United States Senate

COMMITTEE ON FINANCE

WASHINGTON, DC 20510–6200

December 12, 2025

Seema Verma
Executive Vice President and General Manager
Oracle Health and Life Sciences
2300 Oracle Way
Austin, TX 78741

Dear Ms. Verma:

I write to seek information about if and how you are protecting national security and Americans' privacy by enabling patients to safeguard their sensitive health information stored in the Electronic Health Record (EHR) systems you sell to their health care providers. I am committed to ensuring that Americans have a full range of tools at their disposal to protect their privacy.

Over the past two decades, the health care industry's widespread adoption of interoperability and EHRs has significantly changed the health information exchange landscape. As you know, interoperability refers to the ability of different health information systems to communicate and exchange information seamlessly to support the provision of timely, coordinated, and high quality health care across providers. A variety of stakeholders take part in this health information sharing, including doctors, laboratories, and claims processors.

Recognizing the importance of interoperability, Congress has taken key steps to mandate electronic health information sharing. In 2009, Congress passed the *Health Information Technology for Economic and Clinical Health Act* (*HITECH Act*) to promote uptake of EHRs across health care organizations. Building on that, Congress passed the *21st Century Cures Act* in 2016. The law required health information be accessible and exchangeable across systems. It also gave patients the right to access their own health records electronically.

While interoperability improves care by enabling better data sharing, it must be balanced with strong privacy protections for sensitive health information. Currently, the sensitive health data of the vast majority of Americans can be accessed by health providers in states around the country, regardless of whether those providers are actually treating the patient, or whether the patient has ever stepped foot in their state. Such widespread access exposes patients to the threat of improper access, theft, and leaking of their sensitive health information. In addition to posing a threat to

the privacy of regular Americans, such data sharing also threatens national security, by making it much easier for foreign spies to obtain sensitive health data on U.S. military and intelligence personnel. This threat is not theoretical — an investigation by the Department of Defense (DOD) Inspector General in 2021 found that the health records of DOD personnel could be improperly accessed for "purposes of extortion, public embarrassment, or sale to others." These issues underscore the need for interoperability frameworks that protect patient rights, ensure data is not misused, and allow essential care to continue without delay or fear of legal consequences.
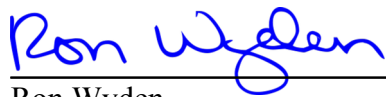
At my urging, Epic, the largest EHR company, recently developed a new feature that empowers individuals to take control of their medical record by controlling the flow of their health information across health care providers. Under this new feature, users will be notified about which health care organizations have access to their record, be prompted to confirm their sharing preferences when they receive sensitive care, and be able to opt out of record sharing, if they determine that is the best course of action for their individual care. According to data that Epic recently provided to my office, this feature has already been deployed. Epic also surveyed fifty customers, representing more than 300 hospitals, regarding their use of various existing privacy features. The survey results show that the provider community has robust adoption of tools that protect patient privacy, and suggests that additional development, including patient-facing tools, would likely be widely adopted.

I believe Americans should be able to have direct control over which entities access their health care information. The changes Epic has made to its system are encouraging in building toward this goal. Given the critical role your company plays in building interoperable systems that rely, in large part, on EHRs, please respond to the following questions by January 20, 2026.

1. Does your patient-facing portal and interoperability framework have the following functionality?
    a. Allow individuals to opt out of record sharing.
    b. Allow individuals to hide their records' existence from other health care organizations using your EHR.
    c. Provide individuals with a list of health care organizations using your EHR that have accessed their health records.
    d. Prompt individuals to confirm their record sharing preferences when they receive sensitive categories of care.
2. If your company does not offer any of the functionality listed in Question 1, will you commit to building and deploying this functionality? Please provide a timeline for when you expect your company to offer these functions for patients.
3. Please describe any patient-facing functionality that you currently offer beyond those listed in Question 1 that allow individuals to control health record sharing.
4. Please describe any patient-facing functionality that you are currently developing, and the timeline for the development of those features, that allow individuals to control health record sharing.

If you have any questions or need additional information, please contact Senate Finance Committee staff. Thank you for your attention to this request.

Sincerely,

Ron Wyden
United States Senator
Ranking Member, Committee
on Finance