

**HIPAA SECURITY GUIDANCE FOR REMOTE USE AND ACCESS TO
ELECTRONIC PROTECTED HEALTH INFORMATION**

The Centers for Medicare & Medicaid Services (CMS) issued guidance recently regarding the remote use and access of patients' electronic protected health information (ePHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA) security rule. The HIPAA security regulation, which applies to entities including health plans and many health care providers, requires covered entities to ensure the confidentiality, integrity, and availability of ePHI. The guidance includes strategies that may be reasonable and appropriate for covered entities to adopt when using portable media or devices that store ePHI, or allowing off-site access or transportation of ePHI through laptops, personal digital assistants, or home computers.

The CMS guidance sets out possible problems that are endemic to the use of portable data-storage devices such as flash drives and to offsite access of data via laptop computers. It also outlines strategies available for dealing with such problems. CMS seems to generally discourage remote access or storage, but specifically acknowledges that certain business cases exist where allowing data access, storage or transportation is necessary. The guidance encourages HIPAA covered entities to limit any such remote access or transportation to those instances where it is clearly necessary for the proper operation of the medical entity or for good patient care, and then only where great rigor has been taken to ensure that policies, procedures and workforce training have been effectively deployed and access is provided consistent with applicable requirements of the HIPAA Privacy Rule.

The guidance notes that covered entities should conduct rigorous risk analysis and risk management to develop policies and procedures for safeguarding health information and should emphasize training and awareness of the security policies as well as strong sanctions against violators. The guidance then outlines possible data security problems and potential solutions, divided into categories of access, storage, and transmission. Some potential solutions, such as encryption, apply to multiple issues. Virus protection is relevant to all three categories, since contamination with a computer virus is a problem that could relate to access, storage, and transmission. CMS specifically noted that, with respect to remote access to or use of ePHI, health care organizations should place significant emphasis and attention on their: (1) risk analysis and risk management strategies; (2) policies and procedures for safeguarding ePHI; and (3) security awareness and training on the policies and procedures for safeguarding ePHI.

Health care organizations "should be extremely cautious" about allowing remote access to ePHI, according to CMS. Remote access is appropriate only when business cases require its use, CMS notes in the guidance.. Examples of rationale business purposes for remote access include the following: (1) a home health nurse collects and accesses patient data using a personal digital assistant (PDA) or laptop during a home health visit; (2) a physician accesses an e-prescribing application on a PDA while out of the office to respond to patient requests for refills; (3) a health plan employee transports backup enrollee data on a media storage device to an offsite storage facility.

The CMS guidance was provided in response to frequent news stories about actual and potential public exposure of patient information due to inadequately secured laptops and other portable devices as well as the increasing use of remote or off-site access to ePHI within a health care organization. Remote access to ePHI presents a variety of risks. A few recent data theft cases are illustrative: ChoicePoint; the Department of Veteran's Affairs; Providence Health System; Kaiser Permanente; Allina Hospitals and Clinics; and Georgetown University Medical Center. Most of these cases were the result of lost or stolen laptop computers or data storage devices. CMS recommends that health care organizations take the following

steps, in accordance with their risk assessments: (1) employ encryption of the appropriate strength on all portable or remote devices that store ePHI; (2) back up all ePHI entered into remote systems; and (3) install virus-protection software on portable devices.

As CMS makes clear, the identified “risks” and proposed “possible risk management strategies” are not exhaustive or comprehensive, and that health care organizations must assess risks to ePHI and develop and implement strategies to mitigate those risks. The guidance merely sets forth CMS' minimal compliance expectations for health care organizations, as well as to indicate that a failure to comply with the referenced standards would be evidence of a HIPAA compliance failure.

Compliance Steps

Develop and Implement Risk Management Strategies. Health care organizations should conduct rigorous risk analysis and risk management to develop policies and procedures for safeguarding ePHI.

Training. It is important that a health care organization's HIPAA training program specifically address vulnerabilities associated with remote access to ePHI. Training should provide, at a minimum, clear and concise instructions for accessing, storing and transmitting electronic PHI.

Addressing a Security Breach. Even with reasonable security measures, security breaches happen as the result of hackers, lost or stolen mobile devices, or disgruntled employees. Health care organizations need a prompt and effective response to a security breach. HIPAA requires a health care organization to mitigate the harmful effects of a security incident. State consumer protection laws may also be applicable regarding consumer notice and/or failure to implement reasonable information security practices. Security incident policies and procedures must specify the actions employees must take to manage the harmful effects of a loss of protected health information. The security incident policies and procedures should address the following scope of issues: (a) investigation of the breach; (b) determination of whether a crime has been committed and law enforcement needs to be notified; (c) determination as to whether to notify consumers, and if so, who should be notified; (d) timely notification, if appropriate; (e) sanctions for the party responsible for the breach; and (f) how to fix and mitigate the breach.

Our firm has assisted numerous companies in addressing ePHI security breaches. We can provide practical advice as you develop and implement the requisite policies and procedures, and training programs. If you have any questions about HIPAA Security matters, please contact Michael Dowell at mdowell@tocounsel.com or the lawyer in the firm who generally handles your health care law legal matters.

©Theodora, Oringher, Miller & Richman