EHRVA

HiMSS Electronic Health Record Vendors Association

Privacy and Security Whitepaper

A Work Product of the
Electronic Health Record Vendors Association (EHRVA)
and the Healthcare Information and
Management Systems Society (HIMSS)

The members of the Electronic Health Record Vendors Association (EHRVA) are committed to achieving the benefits that are inherent in the use of healthcare information technology (IT) and electronic health record (EHR) systems across the healthcare system, including cost savings, process efficiencies and improved quality of care. At the same time, it is clear that there are concerns over the privacy and security of protected health information (PHI), which is defined as any individually identifiable health information about a patient.

The fact is that in many ways, the further adoption of EHRs and healthcare IT, in coordination with current laws, increases the privacy and security of PHI over the current paper-based system. And, where additional controls and provisions are needed, there are private and public sector initiatives already in place to address identified gaps. It is with that in mind that we ask for your support of our requests detailed below.

In order to ensure the continued momentum on achieving the benefits of healthcare IT, the EHRVA calls on members of the U.S. Congress and State Legislatures to move forward with legislative action that:

- Supports and incentivizes the use of IT in healthcare delivery and related business work flows.
- Provides essential funding for federal (and state) healthcare IT-related initiatives including the Office of the National Coordinator for Health Information Technology (ONC) and the Health Information Technology Standards Panel (HITSP).[1]
- Supports the development and promulgation of standards to facilitate the secure exchange of health information, in particular those standards established by HITSP.
- Ensures the protection, confidentiality and integrity of PHI while balancing the needs of healthcare delivery, healthcare research and public health stakeholders to access health data in order to ensure safe, timely, appropriate and high quality healthcare. In doing so, we recommend that you utilize the recommendations already put forth by the National Committee on Vital and Health Statistics (NCVHS)[2] and to specify HITSP as responsible for defining the technology standards to implement these new policy recommendations.
- Increases the enforcement and the public understanding of the enforcement of current HIPAA privacy and security laws and regulations by entities that control PHI.

Background

The adoption and widespread use of health information technology and electronic health records as tools to increase care quality and decrease costs of healthcare in the United States continues to gain momentum. Executive Order # 13335 established that most Americans should have an EHR by 2014. As the momentum builds and the benefits of healthcare IT adoption become more apparent, so have concerns for the *potential* impact to patient privacy and security.

[1] In 2005, the U.S. Department of Health and Human Services (HHS) awarded a contract targeting the creation of processes to harmonize standards to advance the vision for widespread adoption of interoperable electronic health records (EHRs) within 10 years. HITSP is administered by the American National Standards Institute (ANSI) in cooperation with strategic partners including the Healthcare Information and Management Systems Society (HIMSS), the Advanced Technology Institute (ATI), and Booz Allen Hamilton.

[2] The National Committee on Vital and Health Statistics was established by Congress to serve as an advisory body to HHS on health data, statistics and national health information policy. It fulfills review and advisory functions relative to health data and statistical problems of national and international interest, stimulates or conducts studies of such problems and makes proposals for improvement of the nation's health statistics and information systems. In 1996, the Committee was restructured to meet expanded responsibilities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Privacy, in this context, is an individual's right to control the acquisition, uses or disclosures of his or her identifiable data. Security controls, in this context, are the administrative, physical and technical actions taken to protect individually identifiable health information, including relevant privacy policies, regardless of the medium or format.

Concerns over the privacy and security of electronic health information primarily fall into two general categories:

- Inappropriate release of information from provider organizations resulting from authorized users who disseminate information in violation of organizational policy *or* from non-authorized users who gain access to an organization's information system with malicious intent.
- The flow of information through the healthcare system that are direct patient care-related activities. This information flow normally occurs between providers, payors and secondary users, with consent or with "implied consent" to conduct treatment, payment and healthcare operations.

Privacy advocates want laws, regulations, and policies that mandate additional privacy and security protections, beyond those already provided by federal law. The HIPAA privacy rule provides protections of PHI that lie outside of treatment, payment and healthcare operations (TPO). The current policy discussions are focused on putting additional laws and regulations around these TPO processes. As currently defined, these recommendations could require overburdening administrative and technical requirements that are unfunded and unnecessary. NCVHS has already made recommendations to the Secretary of HHS on many of the recognized privacy and security gaps with existing HIPAA regulations that did not anticipate the capabilities such as personal health records, health information exchanges or advanced medical homes.[2,4,5] And, HITSP is already in the process of defining technology standards to implement these new policy recommendations.

Please support the tremendous progress that healthcare IT stakeholders have made over the past four years to address the privacy and security concerns. The details of privacy and security are complicated and must be well-balanced, but they are also well-understood by key recognized stakeholders and are being addressed at the federal and state level. Privacy advocates are stakeholders in these discussions and are contributing and vetting the work products in these areas.

The EHRVA supports addressing the privacy and security concerns of consumers and their advocates, thus enabling further adoption of healthcare IT. We ask for your support and leadership in moving forward on the requests made in this paper with the goal of further adoption of healthcare IT resulting in of improved efficiency and quality of care across our healthcare system.

[3] NCVHS. Letter to Secretary Michael Leavitt, HHS. "Update to privacy laws and regulations required to accommodate NHIN data sharing practices." June 21, 2007.

[4] NCVHS. Letter to Secretary Michael Leavitt, HHS. "Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data," December 21, 2007.

[5] NCVHS. Letter to Secretary Michael Leavitt, HHS. "Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment," February 20, 2008.