HEALTH CARE PRIVACY ALERT

10/27/16

New HIPAA Guidance Sheds Light on Existing Rules

By Christina M. Kuta, Associate

Recently, regulators issued new guidance related to the Health Insurance Portability and Accountability Act ("HIPAA"), Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996. Specifically, on October 6, 2016, the Department of Health and Human Services ("HHS") issued "Guidance on HIPAA & Cloud Computing." While this publication created no new obligations for those subject to HIPAA, it clarified existing obligations and expectations to remain HIPAA-compliant.

Use of the "cloud" has become a common method of storing and transmitting electronic information. In the health care industry, the cloud is often used to store data designated as electronic protected health information ("ePHI") under HIPAA through third-party cloud providers. Until the published HHS guidance, there was no general consensus on the HIPAA obligations (if any) of the cloud provider that simply provided no services other than acting as a repository for ePHI.

Notable information from the new guidance includes the following:

1. A cloud provider is deemed to be a business associate under HIPAA even if it only stores ePHI. Accordingly, health care providers must enter into HIPAA-compliant Business Associate Agreements with cloud providers prior to transferring any ePHI. Additionally, if a cloud provider subcontracts with another cloud provider (a subcontractor) related to the use or transmission of ePHI on behalf of the business associate, the subcontractor is deemed a business associate as well. This is true even if the ePHI stored is encrypted and the cloud provider does not hold the "key" to unlock the encryption. Clear designation as a business associate requires the cloud provider to comply with many aspects of HIPAA, including its Privacy Rules, Security Rules, and Breach Notification Rules.

2. ePHI in the cloud can be accessed through the use of mobile devices, as long as the appropriate physical, technical, and administrative safeguards are in place to protect the confidentiality and integrity of the ePHI.

3. ePHI can be stored by a cloud provider who maintains servers outside the United States, but providers should understand the potential for increased security risks in this scenario.

4. A cloud provider will not be deemed a business associate if it only stores "de-identified" information (as that term is used under HIPAA).

5. Not having a business associate agreement in place with a cloud provider can be costly. HHS specifically noted a case that settled in July 2016 for $2,700,000. In that matter, a large health care provider was storing ePHI on a cloud-based system and did not maintain a Business Associate Agreement with the cloud provider. After reporting a breach incident, the Office of Civil Rights (the federal agency charged with HIPAA enforcement) conducted an investigation, finding evidence of widespread vulnerabilities with the health care provider's HIPAA compliance program, "including the storage of the electronic protected health information (ePHI) of over 3,000 individuals on a cloud-based server without a Business Associate Agreement."

This guidance comes at a time of increased audits and review by regulators of providers' HIPAA policies and procedures. While many providers believe that HIPAA impacts only their ability to disclose a patient's medical records, amendments and additional laws enacted over the past few years have expanded HIPAA's reach and increased the responsibilities for covered entities and business associates. If you have not (1) reviewed and

revised your HIPAA policies and procedures in the last two years; and/or (2) conducted a HIPAA risk assessment and risk mitigation plan in the last year, you likely are not in compliance with current HIPAA requirements. We urge you to contact the listed Roetzel attorneys to discuss your practice's obligations and HIPAA compliance objectives.

Author
Christina M. Kuta
ckuta@ralaw.com

Additional Contacts
Ericka L. Adler
eadler@ralaw.com

Mazen Asbahi
masbahi@ralaw.com

David J. Hochman
dhochman@ralaw.com

Avery Delott
adelott@ralaw.com

Media Contact
Ashley McCool
amccool@ralaw.com