CONFIDENTIALITY COALITION

wedi™
Technology Today For A Healthy Tomorrow

March 24, 2022

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

The Honorable Gina Raimondo
Secretary
Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Dear Secretaries Becerra and Raimondo:

On behalf of the Confidentiality Coalition and the Workgroup for Electronic Data Interchange (WEDI), we write today to raise concerns regarding the potential misuse of patient health information by certain third-party applications (apps) and offer recommendations on how better to protect this information. While the Health Insurance Portability and Accountability Act (HIPAA) safeguards a specific subset of "protected health information" (PHI), the law applies only to traditional health care covered entities (CEs) and their business associates. A vast amount of health-related information does not fall within the HIPAA regulatory framework and is largely unprotected from misuse. We urge the Departments of Commerce and Health and Human Services (HHS) to take action to protect patients from inappropriate disclosures of their health information.

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions

WEDI was formed in 1991 by then HHS Secretary Dr. Louis Sullivan to identify opportunities to improve the efficiency of health data exchange. WEDI was named in the HIPAA legislation as an advisor to the Secretary of HHS. Recognized and trusted as a formal advisor to the Secretary, WEDI is the leading authority on the use of health information technology (IT) to efficiently improve health information exchange, enhance care quality, and reduce costs. With a focus on advancing standards for electronic administrative transactions, and promoting data privacy and security, WEDI has been instrumental in aligning the industry to harmonize administrative and clinical data.

Our two organizations fully support moving to a health care system where data flow seamlessly among stakeholders to achieve improved health outcomes for all individuals, while at the same time ensuring that the privacy and security of the information is maintained. We recognize the ability of application programming interfaces (APIs) and health apps to facilitate patient access to health data and as such the API can allow patients to take increased ownership of their health.

Some CEs, including health plans, physician practices and inpatient facilities have already built or have contracted with business associates to develop patient access APIs and apps and are actively promoting their use. Specifically, these apps deployed by providers and health plans are typically covered under HIPAA and therefore the individual's accessing data have assurances that their information is being kept private and secure. We are concerned, however, regarding the lack of robust privacy standards applicable to the large percentage of third-party app developers not associated with CEs and therefore not covered under HIPAA and the fact that there currently is no federally recognized certification or accreditation for these apps. The potential exists for PHI gained via the apps to be inappropriately disclosed to the detriment of patients and their families. While we strongly support patient access to their PHI via apps, we assert that a national framework is required to ensure that health care data obtained by third-party apps is held to high privacy and security standards.

The protections afforded by HIPAA privacy and security have been a fixture in our health care system for more than two decades. These privacy and security rules lay out a framework to ensure that PHI will be kept secure, and patients rely on HIPAA to ensure that the confidentiality of their information is maintained. Organizations that are CEs under the law have a responsibility to take necessary steps to maintain the trust of individuals. However, these same individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA CE or under a business associate agreement (BAA) are not afforded HIPAA privacy and security protections.

We continue to be concerned that patients will not have adequate information to be educated consumers regarding third-party apps and may not fully comprehend that they are assuming the risk of the security practices implemented by their chosen app. Specifically, patients may not understand when their information is and is not protected by HIPAA. We appreciate the Federal Trade Commission's (FTC) emphasis on developing robust consumer privacy protections and we encourage the FTC to explicitly identify steps to protect health data. We strongly support the September 15, 2021, FTC policy statement[1] that health apps and connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule, which requires that they notify patients and others when their health data is breached. As well, we support HHS's guidance[2] clarifying that health care providers are not responsible under the HIPAA Security Rule for verifying the security of a patient's chosen third-party app. However, we note that this "safe harbor" does not address the potential vulnerability of patient information when sent to the app.

[1] FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule, posted September 15, 2021.

[2] HHS Office for Civil Rights Frequently Ask Question posted January 31, 2020

Recent evidence suggests that third-party apps in the health care environment are vulnerable to security issues. The 2019 Gartner Research report[3] suggests that, despite growing awareness of API security, breaches continue to occur. A recently released report by Approov[4] found significant vulnerabilities in the APIs that underpin dozens of the mobile health apps used by patient care organizations for remote account management and telemedicine appointments with patients. Of the three APIs tested, which serve a network of 48 mobile apps and APIs, all of them allowed the tester to access health data from other patients by using one patient's login. More than half (53%) of the mobile apps tested had hardcoded API keys and tokens that would enable hackers to attack the APIs. It is important to note that these vulnerabilities are not a result of problems with the underlying Fast Healthcare Interoperability Resources (FHIR) standards, but rather a failure of the app to adhere to appropriate security protocols. According to research conducted by TechCrunch,[5] a security "bug" in the health app Docket exposed the private information of New Jersey and Utah residents vaccinated against COVID-19, despite the fact that the app received the endorsement from state officials. Most notably, a Pew Charitable Trust survey conducted in September 2020 found that 90% of Americans are concerned about the privacy of their health data when not protected by HIPAA or other federal regulations.[6]

HHS through its recent HIPAA modification proposed rule,[7] appears be seeking a new avenue for requiring CEs to transmit ePHI. HHS, in this proposed rule, requests comments on whether CEs should be required to educate or warn individuals that they are transmitting PHI to an entity that is not covered by the HIPAA privacy and security rules. We note that the existing HIPAA Privacy Rule requires that, in many cases, patients be asked to sign a written authorization before their PHI may be shared with third parties. In requesting comments on whether CEs be required to educate or warn individuals that they are transmitting PHI to an entity that is not covered by these rules, we believe the Department is correctly assuming that there is potential danger in moving ePHI to third-party apps.

Again, while we are supportive of increasing data exchange for patients via third-party apps, there is a clear potential that using these apps could result in patients having their information inappropriately disclosed. We also assert that it is inappropriate to put the burden of warning the individual solely as the responsibility of the CE. CEs will typically not be experts on app data privacy and security protocols and will have little time to warn patients of the potential dangers associated with transmitting ePHI to third parties not covered by the HIPAA protections. Under current regulation, CEs are not permitted to require formal verification checks on individual third-party apps before allowing the application to connect to its API.

We believe that for health care data exchange to occur in an interoperable manner as called for under the 21st Century Cures legislation, there must be a consistent and high level of trust among all participants, including entities that are not legally a CE or bound by a BAA. The deployment of effective federal policies is critical to assist in facilitating this trust framework.

[3] M. O'Neill , D. Zumerle , and J. D'Hoinne API Security: What You Need to Do to Protect Your APIs, Gartner Research, Published August 28, 2019.

[4] Approov: The New Healthcare Ecosystem will depend on FHIR APIs, But Are They Secure? Published October 2021.

[5] Z. Whitaker, A security bug in health app Dockett exposed COVID-19 vaccination records. Published October 27, 2021.

[6] B. Moscovitch, Americans Want Federal Government to Make Sharing Electronic Health Data Easier, The Pew Charitable Trusts (September 16, 2020).

[7] Federal Register Vol. 86, No. 12, Thursday January 21, 2021: Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement.

The Centers for Medicare & Medicaid Services' (CMS) own Blue Button 2.0 program recognizes the importance of third-party apps maintaining strict privacy protocols. For example, the Blue Button 2.0 Production Access Checklist includes an adherence to the Blue Button 2.0 API terms of service and general privacy guidelines. These guidelines include developers specifying: (i) data collection practices; (ii) the risks in their privacy policy; (iii) the company's data disclosure practice, including any use and sharing of de-identified, anonymized or pseudonymized data; (iv) the company's data access practice, including any use and sharing of de-identified, anonymized or pseudonymized data; (v) the company's security practice, including any use and sharing of de-identified, anonymized or pseudonymized data; and (vi) the company's retention/deletion practice, including any use and sharing of de-identified, anonymized or pseudonymized data. Collecting this information from developers will be a critical component of the agency's effort to protect the data of Medicare beneficiaries.

Further, the CMS Data at the Point of Care (DPC) API initiative is currently in a pilot phase in which a limited number of users can access Medicare Fee-For-Service claims data through the API once their solution has been approved for production. This pilot program promotes the industry standard FHIR, specifically the Bulk FHIR specification.

We note that health IT implementers preparing to onboard the DPC production environment are required to provide one of the following CMS-accepted security certifications: (i) Office of the National Coordinator for Health Information Technology (ONC) Health IT Certification; (ii) HITRUST CSF Validated Assessment; (iii) HITRUST self-validation assessment (valid for one year from date of first implementation if currently pursuing the HITRUST validated assessment); Electronic Healthcare Network Accreditation Commission (EHNAC) Accreditation; System and Organization Controls (SOC) 2 type 1 certification (valid for one year from date of first implementation if currently pursuing type 2), or type 2 certified; and (v) International Organization for Standardization (ISO): 27001, 27017, or 27018 certified.

We offer the following recommendations that we believe will encourage organizations to take full advantage of electronic exchange and help patients reap the benefits of streamlined sharing of clinical data:

- Release additional guidance on the types of third-party app security and privacy verification that will be permitted and allow CEs themselves to undertake an appropriate level of review of a third-party app before permitting it to connect to their APIs.

- Require entities that are not HIPAA CEs or business associates to clearly stipulate to the individual the purposes for which they collect, use, and disclose identifiable health information and require that these individuals be given clear, succinct notice concerning the collection, use, disclosure, and protection of individually identifiable health information that is not subject to HIPAA.

- Work with the private sector in the development of a privacy and security accreditation or certification framework for third-party apps seeking to connect to APIs of certified health IT. Once established, CEs should be permitted to limit the use of their APIs to third-party apps that have agreed to abide by the framework. Such a program would not only foster innovation, but also establish improved assurance to patients of the security of their information.

- Apply similar security requirements in the private sector as CMS applies to its Blue Button 2.0 and DPC initiatives, requiring all third-party apps seeking to access PHI via provider or health plan APIs to prove adherence to a strict set of privacy and security guidelines or successfully complete a CMS-approved security certification.

- Partner with groups like the Confidentiality Coalition, WEDI and other professional associations in the development and deployment of education aimed at a wide range of consumers and CEs. Enhanced consumer and CE education will lead to significant improvement in the ability of the consumer and the CE to understand their rights and responsibilities under the law.

We appreciate the opportunity to share our perspective regarding privacy and security concerns associated with third-party apps and the need to create a framework to ensure patient record confidentiality is maintained. As we have asserted, an important barrier to the attainment of interoperable health care data exchange across all parties involved is the lack of trust. We believe our recommendations will serve to increase the assurance that health information is being securely exchanged and provide patients the confidence to become more engaged in their health decisions. Please contact Tina Grande at tgrande@HLC.org or Charles Stellar at cstellar@WEDI.org to discuss these recommendations or explore opportunities to educate impacted stakeholders.

Sincerely,

Tina Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council

Charles Stellar
President and CEO, WEDI

cc: House Committee on Energy and Commerce

Senate Committee on Commerce, Science and Transportation

Senate Committee on Health, Education, Labor and Pensions