221 of the CARES Act enables HHS to bring about greater alignment to certain Part 2 requirements by bringing them closer to HIPAA requirements, enabling those subject to Part 2 to use and disclose relevant SUD. CHI encourages updates consistent with the above.

Further, CHI encourages HHS to enable the responsible use of new technologies to facilitate SUD treatments while protecting patient privacy and safety. For example, cloud

computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[3] In simple terms, cloud computing allows organizations to leverage servers and access computer system resources—such as computing power, storage, and network power—to meet their changing technology needs. Several HIPAA Covered Entities and Business Associates have adopted cloud computing solutions in accordance with guidance on HIPAA.[4] However, most cloud computing providers cannot comply with Part 2 because they cannot sufficiently operationalize certain requirements within Subpart E of Part 2 (Court Orders Authorizing Disclosure and Use), effectively removing the use of cloud computing services as an option when Part 2 applies.

In an effort to appropriately balance law enforcement and other legal requests with customer and patient privacy rights, cloud computing providers typically first notify customers of any legal requests for their information and redirect the requests to the customer. This practice is encouraged by the U.S. Department of Justice. That said, there are instances where cloud computing providers are subject to gag orders in which they are unable to inform customers of these requests. In such situations, cloud computing providers typically review the validity of the request and either respond or challenge the demand in court. One concern with Subpart E of Part 2, however, has been that it requires that holders of SUD patient records disclose these records only if a court order is accompanied by a subpoena or similar court-issued legal mandate. The burden of ensuring that the requestor has the appropriate subpoena and court order falls to the SUD record holder, but cloud computing providers do not have standing access to customer data stored within their cloud. As a result, cloud computing providers cannot ascertain if the legal request relates to a customer's SUD information. Further complicating the matter is the fact that Part 2 programs are not necessarily readily ascertainable by customer name or contracting entity and are often part of a larger entity whose operations are not all subject to Part 2. For example, in addition to standalone facilities, Part 2 programs may be embedded within health systems and other healthcare providers, behavioral health organizations, and state and federal agencies, many of which have significant cloud operations and leverage cloud computing services and solutions. Because cloud computing providers cannot assess whether a Part 2-compliant court order and subpoena are required without compromising the privacy and integrity of the data, CHI requests that protections be added within 42 C.F.R. § 2.66 for a "person holding the record" who coordinates with the SUD data owner (to the extent permitted by the legal request) and, despite such coordination, when permitted, unknowingly makes a record subject to Part 2 available in response to an investigatory court order or subpoena, including limitation of liability

[3] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology* (2011), available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[4] HHS Office of Civil Rights, *Guidance on HIPAA & Cloud Computing* (last updated December 23, 2022), available at https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html.

against civil and criminal penalties set forth in 42 C.F.R. § 2.3. The nature of cloud computing has required similar protections in other bodies of law such as the Stored Communications Act, a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" by electronic communication services and remote computing services, that expressly provides civil immunity to cloud computing providers.

The provisions within 42 C.F.R. §§ 2.31 and 2.33 suggest that if a recipient of SUD patient records receives them in reliance on consent for treatment, payment, and health care operations, the recipient (e.g., another HIPAA Covered Entity or Business Associate) can use or disclose the SUD patient records in accordance with the HIPAA privacy rule, except for uses and disclosures for civil, criminal, administrative, and legislative *proceedings against the patient*. Law enforcement and other legal requestors of SUD patient records may not be forthcoming about the nature of the proceedings. Further, the number of record requests cloud computing providers field (nationally and globally) is significant, necessitating a streamlined process to ensure that any requests for records do not relate to proceedings against the patient. For these reasons, CHI requests that HHS allow cloud computing companies to, at their discretion, require requestors to certify or attest that, to the best of the requestor's knowledge, SUD patient records are not part of the request or the information sought will not be used as part of proceedings against a patient of a Part 2 program. We further request that HHS allow cloud computing companies to rely on such certifications or attestations of requestors when making disclosures in response to an investigatory court order or subpoena. CHI appreciates the opportunity to submit its comments to HHS and urges its thoughtful consideration of the above input.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Regulatory Policy Associate

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005