May 6, 2021

Robinsue Frohboese, PhD, JD
Acting Director and Principal Deputy
Office for Civil Rights
Department of Health and Human Services
Washington, DC 20201

Dear Dr. Frohboese:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments in response to the Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement (RIN 0945-AA00) published in the Federal Register January 21, 2021. HIMSS applauds the Department's decision to review and modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The twenty-plus years that have passed since the passage and first round of HIPAA regulations have seen dramatic changes in technology and data usage. The Department's review has the potential to remove antiquated or unintended regulatory barriers to sharing protected health information (PHI) as a means to improve care coordination and interoperability, while ensuring the confidentiality, integrity, and availability of patient data.

HIMSS is a global advisor and thought leader supporting the transformation of health through information and technology. As a mission driven non-profit for more than 60 years, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and analytics to advise global leaders, stakeholders and influencers on best practices in health information and technology. With a community-centric approach, our innovation engine delivers key insights, education and engaging events to healthcare providers, governments and market suppliers around the world. HIMSS serves the global health ecosystem with focused operations across North America, Europe, the United Kingdom, the Middle East and Asia Pacific. Our members encompass more than 105,000 individuals, 480 provider organizations, 470 non-profit partners and 650 health services organizations.

Across our organization, HIMSS is committed to ensuring that HIPAA facilitates the transition to value-based health care by promoting care coordination and case management communications among individuals and covered entities and alleviating unnecessary burdens, all while continuing to protect the privacy and security of individuals' PHI. HIPAA-related regulatory barriers may impede the transformation of the health ecosystem from one that pays for procedures and services to a system of value-based health care that pays for quality care.

As a result of HIPAA, there is an ever-expanding role for patients and how they contribute to their own personal health journey. Combined with the recently implemented regulations from the Office of the National Coordinator for Health

Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS), HIPAA contributes to patients accessing and controlling their health information and placing them in a position of greater empowerment to direct their own healthcare.

Overall, HIMSS will continue to work across the Department of Health and Human Services (HHS) and Congress to ensure that we are progressing toward a comprehensive health privacy law that applies across the health ecosystem. Federal and state regulations surrounding health data privacy are being revisited, and new ways of thinking about the privacy of an individual's data are being developed in an effort to keep pace with advances in technology.

As new market entrants enter healthcare, how we think about data privacy broadly also needs to evolve. How HIPAA applies and intersects with other privacy regulations may be an unintended barrier for broader information sharing as well as efforts to better engage patients in their own care. The lack of educational awareness as well as the lack of clarity regarding the scope of HIPAA, who is obligated to abide by HIPAA, as well as how it is interpreted, enforced, and intersects with other privacy laws has created significant gaps in compliance and enforcement. Our nation needs a comprehensive health privacy law that encompasses all these issues from a broader perspective and one that is implementable.

We offer the following thoughts and recommendations for ensuring that HIPAA promotes the sharing of PHI while guaranteeing the confidentiality, integrity, and availability of patient data:

**Align HIPAA with Other Regulations Focused on Privacy and Data Sharing**

As HHS moves forward with implementation of the new interoperability regulations as well as Title 42 of the Code of Federal Regulations (CFR): Confidentiality of Substance Use Disorder Patient Records (Part 2) Regulation, the Department must ensure that any changes to the HIPAA Regulation are harmonized with other federal privacy regulations. These rules should be clear and concise, and avoid any redundancies, conflicts, or inconsistencies that may result in confusion and impede progress. Ideally, these rules should collectively encourage innovation and provide the right balance concerning the sharing of information to enable care coordination, interoperability, and foster medical advancements and innovation.

Federal agencies must work together to foster the development of robust, up-to-date, privacy and security frameworks and guidance to encourage widespread adoption, acceptance, and trust of new, innovative technologies that support the free flow of information between patients and providers. States also have a role to play in how their laws interact with federal data privacy regulations.

HIMSS created an infographic (Appendix A) that demonstrates HIPAA's scope and how other privacy laws that intersect with it draw our nation further away from clarity on when an individual's data can be shared, and the protections that exist in keeping that information secure. Health data privacy laws, at the federal and state levels, will need to evolve as the needs of patients shape new ways of delivering healthcare and technology progresses to assist in that transition.

The HIPAA Privacy and Security Rules govern how protected health information may be used and disclosed, as well as how it may be secured in terms of physical, technical, and administrative safeguards to ensure the confidentiality, integrity, and availability of information. Good cybersecurity practices help to ensure that data will be kept confidential, have integrity, and be available on demand.

Cybersecurity, a key responsibility of data stewardship, is a necessary predicate to data privacy, access, and usage. These elements cannot exist were it not for cybersecurity, especially within an electronic environment. Additionally, data should be protected, not just to preserve privacy, but also to protect the patient and maintain safety. Recognizing the value of such data, we need to have robust cybersecurity practices (and policies) in order to ensure interoperability of healthcare data as well. People, processes, and technology must work in tandem with each other.

As such, when discussing harmonizing federal health data privacy laws, a 2017 Report from the Health Care Industry. Cybersecurity Task Force entitled, *Report on Improving Cybersecurity in the Health Care Industry*, included a key recommendation (1.3) to "(r)equire federal regulatory agencies to harmonize existing and future laws and regulations that affect health care industry cybersecurity."

The Report discusses how the healthcare industry faces significant challenges due to federal and state cybersecurity laws and regulations that can be inconsistent and establish conflicting standards of compliance. These laws work in conjunction with laws on data breach notification, data disposal, and data security, often dictating different responses than federal laws. Additionally, complying with these laws and regulations is resource intensive and creates financial burdens for the health ecosystem.

Overall, it is important to note how privacy and security are inextricably linked and that the concerns in the cybersecurity world are even more manifest with respect to privacy, HIPAA, and the interoperability regulations. For this reason, HIMSS supports greater alignment and harmonization of federal and state health data privacy laws, including HIPAA.

**Support for Modifications to Individual Access Rights**

HIMSS is supportive of the explicit modifications to the HIPAA Privacy Rule that include straightforward guidance for providers to administer PHI transfer to patients. The improvements set forth within this Proposed Regulation allow for more efficient information sharing with the patient's provider of choice, at a time during the care experience that enhances optimal care delivery. HIMSS applauds the steps OCR has taken to document in official guidance, processes, and authorizations to put more power in the hands of patients. The proposed modifications related to patients' right to access are an opportunity to gain a greater level of transparency in PHI processes, while asserting patient preference in the level of access. An example of greater transparency from this Proposed Regulation would be a covered entity informing a patient of their expressed right to view and document a health record via photograph, in real-time, during a clinical encounter. Patients may not completely understand that

OCR is proposing to give them this right. Overall, OCR's proposed changes accomplish the objective to bring forth more clarity around PHI transfer to patients.

***Strengthening the Right to Inspect with the Express Right to Take Notes, Videos, and Photos to Capture PHI***

HIMSS believes this expressed patient right is a necessary solution that will result in the immediate capture of information during the care encounter at the patient's discretion. By expanding individuals' rights to access their PHI, HIMSS is optimistic that these modifications—working in concert with the provisions outlined in ONC's Information Blocking Regulation—will ultimately help curb the frequency of this issue. However, it is imperative that the necessary education and clarity about these changes be made available to providers and their patients.

The Final Regulation must include details on patient education opportunities, particularly around the patient right of access to their personal data. As It is often left to the provider to educate the patient of their rights, patients need to clearly understand that they have a right to the information in their record to ensure they receive timely care as well as minimize the risk of undergoing duplicative tests, procedures, and other inappropriate services.

HIMSS will continue to advocate that HHS identify innovative ways to educate the public and providers about the scope and reach of HIPAA. Patient education regarding access rights is necessary as the HIPAA Privacy Regulation works hand-in-hand with the new interoperability regulations, particularly the information blocking provisions.

OCR asks a pertinent question about whether conditions or limitations should apply to ensure that a covered health care provider does not experience unreasonable workflow disruptions when providing this access. We note that clinicians' offices may need to develop contingency plans that ensure the privacy and security of other patients' PHI when providing a patient access to their own information during an in-office visit. HIMSS wants to work with the agency to ensure clinicians can provide patients with true access to their PHI while safeguarding the privacy of other individual's health records. Ideally, this must be done while minimizing clinician and staff burden and unnecessary workflow disruptions. As more care is delivered via telehealth, OCR may want to explore the privacy and security protocols that are needed during care delivery through other modalities as well as with in-person care.

OCR's policy changes in this area are overwhelmingly positive and would eliminate the persistent barriers that individuals face when seeking to inspect or obtain copies of their PHI. However, the agency needs to allow covered entities to establish a balance between patient access and potential workflow disruptions.

Covered entities should be permitted to impose requirements to ensure that an individual records only PHI in the designated record set to which the individual has a right of access, which could reside or be maintained in multiple health IT systems, beyond electronic health records (EHRs). In addition, a covered entity should be able to establish reasonable policies and safeguards to ensure that an individual's use of

personal resources minimizes disruptions to their covered operations, and the access provided to an individual is not used in a nefarious manner. However, the overarching concern must remain that a covered entity not be permitted to establish policies and safeguards that impose unjustified or unreasonable barriers to individual access.

***Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access***

HIMSS supports the proposed prohibition on imposing unreasonable measures on an individual that creates a barrier to or unreasonably delays the individual from obtaining access. We believe that if the form and format requested is "readily producible," including copies of electronic PHI (ePHI), the request must be granted in that format and within the proposed timeframe.

In addition, we endorse the proposed requirement of "as soon as practicable," but in no case later than 15 calendar days after receipt of the request, with the possibility of one 15 calendar-day extension. This proposal is a reasonable measure of timeliness regarding a request for ePHI. HIMSS would favor establishing this standard as a floor that would not preclude a covered entity from providing records in a shorter timeframe.

Administrative barriers related to undue delay in producing copies of PHI and ePHI and transferring the content from one covered entity to another run the risk of unnecessary lags in care, leading to preventable hurdles in receiving quality care at the time it is most needed. While more restrictive state laws may still exist that potentially pose the threat of slowing down the flow of information, modifications in this rule will help to set a positive precedent. We applaud OCR for taking steps to clarify its guidance is geared towards getting patients their data in a timely manner, without administrative procedures serving as an impediment.

***Addressing the Individual Access Right to Direct Copies of PHI to Third Parties***

HIMSS generally supports OCR's proposal to create a separate set of provisions for the right to direct copies of PHI to an authorized third party. Individuals' ability to access and direct disclosures of their health information is key to their care coordination. We encourage OCR to continue to work closely with stakeholders as the scenarios involving third parties evolve with the advancement of technology.

***Adjusting Permitted Fees for Access to PHI and ePHI***

We find the proposed fee structure consisting of two elements based on the type of access request is appropriate as long as it remains transparent and it is clearly specified to the patient upon a request for PHI and ePHI. We find having this type of fee structure readily available will further bolster the notion of transparency. If publicly available, the patient will see when covered entities cannot charge a fee and when allowable costs are in line with the request's circumstances.

For example, we believe it is reasonable to impose a fee that would encompass the labor of copying requested PHI, the supplies for mailing non-electronic copies, and the postage and shipping costs. Furthermore, we would encourage OCR to revise

language to recognize that manual effort is often necessary to compile requests, particularly for internet-based access by businesses and commercial third parties. As such, fees equivalent to the effort required that cover the costs of production should be allowed for these requests, as the current HIPAA Regulations require.

The Proposed Regulation would allow covered entities to manage the costs of producing, compiling, and sending PHI while ensuring maximum transparency.

***Eliminating the Requirement for Individuals to Provide Written Acknowledgment of Receipt of Notice of Privacy Practices***

HIMSS supports eliminating the current requirements related to the written acknowledgement of receipt of notice of privacy practices (NPP) and the retainment of that document. We believe these requirements can be sunsetted as long as there is an alternative that would support acknowledging a patient understands how to access their health information; file a HIPAA complaint; or confirms the patient's understanding that they have the right to receive a copy of the notice and opportunity to discuss the contents. We also support the proposed components in the NPRM, encouraging a covered entity to designate an individual to discuss the NPP. HIMSS believes this path may improve patients' awareness of their rights relative to privacy while decreasing administrative burden for the provider and staff.

**Refocus the Definition of EHR**

The Privacy Rule currently does not define the term "EHR." We recommend that the proposed definition be modified to focus more on the functions performed by an EHR and health IT systems more broadly. The definition in the Proposed Regulation is focused on "health-related information on an individual created, gathered, managed, and consulted by authorized health care clinicians and staff"—which would include information captured in EHR technology as well as many other health IT systems. OCR should focus its definition on how all health IT systems can support users in managing privacy as well as data sharing policies—specifically defining policies and protections for all relevant patient data, not the systems where it may or may not be captured. If OCR moves forward with its draft limited-scope EHR definition focused only on one system, it could potentially exclude data in other health IT systems that should be subject to the HIPAA Privacy Framework.

The data in a HIPAA designated record set may reside in or be maintained in multiple health IT systems, some specified as EHRs, but also encompassing laboratory information systems and payer systems. This point further underscores the need to focus a definition on the data itself--how it is managed under a governance structure, not the name of a specific system.

OCR should focus its EHR definition on the protection and accessibility of "health-related information on an individual," not the multiple systems that may include this information. Such a step will help ensure that there is consistency and clarity for HIPAA-covered entities that are seeking to protect patient privacy and enable broader sharing of "health-related information on an individual."

**Recommend Changes to the Personal Health Application (PHA) Definition**

The Proposed Regulation defines PHA as a service offered directly to consumers--the covered entity does not manage, share, or control the information, nor does the application developer manage the information on behalf of or at the direction of a health care provider, health plan, or another organization that collects or manages PHI. We encourage OCR to review this definition to ensure that it is inclusive of the expanding uses of PHAs. The most pressing question is how OCR defines "at the direction of."

The Proposed Regulation notes that a PHA is not acting on behalf of, or at the direction of a covered entity, and therefore would not be subject to the privacy and security obligations of the HIPAA Rules. In the course of a clinical encounter, a clinician may recommend a patient download a PHA to monitor personal health status, assist with fitness, or weight management. Under this scenario, would OCR consider the recommendation to be "at the direction of" a covered entity? If a clinician makes such a recommendation, how would OCR consider that PHA to be interacting with HIPAA?

We want to ensure that a PHA definition provides an opportunity to strengthen and amplify the clinician-patient relationship. OCR clarifies in the NPRM that the right of an individual to access electronic copies of their PHI can be fulfilled by transmitting an electronic copy of an individual's PHI to a PHA used by the individual. The interoperability efforts from ONC and CMS encourage the use of mobile applications to give individuals greater control of and access to their health information. OCR should use this definition to provide clinicians with more clarity on PHAs and take the necessary steps to ensure providers are empowered to make recommendations on PHAs that can help an individual improve their lifestyle and better manage their health.

**Ensuring an Individual Provides Permissioned Access for Disclosures to Third Party Entities**

HIMSS appreciates OCR's efforts to clarify the scope of covered entities' abilities 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 facilitate coordination of care and case management for individuals. The "wraparound" services that these entities can provide to individuals are critical if our health ecosystem and broader society are going to better address social determinants of health. The coordination of these services will ensure individuals are receiving the appropriate coordinated services and case management practices that they need for an outcomes-focused treatment plan.

We emphasize that disclosing an individual's information to a third party that may be operating outside of the confines of HIPAA should be done only with the authorization of that individual specifically for direct health and human services-related services. As the terms "community-based organization" and "HCBS providers" could consist of many different kinds of entities, it should be up to an individual (in consultation with a clinician or a health care organization) to determine the universe of entities that could be permissible recipients of their PHI.

When referral information is being disclosed, this universe of entities should be specifically defined organizations or networks and not undefined, unknown, or changing networks. This ensures the individual knows exactly where their information is being shared. In addition, as some of these third party recipients of PHI may be covered health care providers under HIPAA, HIMSS supports the idea that disclosures to these entities not be limited as they could be part of the discloser's own treatment and health care operations for an individual.

Ultimately, it should be up to the impacted individual to provide authorized access to their PHI for referrals of health-related services to outside entities.

**Balancing Patient Identity Verification Burden with Right of Access**

As OCR previously explained in guidance, the HIPAA Privacy Rule does not mandate any particular form of verification but generally leaves the type and manner of the verification to the discretion and professional judgment of the covered entity, provided its verification processes and measures do not create barriers or unreasonably delay an individual from obtaining access to their PHI. OCR emphasized that verification may be done orally or in writing and is often dependent on how the individual is submitting a request and/or receiving access.

HIMSS supports the flexibility that OCR is providing to minimize verification burden and focus on less burdensome and practicable verification measures. Such steps are appropriate and support broader policies to facilitate greater patient access to their information. We believe this flexibility also allows the option for a covered entity to adopt an identity management solution at its discretion, but by doing so would be going beyond a mandated requirement to implement such technology. We also support OCR's work to expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual (or his or her personal representative) exercising a right under the Privacy Rule.

HIMSS is a member of Patient ID Now, a coalition of healthcare organizations representing a wide range of stakeholders committed to advancing through legislation and regulations a nationwide strategy to address patient identification. As demonstrated by the coalition's newly-released Framework for a National Strategy on Patient Identity, we want to be a resource to OCR on these important topics moving forward.

Overall, HIMSS recommends that any changes to the HIPAA Regulation be harmonized with other federal privacy regulations. These rules should be clear and concise, and avoid any redundancies, conflicts, or inconsistencies that may result in confusion and impede progress. HIPAA's proposed modifications related to patients' right to access are an opportunity to gain a greater level of transparency in PHI processes, while asserting patient preference in the level of access. Patients must be in a position of greater empowerment to direct their own healthcare without compromising the privacy and security of that data. Under any scenario, the key principles are that the patient is involved, engaged, and at the center of any decision-making involving the sharing of their personal data.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact Ashley Delosh, HIMSS Senior Manager of Government Relations, at Ashley.Delosh@himss.org, or Jeff Coughlin, HIMSS Senior Director of Government Relations, at Jeff.Coughlin@himss.org, with questions or for more information.

Thank you for your consideration.

Sincerely,

Harold F. Wolf III, FHIMSS
President & CEO

Appendix A

# U.S. Privacy Policy Challenges

## Who must comply with HIPAA?

### Providers, such as:

Clinics

Dentists

Doctors and Nurses

Nursing Homes

Pharmacies

...but only if they transmit any information in an electronic form in connection with a transaction for which Health and Human Services has adopted a standard.

### Health plans, such as:

Company health plans

HMOs

Health insurance companies

Government programs*

*pays for healthcare, such as Medicare, Medicaid, and the military and veterans' healthcare programs

### A healthcare clearinghouse, such as:

Entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa

## U.S. Federal Privacy Laws

| |
|---|
| Health Insurance Portability and Accountability Act of 1996 |
| Family Educational Rights and Privacy Act |
| Genetic Information Nondiscrimination Act |
| 42 CFR Part 2 |
| Privacy Act of 1974 |
| Americans with Disabilities Act of 1990 |
| Children's Online Privacy Protection Act |
| Controlling the Assault Non-Solicited Pornography and Marketing Act |
| Electronic Communications Privacy Act |
| Fair Crediting Reporting Act & Fair and Accurate Credit Transactions Act |
| Federal Communications Commission Robocall Rules |
| Federal Trade Commission Act of 1914 |
| Federal Trade Commission Telemarketing Sales Rule |
| Sarbanes Oxley |
| Stored Communications Act |
| Telecommunications Act of 1996 |
| Telephone Consumer Protection Act of 1991 |
| Wiretap Act |

## State Privacy Laws

| |
|---|
| Anti-spam laws |
| Consumer privacy laws (including California Consumer Privacy Act of 2018, California Privacy Rights Act of 2020, Consumer Data Protection Act) |
| Data breach laws (including New York SHIELD Act) |
| Data disposal laws |
| Information security laws |
| Internet of things laws |
| Medical privacy laws (including California Confidentiality of Medical Information Act) |
| Safe harbor laws |
| Wiretap laws |
| Also consider: Information blocking |

## Examples of Compliance Responsibilities | Costs for compliance may vary greatly

| |
|---|
| Administrative |
| Business Associate Agreements |
| Minimum necessary standard |
| Nominate a privacy Officer |
| Patient Authorization |
| Privacy Procedures and Notice of Privacy Practices |
| Technical and Physical Safeguards to protect protected health information |
| Training |

Sources

https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html