

Board of Directors

Kristine Martin Anderson
Booz Allen Hamilton

William Bernstein, Esq.
Manatt, Phelps & Phillips,
LLP

Saurabha Bhatnagar, M.D.
UnitedHealthcare

Paul Brient
athenahealth, Inc.

Joe Corkery, M.D.
Google Cloud

Jennifer Covich Bordenick
eHealth Initiative &
Foundation

Paul Eddy
Wellmark

Kristin Ficery
Accenture

Daniel Garrett
WellDoc

Sarah Jones
Best Buy Health

Kris Joshi, Ph.D.
Change Healthcare

Amy McDonough
Board Chair
Fitbit

Susan Murphy R.N.
UChicago Medicine

Adam Pellegrini
CVS Health

Drew Schiller
Validic

Josh Schoeller
LexisNexis Risk Solutions

Roy Schoenberg, M.D.
Amwell

Laura Semlies
Northwell Health

Mona Siddiqui, M.D.
Humana

Eric Sullivan
Inovalon

Susan Turney, M.D.
Marshfield Clinic Health
System

Ashwini Zenooz, M.D.
Salesforce

eHEALTH INITIATIVE & FOUNDATION
ONE THOMAS CIRCLE, NW, SUITE 700
WASHINGTON, DC 20005
www.eHIDC.ORG
@eHEALTHDC
(202) 624-3270



May 6, 2021

The Honorable Xavier Beccera
Secretary
Department of Health & Human Services
200 Independence Ave, SW
Washington, DC 20201

RE: RIN0945-AA00

Dear Secretary Beccera:

The eHealth Initiative (eHI) appreciates the opportunity to comment on the proposed rule entitled *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement*.

We are generally supportive of the notice of proposed rulemaking's (NPRM) proposals, and certainly of its broad intent: to facilitate patients' access to their own health information, and to promote information exchange to support care-coordination. Meaningful and useful patient access to health information has long been a goal shared by the various entities in the healthcare ecosystem, and we applaud the Office for Civil Rights' (OCR's) effort to improve this. We are also committed to supporting efforts to allow timely and robust information exchange with all members of a patient's care team.

However, we urge OCR and the administration to weigh carefully the privacy risks inherent in promoting greater patient access to protected health information (PHI), as well as the exchange of that information with an expanded array of actors and organizations, potentially without the patient's knowledge or consent.

Specifically, we write to comment on aspects of five proposals in particular: (1) the right of individuals to access their PHI; (2) the elimination of the requirement for a written acknowledgement of the notice of privacy practices (NPP); (3) prohibiting covered entities from imposing unreasonable verification requirements; (4) the right of patients to direct a covered entity to send PHI to a third party when request is clear, conspicuous, and specific; and (5) patient education regarding privacy risks

Rights of Individuals to Access their Personal Health Information

Shortening the Access Time Limits

In the NPRM, HHS proposes to shorten covered entities' required response time to no longer than 15 calendar days (from current 30 calendar days) with the opportunity for an extension of no more than 15 calendar days (from current 30-day extension period). Although eHI supports shortening time limits for responding to access requests, we believe the misalignment with the Office of the National Coordinator for Health IT (ONC) information blocking regulations will cause significant confusion among providers. Under the ONC Cures Act Final Rule, the infeasibility exception states that the actor must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible; therefore, an actor must respond to a requestor within 10 business days in order to not be in violation of the regulations. However, under proposals in this NPRM, covered entities would be required to respond within 15 business days. We urge HHS to issue further guidance to clarify timelines related to provider responses to patient request in both the Cures Act Final rule and this proposed rule.

Further, we would also note that the CMS Interoperability and Patient Access Final Rule requires certain payers to make certain data, including adjudicated claims and clinical information, available to third-party applications to retrieve within one day after a claim is adjudicated or encounter data is available. Because third-party applications can only access data at a patient's request, it is unclear how this one-day requirement in the CMS Interoperability and Patient Access Final Rule correlates with the 15-day response requirement in the NPRM. We urge HHS to clarify this in order to ensure covered entities are prepared to comply with both regulatory requirements.

Improving Access to PHI by Specifying When Access Must be Free of Charge

HHS proposes to prohibit covered entities from charging fees for access when an individual inspects PHI about the individual in person or accesses an electronic copy using an internet-based application method. Again, while we agree with HHS' intent in providing these clarifications, we urge consideration of the regulatory inconsistencies and potential to increase provider burden.

The ONC Cures Act Final Rule and CMS Interoperability and Patient Access Final Rule, along with other federal regulations, require certain providers and payers to implement APIs to allow patients access to their own health information. Under the rules, actors are allowed to charge fees as long as the fee is not prohibited under the HIPAA Privacy Rule for individuals' requests for access to their protected health information. The NPRM proposes to clarify that a covered entity may not impose a fee when an individual accesses electronic protected health information maintained by or on behalf of the covered entity using an internet-based method such as a personal health application. The NPRM also proposes to clarify that a covered health care provider may impose a reasonable, cost-based fee for an access request to direct an electronic copy of protected health information in an electronic health record to a third party. While we agree that all fees should be cost-based and reasonable when a patient is exercising his or her right of individual access, including through a patient portal or other internet-based method, we also acknowledge that this creates inconsistencies between HIPAA and the ONC and CMS Final

Rules with regard to third-party access to patient information. Under the ONC and CMS Final Rules, actors are allowed to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met; however, because of HIPAA requirements, providers would only be allowed to charge fees associated with labor to aggregate and make data available to third parties. We urge HHS to take this into consideration in finalizing the NPRM and find a solution that does not pass along excessive costs to patients, but evens the playing field between health IT vendors, third-party applications, and providers.

Changes to Requirements Regarding the Notice of Privacy Practices

eHI supports the proposal to eliminate the requirement for written acknowledgement of receipt of the NPP for covered health care providers with a direct treatment relationship with a patient. We agree that this can impose unnecessary paperwork burdens, workflow congestion, and unintended confusion on the part of patients, who may not be aware of what they are signing or believe that their signature is on this acknowledgment form is necessary in order for them to receive care.

We are also supportive of the proposed NPP content adjustments, in particular the header that would clarify to individuals what the notice includes, how to access their health information, how to file a HIPAA complaint, and their right to receive a copy of the notice and to discuss its contents with a designated person. Educating patients both on their right of access and how to exercise it is a priority of eHI and our work, and any effort to clarify these issues at the point of care, particularly by a trusted provider, is one we encourage.

Third Party Access to PHI

eHI supports the proposal to clarify and expand the right of a patient's access to his or her own health information by requiring that a covered health care provider transmit an electronic copy of PHI in an EHR to a third party at the patient's "clear, conspicuous, and specific" request, which may be orally or in writing. eHI recognizes the value of individuals' engagement in their own care, which is made possible by access to their own data and subsequent engagement, should they choose, with the ever-increasing array of health and wellness technologies. Although the legal protections of health data outside of HIPAA-covered entities are lacking and in dire need of legislative action, individuals deserve the autonomy of being an active member of their own care team and to easily direct the flow of their health information to the parties and platforms of their choosing.

We do recognize, however, that providers are not primarily in the business of health information exchange with third parties, and that this proposal must therefore be implemented in such a way that any additional affirmative obligations for them are minimized. Importantly, the provision, if adopted, should make clear that health care providers bear no responsibility for the use of PHI disclosed to third parties at an individual's request. As discussed in more detail below, there is an important patient education component of all of these proposed expanded-access provisions.

Prohibiting Unreasonable Verification Requirements

eHI supports the intent behind this proposed modification to address the types of anecdotal examples included in the rule of covered entities imposing burdensome verification requirements (e.g. requiring individuals to receive their PHI in person, or obtain notarization for a written request). We would underscore the importance of maintaining and enhancing robust remote verification protocols as covered entities are likely to encounter increasing requests for access under the interoperability rule, and as PHI is transmitted beyond entities subject to HIPAA.

Necessary Patient Education Regarding Privacy Risks

eHI appreciates the Department's request for comment on whether a covered health care provider should 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. Although eHI is broadly supportive of increasing individuals' access to their own data, including by directing it to a third-party app of their choosing, we also recognize the concomitant risks of removing health data from HIPAA protections.

Since 2020, with the support of the Robert Wood Johnson Foundation (RWJF) and in partnership with the Center for Democracy and Technology (CDT), eHI has been engaged in an effort to shore up protections for health data held by health technologies that are not HIPAA-covered entities nor business associates. Our Consumer Privacy Framework for Health Data was released in February of this year, and we are currently working to refine its data use standards and develop the accountability structure for companies who hold this data. We are also strongly supportive of new federal data privacy legislation that recognizes the proliferation of non-HIPAA covered health data and its under-protection.

Health care providers are historically the most trusted messengers when it comes to informing patients, including about privacy rights and risks. However, we recognize that the burdens on providers are already substantial, and expecting them to provide a legal overview of data protections to their patients in addition to care is unrealistic. That said, there is certainly a role for providers to play in making patients aware of the risks that arise when data leaves their provenance, and we urge the Department to work with stakeholders such as eHI on creative and innovative ways to partner with providers on patient education.

Conclusion

Thank you for your efforts to ease patient access to their health data and reduce provider burden. We look forward to continuing to work with you to ensure any final regulation strikes the right balance between the need for increased information flow to coordinate care and the privacy rights of individuals. Should you have any further questions, please contact Catherine Pugh at catherine@ehidc.org.

Sincerely,



Jennifer Covich Bordenick
Chief Executive Officer