The Office of the National Coordinator for Health Information Technology

Building Trust in Health Information Exchange

Statement on Privacy and Security

David Blumenthal, M.D., M.P.P., National Coordinator for Health Information Technology, U.S. Department of Health and Human Services (HHS); and
Georgina Verdugo, Director, Office for Civil Rights, HHS

As the Department of Health and Human Services (HHS or The Department) continues its efforts to improve the health and care of all Americans by promoting the advancement of health information technology (IT), one of the Department's guiding principles is that the benefits of health IT can only be fully realized if patients and providers are confident that electronic health information is kept private and secure. HHS's goal, as directed by the 2009 Health Information Technology for Clinical and Economic Health (HITECH) Act, is to improve the nation's health care system by enabling health information to follow the patient wherever and whenever it is needed. The HHS Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) are working jointly on a number of projects to ensure that this electronic exchange of health information is built on a foundation of privacy, and security.

On July 8, 2010, HHS announced proposed regulations under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that would expand individuals' rights to access their information and restrict certain disclosures of protected health information to health plans, extend the applicability of certain of the Privacy and Security Rules' requirements to the business associates of covered entities, establish new limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without patient authorization. In addition, the proposed rule is designed to strengthen and expand OCR's ability to enforce HIPAA's Privacy and Security provisions. This rulemaking will strengthen the privacy and security of health information, and is an integral piece of the Administration's efforts to broaden the use of health information technology in health care today. We urge consumers, providers, and other stakeholders to read these proposals and offer comments during the 60-day comment period, which will officially open on July 14, 2010. Information about posting comments will be available at http://www.regulations.gov.

Additionally, over the past few months, ONC and OCR have embarked on a number of other initiatives that serve to integrate privacy and security into the nation's health IT efforts. As directed by HITECH, ONC established a new Chief Privacy Officer (CPO) position to provide critical advice to the National Coordinator in developing and implementing ONC's privacy and security programs. The new CPO, Joy Pritts, JD, will play a key role in helping ONC design new policies to address privacy and security issues in every phase of health IT development and implementation.

On August 24, 2009, OCR issued an interim final breach notification regulation, which improves transparency and acts as an incentive to the health care industry to improve privacy and security by requiring HIPAA covered entities to promptly notify affected individuals, the HHS Secretary and, in some cases the media, of a breach. This new federal law holds covered entities and business associates accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care.

ONC is coordinating with the Centers for Medicare & Medicaid Services (CMS) on CMS's development of a final regulation on the Medicare and Medicaid Electronic Health Record Incentives Programs. The incentives programs promote critical privacy and security measures and business practices. ONC also is developing a final regulation on standards and certification criteria to ensure that electronic health records (EHRs) contain the capabilities to support needed privacy and security requirements.

With respect to security, the Department also embarked on a number of initiatives. OCR coordinated with the National Institute of Standards and Technology to host a conference focused on the HIPAA Security Rule. OCR also issued draft guidance in conducting a HIPAA Security Risk Analysis to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Additionally, an advisory committee on HIT standards held hearings to better understand security priorities, the effectiveness of security procedures, and vulnerabilities.

All these activities only serve as a prelude to our ongoing efforts to ensure that electronic health information is private and secure. In addition:

- ONC and OCR are working together with representatives of consumer and industry groups to promote the adoption of privacy and security safeguards as essential components of implementing health information technology.
- ONC is ensuring that the technical and policy foundations of the nationwide health information network will demonstrate methods for achieving trust among entities exchanging information while integrating best practices for privacy and security. A privacy and security workgroup (known as a "Tiger Team") of the Health Information Technology Policy Committee (HITPC) was convened with strong consumer representation to hold public deliberations and make recommendations related to patient choice in how health information is exchanged; consumer access to health information; personal health records (PHRs); segmentation of health information; and transparency about information sharing and protections.
- ONC staff is working with the President's cybersecurity initiative and other Federal partners to solicit input from the best security minds in the federal government. Based on these activities, ONC will provide direction on security best practices and standards to technical and policy decision makers for inclusion in health information exchange programs.
- Finally, the Department is working to provide the private sector with greater resources for improving privacy and security. Regional Extension Centers will educate providers about necessary privacy and security measures. Curriculum Development Centers Programs will incorporate necessary information into standard curricula for Community College Consortia, where a new cadre of HIT professionals will be trained, and for University-Based Training Programs, where health professionals will learn about HIT. State Health Information Exchange Cooperative Agreements and Beacon Communities grants will provide living examples of how privacy and security are successfully implemented and brought to scale.

Our Nation is poised to harness the power of information technology to improve health care. Transforming our health care system into a 21st century model is a bold agenda. As we enter into a new age of electronic health information exchange, it is more important than ever to ensure consumer trust in the privacy and security of their health information and in the industry's use of new technology.