Data Privacy and Portability at VA: Protecting Veterans' Personal Data

Feb 12, 2020

Statement of
Ramsey Sulayman, Associate Director
National Legislative Service
Veterans of Foreign Wars of the United States

Before the

United States House of Representatives
Committee on Veterans' Affairs
Subcommittee on Technology Modernization

With Respect To

"Data Privacy and Portability at VA: Protecting Veterans' Personal Data"

WASHINGTON, D.C.

Chairwoman Lee, Ranking Member Banks, and members of the subcommittee, on behalf of the men and women of the Veterans of Foreign Wars of the United States (VFW) and its Auxiliary, thank you for the opportunity to address the issues of data privacy and portability and our members' expectations of the Department of Veterans Affairs' (VA) responsibilities to protection their privacy.

As the Department of Defense (DOD) and VA move toward a joint electronic health care record (EHR), veterans' information will become more accessible for VA and DOD providers

NATIONAL HEADQUARTERS
406 W. 34th Street Office 816.756.3390
Kansas City, MO 64111 Fax 816.968.1157

WASHINGTON OFFICE
200 Maryland Ave., N.E. Office 202.543.2239 info@vfw.org
Washington, D.C. 20002 Fax 202.543.6719 www.vfw.org

Online Version: https://www.vfw.org/advocacy/national-legislative-service/congressional-testimony/2020/2/data-privacy-and-portability-at-va-protecting-veterans-personal-data

and their community partners. This is a good thing. The concentration of personal data in a joint electronic health care record also makes the record more desirable for nefarious actors from foreign governments, non-state actors, and criminals acting as part of organized crime groups or individually. In 2018, the White House Council of Economic Advisers estimated that cybercrime cost the United States' economy between $57–109 billion. A person's health record contains a vast amount of personally identifiable information that can be used for ill.

While the loss or compromise of veterans' health care data certainly comes with an economic cost, it also carries the non-quantifiable costs in the loss of dignity, trust, and confidence. In creating an EHR that can communicate and easily exchange data with other government agencies, as well as commercial health care systems, insurers, and private providers, VA must ensure that veterans' information remains secure when it leaves the VA ecosystem. VA must also ensure that control of data remains with VA and the veteran, and define the expectations for data retention and control with community partners. VA is responsible for ensuring that sufficient protocols are in place to guard against an unthinkable trusted insider intrusion or even simple unauthorized access.

The VFW is not opposed to commercial off-the-shelf solutions; there is no need for VA to reinvent the wheel when it comes to technological solutions. Creating information technology (IT) solutions is not the VA's core strength. Therefore, the strongest possible privacy protections from third-party vendors must be in place. Very specific policies and procedures must be in place that address data collection, data use, transfer of information, and information retention, in particular through End User License Agreements (EULA). EULA are the terms of service that must be accepted, often unilaterally, for a veteran to use an app or website. EULAs generally incorporate a privacy policy that specifies the four criteria above. As mentioned, EULAs are often "take it or leave it" terms. The difference between the effects of a EULA on a commercial site and a EULA on a VA site is that veterans who opt to "leave it," risk losing access to benefits and services earned through service. VA has a monopoly on administration of veterans' health care and benefits. Whereas monopolies in the commercial market are largely outlawed, so consumers are able to seek service from a competitor if they "leave it" in the private sector.

Beginning with EULAs, VA must ensure that partners collect the minimum amount of information, have the shortest retention time possible, and provide clear opt-in criteria. Opt-in was not a slip of the tongue. Veterans and service members should have to opt-in to data *collection* rather than opt-out; the strictest criteria and the most minimal collection should be the standard. We will address health care data sharing, which the VFW supports

as an opt-out, later in this testimony. Data collection must be limited to only necessary and pertinent data. Tracking a veteran's data from usage of specific sites is not necessary to the conduct of that veteran or service member's business with VA or DOD.

As an example, VA is in the process of consolidating all its veteran facing websites into its updated VA.gov portal. To access their VA.gov portal, veterans are prompted to sign up with ID.me, without a reliable alternative. The use of the ID.me login credentials places veterans in the unique position of having to accept the terms of service and privacy policy in the EULA in order to log on and access VA benefits earned through service. The ID.me process is much easier and reliable, for example, than acquiring a DSLogon account or other VA log on if the veteran is not enrolled in the VA health care system or with the Veterans Benefits Administration, or is no longer active in the Defense Enrollment Eligibility Reporting System (DEERS) or the Defense Financial and Accounting Service (DFAS). While the ID.me EULA and privacy policy specifically states that no veteran information will be sold by ID.me, it also specifically states that data may be transferred to partner websites that have a different privacy policy over which ID.me has no control. In other words, to use ID.me services, a veteran's information may be transferred to a trusted ID.me partner. However, the EULA does not guarantee ID.me's partners will not sell or utilize that data for a commercial purpose, including aggregating it with other sources that may personally identify the veteran.

The security of veterans' health information is of paramount importance. As health care technology advances and more details become available through diagnostic and genetic testing, that information will become more concentrated in locations like the EHR. The VFW urges VA to place the highest priority on security and utilizing the strongest possible technological solutions to safeguard veterans' health data.

Project Nightingale, a joint commercial venture between Google and Ascension Health, the nation's second-largest health care system, underscores some of these issues surrounding data collection and utilization. Google partnered with Ascension to digitize the health records of Ascension's patients and then apply tools such as artificial intelligence (AI) to look for patterns. While some of these patterns related to early prediction of disease or better treatments for existing conditions, one of the goals of the program was also to see where more revenue could be squeezed out of care. While the attempt to use health care data to generate new revenue streams is of concern, the larger philosophical concern is that patients' private health care data may migrate to Google *without the prior consent of patients*. Ascension could provide these records because, under the *Health Insurance*

Portability and Accountability Act of 1996 (HIPPA), Google is a business associate of Ascension helping Ascension execute administrative functions necessary to the provision of health care. I use Ascension as an example because Ascension very actively marketed its services to veterans participating in the VA Veterans Choice Program. Ascension is a fine health care system noted for its quality of care, but what is important for VA and veterans is that a veteran who uses Ascension (or any other health care system that has external partners with big data programs) does not automatically have his or her health care information vacuumed into a program to which he or she did not consent by virtue of existing business partners or covered entity relationships between health care providers, systems, or insurers and data focused enterprises.

Provider records, however, is not the only kind of health care information that people generate. User-generated data, such as that from wearable devices like FitBit, are *not* covered by HIPAA. I pick on FitBit versus Apple Health or Huawei Health because FitBit is owned by Google. One can see that the acquisition of health care data from HIPAA-protected sources and unprotected user generated data is a major effort for Google. Google is not alone, though. Apple, Amazon, Facebook, and Microsoft are but a few of the major established information technology players also working on cornering the big data market in health care. The combination of data from FitBit users whose data is also contained in Project Nightingale leads to questions about what that data and its commercialization will lead to.

Smaller players like Xealth are also in the market and working on similar products and initiatives. Xealth, which has attracted investors that include the Cleveland clinic, University of Pittsburgh Medical Center, Atrium Health, and Amazon, has developed a product where health care providers can check off products and services from a digital shopping list, and offer or prescribe them to patients as part of the visit or consultation. Patients can then use the recommendations from Xealth to order products, services, and prescriptions directly from vendors, including Amazon. Even excluding the sharing or leakage of health data, purchasing patterns of consumer goods can lead to predictions about health conditions. For example, the purchase of compression socks, syringes, and testing strips can be analyzed to determine that a consumer suffers from diabetes –– all from non-HIPAA protected information.

Genetic information adds to the mix and can present daunting questions of privacy. While major commercial providers of DNA testing for purposes of determining ancestry and genealogy are pretty good about requiring opt-in for certain information sharing, and

informed consent for research purposes, they also note that they are not required to comply with HIPAA and that they may store and share information, including genetic information, with their service or business partners. As with EULAs, these partners may have different privacy policies, and one has to review *all* the privacy policies of *all* partners. Other sites, for instance GEDmatch, make all genetic information submitted publicly available. It is estimated that 60 percent of Americans who are of Northern European descent can be identified through data in public databases, with that figure expected to rise to 90 percent in the next few years.

How does this affect veterans? VA's Million Veteran Program (MVP) immediately comes to mind. VA is merging the health care and genetic data of veterans who opt-in in a landmark study that has revolutionary implications for the provision of health care. However, little is discussed about data security, and what is available is not in plain language. However, VA does note that "There could be a slight risk of a breach of confidentiality, and if information about you does leak out, the VA will not be able to guarantee that it will be protected." VA must do what it takes to ensure a breach does not occur. The VFW also urges VA to be more transparent about the policies and procedures in place to assure data safety, and provide prominent links to the full policies, as well as plain language translations.

While all this when placed in a certain context may be Orwellian, we must not see a conspiracy around every corner. Health care data sharing can yield immense benefits. As much as we believe that medicine is science, it is also art and relies heavily on providers' experience and judgment. At a certain point, the symptoms of a common cold can look an awful lot like those of a life-threatening disease, or a major medical event such as an aneurysm, heart attack, or stroke. Growing up in a medical family, I have heard enough anecdotes about medical miracles and missed diagnoses that I could churn out scripts for tearjerkers on the Hallmark Channel indefinitely into the future. Often, these missed moments or life-saving revelations were the result of experience and noticing details that may have been overlooked, or were not in a provider's experience base. Technology can help solve this.

A doctor can have a patient's entire medical history at hand without relying on the limitations of a patient's memory or self-reporting. The availability of the complete medical record can allow the doctor to make a more informed diagnosis. That diagnosis can be checked by an impartial AI system that might see patterns missed in the rush of an emergency room visit on a busy day. User-generated information from health trackers can objectively report a patient's activity levels, sleep, and other vitals without having to rely on

memory and self-reporting from patients who may be in crisis or less than one hundred percent. Amalgamated, de-identified patient data can be searched, and research populations identified, with big data tools in a fraction of the time as in the past by hand. There are benefits, but the benefits must balance the risks, and we must look at what may be possible in the future versus what we merely see as possible today.

The laws governing privacy rights, particularly with electronic data, are more of a patchwork than a comprehensive whole. HIPAA was passed in 1996, in an era before big data when records were kept locally and on paper before today's computing power was available. For reference, Amazon was merely an online book seller and my Apple Macintosh LC 3 had a whopping 80 megabytes of memory. The VFW applauds this subcommittee for looking at this issue intently and, ever so importantly, with an eye to the effects from the perspective of veterans. As institutions that safeguard the rights for which our veterans fought, and as organizations that represent our veterans' best interests, we must ensure that privacy and security, or information, particularly health data, is paramount and that veterans remain in control.

This concludes my statement. Thank you for your time and I look forward to answering any questions you may have.