ConnectedHealth

May 6, 2021

Attention: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement NPRM, RIN 0945-AA00
U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, SW
Washington, District of Columbia 20201

RE: *Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement (Docket No.: HHS-OCR-0945-AA00*)

The Connected Health Initiative (CHI) appreciates the opportunity to respond to the Department of Health and Human Services (HHS) Office for Civil Rights' (OCR) Notice of Proposed Rulemaking (NPRM) proposing modifications to the Standards for the Privacy of Individually Identifiable Health Information (Privacy Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).[1]

I. Introduction & Statement of Interest

The Connected Health Initiative (CHI) is the leading effort by stakeholders across the connected health ecosystem to enable the responsible deployment and use of digital health tools throughout the continuum of care, supporting an environment in which patients and consumers can see improvements in their health. Across a range of touchpoints in the healthcare ecosystem, we seek essential policy changes that will enable all Americans to realize the benefits of an information and communications technology-enabled American healthcare system. For more information, see www.connectedhi.com.

[1] 86 FR 6446.

CHI is a longtime active advocate for the increased use of telehealth and remote monitoring. For example, in addition to serving as a leading advocate across the Department of Health and Human Services as well as other agencies, CHI is an appointed member of the American Medical Association's (AMA) Digital Medicine Payment Advisory Group, an initiative bringing together a diverse cross-section of 15 nationally recognized experts that identifies barriers to digital medicine adoption and proposes comprehensive solutions revolving around coding, payment, coverage and more.[2]

II. The Connected Health Initiative's Commitment to Protecting Sensitive Health Data and the Need for Clarity Under HIPAA

No data is more personal to Americans than their own health data. Since October of 2009, when the HITECH Act's enactment started requiring reporting of breaches, 1,473 health data breaches have occurred (a qualifying breach must affect 500 or more people). In 2015 alone there were 253 healthcare breaches representing a collective compromise of over 112 million electronic health records.[3] CHI members acknowledge this significant threat to Americans' most sensitive data and put extensive resources into ensuring the security and privacy of health data to earn the trust of consumers, hospital systems, and providers.

The HIPAA privacy and security rules provide a set of minimum standards for protecting all electronic Protected Health Information (PHI) that a Covered Entity (CE) and Business Associate (BA) create, receive, maintain, or transmit.[4] The concerns addressed by these laws are taken seriously by CHI members, who in turn work to meet the letter and spirit of the law. However, HIPAA privacy and security rules and guidance applicable to mobile apps have not been updated since before the 2007 introduction of the iPhone. The persistent lack of clarity around HIPAA applicability in a mobile environment prevents many patients from benefiting from these services. As a result, many physicians are reluctant to receive health readings from their patients electronically, and hospital systems are discouraged from adopting patient-centered technologies. To date, clear guidance does not exist to explain whether physicians and patients can text or email each other.

[2] https://www.ama-assn.org/delivering-care/digital-medicine-payment-advisory-group

[3] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[4] 45 CFR Part 160; 45 CFR Part 164 Subparts A and C.

CHI is a longtime advocate for certainty and clarity regarding HIPAA requirements. For example, in 2014 we worked with Members of Congress to attain a public commitment from then-HHS Secretary Burwell to work with us to:[5]

- Provide up-to-date and clear information about what is expected of technology companies for compliance with the HIPAA rules, and identify the implementation standards that can help technology companies conform to the regulations;
- Provide more clarity on HIPAA obligations for companies and services that store data in the cloud; and
- Engage regularly with technology companies to provide compliance assistance.

Building on these commitments, CHI worked with OCR to develop and launch http://HIPAAQsportal.hhs.gov, a platform for mobile health developers and others interested in the intersection of health information technology and HIPAA privacy protection. This platform allows for any stakeholder to submit questions, offer comments on other submissions, or vote on how relevant a topic is with their identity remaining anonymous to OCR. Further, the platform provides a means for OCR to provide guidance and technical assistance to the digital health stakeholder community. CHI encourages OCR to continue to leverage this important platform moving forward in its efforts to advance value-based health care.

As we have emphasized in numerous congressional testimonies and filings, up-to-date and clear information about obligations under HIPAA is critical. HHS issued guidance with specific scenarios which may be helpful in a narrow range of circumstances.[6] However, CHI asserts that regulatory relief, or, at minimum, more guidance, is needed to address the use of new innovative modalities and software app-powered products and services that facilitate the flow of PHI. With advances in other key federal regulatory contexts to advance the uptake and use of digital health tools (e.g., new Medicare reimbursement for the use of innovative remote patient monitoring tools), OCR's efforts to improve the HIPAA rules could not come at a more vital moment.

CHI is appreciative of OCR's willingness to explore how to improve the HIPAA rules for the purposes of care coordination and to support the shift to value-based medicine. We note that this examination is linked to the recently released rules from the Office of the National Coordinator (ONC) regarding "information blocking" as required by the 21st Century Cures Act, as well as a health data interoperability rule proposal from CMS. Harmonization across regulatory requirements and enforcement bodies will be key as OCR continues to consider possible updates to the HIPAA rules.

[5] Letter from ACT | The App Association, et al., to Reps. Tom Marino and Peter DeFazio, U.S. House of Representatives (September 15, 2014).

[6] http://hipaaqsportal.hhs.gov/a/pages/helpful-links.

CHI believes that as a nation, the United States is not realizing meaningful interoperability in health data today. Our members continue to face barriers between systems, as well as exorbitant licensing fees, in order to access health data. Interoperability is a moving target because as technologies evolve, the interoperability of the data that fuels them will shift over time. Therefore, interoperability must be iterative, and it must evolve along with the tools it supports. Government's role should be to ensure that this evolution is possible and remains a pillar of healthcare policy in the United States. Guidance from ONC on how HHS will enforce interoperability under 21st Century Cures, for example, is a crucial component to making it a reality. Interoperability between electronic health records (EHRs), vendors, population health data sets, etc., remains difficult without enforcement guidance from ONC.

As a general note, CHI believes that as OCR continues to work to improve the HIPAA rules to meet the needs of our changing industry and standard of care, it is imperative that OCR continues to work to ensure that the HIPAA rules do not unduly restrict the ability of CEs and BAs to use the most efficient and secure technologies in their operations. OCR can make major inroads in this respect by ensuring its regulations are technology neutral and outcome-driven (i.e., not locked into certain technologies). Past this formal consultation, we also urge OCR to engage in ongoing outreach to the range of stakeholders affected by the HIPAA rules, including the developers and range of users of connected health technologies.

III. Opportunities for the Office of Civil Rights to Enhance Connected Care Through Changes to HIPAA

Based on the above, we provide the following proposals for OCR to enhance a connected care continuum through reforms to HIPAA regulations.

a. *Promoting information sharing for treatment and care coordination*

The success of value-based care models depends heavily on bi-directional interoperability of healthcare data. To reward better outcomes and cost-effective approaches to care, providers must be able to utilize two-way application programming interfaces (APIs) to access, share, and make meaningful use of data about their patients. True interoperability involves not just the ability to access data, but also the ability to use it and manipulate it for the user's purposes and to benefit the patient. Knowing the whole story is important for providers and payers to understand the best treatment plan or prevention measures for patients, as well as for patients who seek greater engagement in their own care. Data from previous care settings becomes more important in value-based care because the viability of the provider depends on outcomes. The process to arrive at these outcomes becomes more efficient with care plans tailored to patients' medical history, genetics, and other factors.

This is especially true for providers in rural areas, where there are fewer physicians serving people who live farther away from care. Because of these geographic challenges, rural providers need data that shows which care plans or prevention and treatment measures are likely to work—and which don't—for the patients they see. Physicians spend about half their time doing paperwork and grappling with EHRs that create friction in their workflow. With fewer caregivers per capita and greater distances in less urban parts of the country, a system that traps physicians in endless stretches of administrative busywork is even more costly for rural patients. Caregivers simply don't have the time. Value-based care models enable providers in rural areas to divert resources to where and when they are needed most. The ability to access and analyze data on patients and populations is central to the ability to deliver cost-effective, high-quality care.

The private sector is making strides to assist with the interoperability of data across EHRs and other platforms, and a diversity of APIs are emerging to assist in bringing patient-generated health data (PGHD) into the continuum of care. For example, Health Level Seven International (HL7) is a standards-setting organization comprised of stakeholders from across the healthcare spectrum that has developed the Fast Healthcare Interoperability Resources (FHIR) standard. This is a "light, thin" standard that attempts to homogenize a relatively small subset of data formats and elements across different data users in the healthcare system. The FHIR standard also comes with an API to facilitate the exchange of EHRs. To effectuate adoption of FHIR, HL7 launched the Argonaut Project, which is also working on standardizing more granular aspects of data formatting and field entries.

It is important that incentives are aligned in such a way that they encourage the adoption of data field and format standards like FHIR, without strict mandates that could lock in standards that fail to keep pace with innovation. Data field and format standardization is likely to change as better data set management develops. Eventually, EHRs and other vendors should provide for two-way APIs that allow software developers to both download data from large sets held by the EHR *and* upload that data into the system. This two-way capability will be central to ensuring that 1) patients will benefit from newer innovations as quickly as possible and 2) interoperability will evolve more naturally with developments in software and hardware. Healthcare providers usually work with a wide variety of vendors, from device makers to software companies, and ensuring they all work together to paint an accurate and seamless picture for caregivers is critical, especially for value-based care models.

Potential changes to the HIPAA rules, as well as related rules such as the information blocking report and Trusted Exchange Framework and Common Agreement (TEFCA) proceeding, are key pieces to the larger shift towards a value-based system, and necessary for care coordination to function. OCR can make major inroads in this respect by ensuring its regulations are technology neutral and outcome-driven (i.e., not locked into certain technologies). Past this formal consultation, we also urge OCR to engage in ongoing outreach to the range of stakeholders affected by the HIPAA rules, including the developers and range of users of connected health technologies. For example, we recommend that OCR convene a working group to investigate whether current rules or internal practices within large organization hinders data sharing for research and population health initiatives due to misperceptions about HIPAA. These regulatory processes should result in more clarity for providers, technology makers, and patients to understand how all stakeholders can most efficiently make healthcare information interoperable without incurring liability, while allowing for seamless care coordination.

b. *HIPAA covered entities should be permitted, but not required, to disclose PHI to non-covered healthcare providers*

The HIPAA Privacy Rule should not be revised to require disclosures for any additional purposes besides to the individual when the individual exercises his/her right of access under the Rule, or to HHS for purposes of enforcement of the HIPAA Rules. Such revisions are not necessary, would significantly increase burdens on HIPAA Covered Entities and Business Associates, and would lessen the protections for the privacy of individuals' PHI.

First, the permissions under the HIPAA Privacy Rule suffice, and appropriately defer to state law requirements that are more stringent and that require disclosures of PHI in certain circumstances. Importantly, any disclosure of substance use disorder records protected by 42 C.F.R. Part 2 (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 for such, if they complied with a required disclosure under the HIPAA Rules. As such, it is likely that the majority of 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, as we discuss further in response to another question.

Rather than mandating disclosures for continuity of care and care coordination and given that interoperability of EHRs is still a significant challenge for the healthcare sector, HHS should consider incenting the use of alternative technologies to increase the sharing of PHI for care coordination and value-based care initiatives. For example, given the explosion in the use of cloud services in the healthcare sector, HHS could support the design and implementation of technologies that allow temporary access to specific PHI in a cloud for treatment, payment, and health care operations purposes by HIPAA Covered Entities and Business Associates. For example, Healthcare Provider A, or its Business Associate, could grant Healthcare Provider B with temporary and limited access to specific PHI in a cloud solution for a care coordination purpose, pursuant to a query by Healthcare Provider B. Given that all parties are covered by the HIPAA Security Rule and given the requirements for encryption of the PHI and the access controls to it, the risks to such technologies would be extremely low and the burdens would be significantly less than those associated with EHR interoperability or a required disclosure.

c. *CHI supports increased public outreach and education on existing provisions of the HIPAA Privacy Rule that permit uses and disclosures of PHI for care coordination and/or case management*

Additional guidance and education on the existing provisions of the HIPAA Rules would greatly help advance information sharing and the improvement of care coordination. However, as it stands, the guidance that has already been developed – in some cases – hasn't made its way to the intended audience. As we mentioned before, OCR has created key guidance for mobile developers and those interested in the intersection between information technology and healthcare. OCR's outreach focus is an educational campaign for that community, and we see vast improvement in the understanding, from connected health companies, of their roles and responsibilities under the HIPAA Privacy Rules.

Conversely, we do not see similarly-focused educational campaigns for the provider community or patients. This leads to continued confusion around how best to implement third party technologies into the care continuum. As such, our members routinely hear "no" from healthcare providers because of a continuing belief that privacy laws inhibit their ability to exchange information even when such laws, in fact, do permit information sharing. For example, some of our member companies, in forming relationships with health systems, encounter conflicting interpretations of HIPAA's requirements for a BA Agreement. Some health systems believe the rules require several BA Agreements to be entered into for various parts of the business, while other health systems insist on only one. Clear guidance, like those developed for mobile app developers, will help to facilitate information sharing and the adoption of connected technology.

CHI urges OCR to update their guidance for providers and physicians, and to undertake targeted educational campaigns to better reach their intended audience. We suggest that in order to address some of the "grey" areas physicians continue to encounter, such as whether HIPAA permits text messaging, how to distinguish between patient-directed third-party access to protected health information and a third-party access request for information, and even distinctions between how to share mental health information generated by a general medical facility versus substance use disorder (SUD) information generated in a Part 2 facility, OCR creates situational guidance similar to the "Health App Use Scenarios & HIPAA" guidance document from 2016. In creating these guidance documents, we urge OCR to strategize ways to alert physicians, patients, and other healthcare industry stakeholders to new and existing guidance during the development process, and in ways that target the intended audience.

d. *OCR should prioritize promoting parental and caregiver involvement and addressing the opioid crisis and serious mental illness*

CHI and its members are concerned with the growing opioid epidemic plaguing the United States. The Centers for Disease Control and Prevention (CDC) reports that 115 Americans die from opioid-related overdoses every day,[7] many of which result from patients fraudulently obtaining a prescription from a physician.[8] Unfortunately, the current regulatory regime has prevented new entrants, particularly American small businesses, that would provide newer and more innovative solutions to physicians and healthcare facilities at lower costs. CHI supports steps by OCR to reduce the regulatory burdens associated with addressing the opioid epidemic and should ensure that providers on the front lines of this war are not forced to ignore advancements in technology and improve care delivery and reduce costs.

[7] *See*, *e.g.*, Opioid Overdose Crisis, National Institute on Drug Abuse (las updated March 2018) Available at: https://www.drugabuse.gov/drugs-abuse/opioids/opioid-overdose-crisis#one.

[8] Drugs for Dollars: How Medicaid Helps Fuel the Opioid Epidemic: Report of the Committee on Homeland Security and Governmental Affairs (Jan. 17, 2018) Available at: https://www.hsgac.senate.gov/imo/media/doc/2018-01-17%20Drugs%20for%20Dollars%20How%20Medicaid%20Helps%20Fuel%20the%20Opioid%20Epidemic.pdf; Michael Collins, *Medicaid Fraud is Helping Drive Opioid Crisis, New Congressional Report Concludes*, USA Today (Jan. 17, 2018) Available at: https://www.usatoday.com/story/news/politics/2018/01/17/medicaid-fraud-helping-drive-opioid-crisis-new-congressional-report-concludes/1040695001/.

e. *Accounting of disclosures*

A natural effect of the HIPAA rules is burdensome reporting requirements that frustrate caregivers and patients. CHI agrees with OCR that new access reporting requirements may add undue burdens for covered entities without providing meaningful information to individuals.

With the implementation of the HITECH Act requirement regarding the accounting of disclosures, CHI believes that physicians and other HIPAA CEs should only be required to produce accounting of disclosure reports based off information maintained in an EHR that has the functionality to readily produce reports that are not burdensome to create and are most meaningful to patients.

OCR could propose to require that covered entities do periodic audits or allow individuals to request an audit for a specific time period. For example, an individual could request an audit of the uses and disclosures of the electronic health record (EHR) for a 30-day period, once a year, and the HIPAA Covered Entity could facilitate tracking of uses and disclosures of the individual's EHR for that length of time, pursuant to the request.

f. *Streamlining notice and consent of privacy practices*

CHI supports eliminating or modifying the requirement for CEs to make a good faith effort to obtain individuals' written acknowledgment of receipt of a provider's Notice of Privacy Practices (NPP). Requiring an organization to obtain acknowledgement of an NPP that is not comprehendible and does not provide meaningful choice or control for patients over their information does not promote privacy or confidence in the whole system.

Removing the written acknowledgement requirement would reduce administrative burden by decreasing the amount of paperwork to print and store; it would also limit unneeded compliance monitoring. However, CHI also believes that OCR should have appropriate safeguards to ensure that patients can access the information contained within an NPP as easily and clearly as possible. The level of detail included in describing uses and disclosures for healthcare operations should be adequate to alert the patient to the multiple categories for which their information is being used, particularly given that OCR has developed model NPPs.

CHI worked closely with ONC on their model privacy notice (MPN) for developers.[9] The MPN is a voluntary and openly available resource to help developers clearly convey information about their privacy and security practices to their users. This approach aims to make it easy for a patient to understand how their privacy is being protected, and how and why their data is being used. CHI encourages OCR to take a similar approach with NPPs.

g. *Additional ways to remove regulatory obstacles and reduce regulatory burdens to facilitate care coordination and promote value-based health care transformation*

CHI offers the following further proposals for HHS and OCR action that will modernize and improve the HIPAA construct while strengthening patient safety:

Issue Guidance to Clarify the Use of Text Messaging & Chat Services

CHI repeatedly requested that OCR provide specific guidance on text messaging between the provider and the patient. Speaking at the HIMSS Health IT conference in Las Vegas on March 6, 2018, the director of OCR said that healthcare providers may share PHI with patients through text messaging but acknowledged that CEs and their risk managers are hesitant to do so in the absence of formal guidance from OCR. We appreciate previous guidance from OCR and ONC on the use of email, which increased understanding of how PHI can be transmitted electronically while still complying with HIPAA.[10] We encourage OCR to issue similar guidance specifically related to text messaging and chat services like Microsoft Teams as soon as practicable. Such guidance would help CEs understand how they may or may not use text messaging and chat services during patient care, including care coordination and communication with family and caregivers, and decrease fear of HIPAA violations leading to OCR enforcement. Similarly, CHI encourages OCR to provide clarity as to how push notifications will be treated under HIPAA.

[9] https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn.

[10] *Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?*, available at https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html; *Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?*, available at https://www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/index.html; and *Guide to Privacy and Security of Electronic Health Information*, available at https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

Business Associate Agreements

For the technology developer community, there continues to be questions around the requirement of BA agreements (BAA) and a lack of transparency around required content in these agreements. Specifically, there continues to be a lack clarity of sample BAA language around the topics developers care about, such as cloud storage and PGHD. CHI strongly encourages OCR to provide sample BAA language for both developers and providers providing such clarity, as well as guidance specifically for providers as to when they need a BAA with an external technology partner.

Connected Device Maintenance Via an App

Some questions around connected device maintenance and authorization created unnecessary steps that disrupt treatments and care continuums. CHI encourages OCR to provide clarity for the following scenario:

> A physician provides their patient with a medical device. The company that created the medical device wants to monitor the maintenance of the machine. All of the information collected by the device that is sent to the physician is covered under a Business Associate agreement. Can the company that created the medical device receive information about the maintenance/operation of the device so that they can alert the patient when a part *needs* to be replaced, etc.? How would that work? Would the device maker have to get the patient to opt-in? Does it require a patient portal or separate app for the patient?

Ensure the Continued Use of Cutting-Edge Encryption in Protecting PHI

Fully leveraging technical measures, including end-to-end encryption (defined as a set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key), is a critical element to protecting PHI. The use of encryption is critical to meeting obligations under the above-noted HIPAA security and privacy rules. More broadly, encryption enables key segments of the economy—from banking to national security—by protecting access to, and the integrity of, data. Encryption's role should not be understated – without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised. We strongly urge OCR to reinforce the important role encryption has in protecting PHI. Further, we strongly encourage OCR to issue guidance on the use of end-to-end encryption services for leading healthcare tools such as Apple FaceTime and other applications that allow video chats.

Artificial Intelligence (AI) in Health Care

CHI encourages OCR to ensure that the revised HIPAA regulations do not curtail AI innovations by taking a technology-neutral approach to any regulation, and that OCR ensure (through future guidance or rulemaking) that innovators have clarity as to when HIPAA rules may be triggered. Any policy framework that includes AI should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks must be scalable and assure that an individual's health information is properly protected, while also allowing the flow of health information. With proper protections in place, policy frameworks should also promote data access, including open access to appropriate machine-readable public data, development of a culture of securely sharing data with external partners, and explicit communication of allowable use with periodic review of informed consent.

CHI urges OCR to review the output of the CHI Health AI Task Force, which has formulated policy recommendations to regulators that address the role of AI in healthcare.[11]

42 CFR Part 2

Relatedly (and raised by OCR in its Request for Information that informed this NPRM), HHS should revise the 42 CFR Part 2 ("Part 2") regulations in favor of HIPAA's requirements for PHI, not only for purposes of deregulation, but also for purposes of ensuring that healthcare providers can communicate effectively with each other and with the friends and family members of those patients suffering from substance use disorders, and that researchers can study the national problem of opioid abuse. HHS should consider whether Part 2 requirements are necessary any longer, given: the specific limitations on disclosure of PHI by the HIPAA Privacy Rule including to employers and law enforcement; the requirements to implement administrative, physical, and technical safeguards to ensure the confidentiality, availability, and integrity of such information under the HIPAA Security Rule; 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 the increased penalties for disclosures and other violations under the HIPAA Enforcement Rule. HIPAA sets the baseline for protection, and the baseline should apply to substance use disorder treatment information as well.

[11] https://actonline.org/2019/02/06/why-does-healthcare-need-ai-connected-health-initiative-aims-to-answer-why/.

An Approach by OCR Coordinated with Other HHS Existing and Developing Rules and Requirements

CHI strongly encourages OCR to ensure that its efforts to reform HIPAA regulations (and its enforcement of HIPAA) are in coordination with other HHS mandates on the healthcare sector, including but not limited to regulatory requirements on transparency, surprise billing, advance explanation of benefits notifications, and interoperability. OCR's HIPAA regulations should be harmonized with such rules, and avoid creating unnecessary burdens.

IV. CHI Views on Specific Proposals in the OCR Notice of Proposed Rulemaking

Based on the above, CHI offers the following on specific proposals in the NPRM:

- Definitional issues:
    - CHI supports OCR aligning definitions of electronic health information (EHI) and electronic protected health information (ePHI) into its definition of an EHR. Currently, there is a lack of alignment between EHI and an EHR in the rules, the NPRM proposes to expand the scope of EHI (only). OCR should ensure that EHI, ePHI, and EHR definitions under HIPAA align and complement each other, which would promote harmonized terminology and understanding of HIPAA requirements across the ecosystem and avoid forcing stakeholders to make arbitrary distinctions between EHI, ePHI, and an EHR.

      Further, CHI encourages OCR to include billing records in the definition of an EHR only to the extent ePHI includes billing information and is included in a designated record set.
    - CHI urges OCR to ensure that any health plan requesting, accessing, or maintaining patient medical records to provide "care coordination" or "case management" to meet the threshold of creating and maintaining an EHR.
    - CHI supports greater transparency for patients that will enable them to make better-informed decisions about their own health data. To this end, CHI urges OCR to incent those entities best positioned to inform patients about the benefits and risks of sharing their health data. For this reason, CHI does not support the OCR proposal for a covered healthcare provider to be required to inform an individual who requests that PHI be transmitted to the individual's personal health application of the privacy and security risks of transmitting PHI to an entity that is not covered by the HIPAA Rules, as those providers are often not fully informed about such privacy and security risks. Instead, we urge OCR to advance easily-understood attestations about data governance, and to advance and educate on

consensus solutions such as the MPN. Further, consistent with our suggestions above, revisions to the definition of personal health applications can be a vehicle for promoting transparency for patients and other stakeholders.

- Individuals' Right of Access: CHI supports OCR's proposal to allow individuals to record PHI as part of the Privacy Rule access right. We urge OCR to direct CEs to develop policy and procedures as appropriate to scope such activities (e.g., ensuring that a patient does not accidentally compromise another patient's privacy). While efficacy of data will always be a concern, CHI supports enhanced collection of patient-generated health data that will augment engagement in care and improve outcomes. Further, CHI supports enhancing the ability of patients to inspect their health data though such allowances should be feasible and practical (e.g., "ready availability" of health data should reflect that not all data is available on demand, such as with respect to lab results).
- Individuals' Requests – Form and Format: With respect to the form and format required for responding to individuals' requests for their PHI, CHI urges OCR to incent those entities best positioned to inform patients about the benefits and risks of sharing their health data. CHI does not support the OCR proposal for a covered healthcare provider to be required to inform an individual who requests that PHI be transmitted to the individual's personal health application of the privacy and security risks of transmitting PHI to an entity that is not covered by the HIPAA Rules, as those providers are often not fully informed about such privacy and security risks. Instead, we urge OCR to advance easily-understood attestations about data governance, and to advance and educate on consensus solutions such as the MPN.
- Fee Proposals: CHI opposes any unreasonable specific fees being charged to patients for copies of PHI. The current rule allows for reasonable fees that correspond to the costs associated with meeting such requests. CHI recognizes that responding to such requests may, in some circumstances, cause a CE to incur costs. However, fees should not be charged to patients for accessing their information through a patient portal or other internet-based method. Further, such an allowance from OCR should not enable the continued insistence of CEs to provide paper-only records and charge $20 (or sometimes more) for such a printout. We strongly encourage OCR to shift the healthcare system away from such legacy practices that have no connection to advancing patient access or safety, and to incent the waiving of fees being assessed to patients for access to their own health data in all circumstances possible.
- Business Associate Disclosures of PHI (45 CFR 164.502(a)(4)(ii)): CHI supports the OCR proposal to clarify 45 CFR 164.502(a)(4)(ii) to specify that a BA is required to disclose PHI to the CE so the CE can meet its access obligations, but that if the BA agreement provides that the BA will provide access to PHI in an EHR directly to the individual or the individual's designee, the BA must then provide such direct access.

- Reducing Identity Verification Burdens (45 CFR 164.514(h)): CHI supports OCR proposals to
    - Expressly prohibit a CE from imposing unreasonable identity verification measures on an individual (or his or her personal representative) exercising a right under the Privacy Rule.
    - Clarify within the regulatory text that unreasonable verification measures are those that require an individual to expend unnecessary effort or expense when a less burdensome verification measure is practicable for the particular CE.
- OCR's Proposed New Exception to the "Minimum Necessary" Standard (45 CFR 164.502(b)): CHI urges further consultations by OCR on its proposal to add an express exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered healthcare provider for care coordination and case management. OCR is encouraged to make sure that any new exceptions to the minimum necessary construct align with data minimization (that any information disclosed should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose of disclosure). We also urge for alignment and coordination with ONC given its inclusion of a "minimum necessary" condition within its information blocking rule's Privacy Exception.
- Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations (45 CFR 164.506): CHI appreciates OCR's proposal to create a new section of HIPAA that would expressly permit Covered Entities to disclose PHI to social services agencies, community based organizations, home and community-based service (HCBS) providers, and other similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management, either as a treatment activity of a covered health care provider or as a healthcare operations activity of a covered healthcare provider or health plan. CHI supports the sharing of PHI with such entities at the patient's request with appropriate safeguards in place to protect patient safety and privacy (e.g., the attestation construct discussed above; promotion of data segmentation techniques, etc.), and in alignment with requirements in the ONC information blocking rule.
- Eliminating Notice of Privacy Practices Requirements Related to Obtaining Written Acknowledgement of Receipt, Establishing an Individual Right to Discuss the NPP With a Designated Person, Modifying the NPP Content Requirements, and Adding an Optional Element (45 CFR 164.520): CHI supports OCR's proposals to:
    - Eliminate the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP) and to retain copies of such documentation for six years.

- Modify the content requirements of the NPP to clarify for individuals their rights with respect to their PHI and how to exercise those rights.

V. Conclusion

CHI appreciates the opportunity to submit comments to OCR and urges its thoughtful consideration of the above input. We look forward to the opportunity to further work with OCR and other stakeholders to improve patient safety and access, driving towards a truly connected care continuum.

Sincerely,



Brian Scarpelli
Senior Global Policy Counsel

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