patientprivacyrights

December 19, 2012

Leon Rodriguez
Director
Office for Civil Rights
US Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Director Rodriguez:

As an organization committed to restoring patients' rights to control sensitive personal health information in electronic systems and online, Patient Privacy Rights (PPR) respectfully requests that the Department of Health and Human Services' (HHS) Office for Civil Rights issue strong guidance on cloud computing. Health providers will benefit from such guidance as they consider moving to cloud services and patients will benefit by knowing which data privacy and security protections should be in place – both will undoubtedly help increase trust and drive adoption.

Cloud computing can improve access to patient information for providers, plans, and others involved in patients' care has and can decrease costs for our health system. Yet, the transition to electronic health records will be slowed if patients do not have assurances that their personal medical information will always have comprehensive and meaningful security and privacy protections. The HHS settlement with Phoenix Cardiac Surgery in April 2012 illustrates the challenges that can arise when providers move to the cloud. PPR encourages HHS to issue guidance that highlights the lessons learned from the Phoenix Cardiac Surgery case while making clear that HIPAA does not prevent providers from moving to the cloud as long as it is done responsibly and in compliance with the law.

To be clear, keeping information confidential and secure needs to be a top priority, and more specific guidance in the health care ecosystem would help ensure that cloud providers, health care professionals and patients alike are aware of how the privacy and security rules apply to clouds. Facilitating plan and provider compliance with federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act is essential. Other stronger federal laws such as 42 CFR Part 2, stronger state laws, and Constitutional rights to health information privacy should also apply to clouds. Both Congress and the Administration support updating and maintaining privacy and security protections as new technologies develop and advance, however, HHS and HIPAA guidance in this area, to date, is limited. It is our understanding that other federal agencies, such as the Office of Management and Budget, National Institute of Standards and Technology, Federal Financial Institutions Examination Council, FedRAMP and the Department of Education already have issued guidance related to the provision of cloud services. We recommend developing guidance for health information with standards at least as rigorous as those developed by NIST.

Therefore, we believe that by issuing guidance HHS/OCR can advance the goal to protect patient information. It is essential that this guidance include the following criteria:

- Secure Infrastructure: Appropriate administrative, physical, and technical safeguards must be in place. These safeguards should include: comprehensive risk assessment by external auditors, audit controls that cannot be turned off, data encryption, robust access controls, and, where appropriate, intrusion detection and automated server management systems.

- Security Standards: Security standards must be implemented that are consistent and compatible with standards required of federal agencies including the HIPAA Security Rule and the HITECH breach notification requirements.

- Privacy of Protected Health Information: Standards must be included that establish the appropriate use, disclosure, and safeguarding of individually identifiable information, which take into account stronger state and federal requirements, Constitutional rights to health information privacy, and the fact that HIPAA is the "floor" for privacy protections and was never intended to replace stronger ethical, or professional standards or "best practices."

- BAA Requirement and Standardization: Consistent with prior OCR guidance, any software company given access to protected health information by a HIPAA-covered entity to perform a service for the covered entity is a business associate. Thus, as OCR representatives have publicly stated on several occasions, a Business Associate Agreement (BAA) is required between a cloud computing provider and any customer entity that uses or discloses protected health information or de-identified health information. It is imperative that these BAA standards promote the protection of privacy and security of health information to ensure public trust in health IT systems and promote quality health care, health care innovation and health provider collaboration.

Issuing guidance to strengthen and clarify cloud-based protections for data security and privacy will help assure patients how sensitive health data they share with their physicians and other health care professionals will be protected. Thank you for your attention to this matter and we look forward to working with you on this significant issue.

Sincerely,

Deborah C. Peel, MD
Founder and Chair, Patient Privacy Rights

cc: The Honorable Kathleen Sebelius, Secretary of Health and Human Services