

Resources

HIPAA Security Guidance

Recent security incidents related to the use of laptops, other portable or mobile devices, and external hardware to access or store electronic protected health information (EPHI) has prompted the Office of eHealth Standards and Services (of the US Department of Health and Human Services) to release guidelines regarding the Health Information Portability and Accountability Act (HIPAA). The guidance is particularly relevant for organizations that conduct some of their business through the use of portable media and devices that store EPHI and offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers, or other noncorporate equipment.

Devices and tools of concern include laptops; home-based personal computers; PDAs and smart phones; hotel, library, or other public workstations and wireless access points (WAPs); USB flash drives and memory cards; floppy disks; CDs; DVDs; backup media; E-mail; smart cards; and remote access devices (including security hardware).

In general, offsite use of these devices and tools should be restricted to necessary business use, such as:

- A home health nurse collecting and accessing patient data using a PDA or laptop during a home health visit
- A physician accessing an E-prescribing application on a PDA, while out of the office, to respond to patient requests for refills
- A health plan employee transporting backup enrollee data on a media storage device to an offsite facility

A covered entity must evaluate its own need for offsite use of, or access to, EPHI, and when deciding which security strategies to use, must consider those factors identified in § 45 C.F.R. 164.306(b)(2):

- The size, complexity, and capabilities of the covered entity

- The covered entity's technical infrastructure, hardware, and software security capabilities
- The costs of security measures
- The probability and criticality of potential risks to EPHI

Covered entities should place significant emphasis and attention on their:

- Risk analysis and risk management strategies
- Policies and procedures for safeguarding EPHI
- Security awareness and training regarding the policies and procedures for safeguarding EPHI

For a more detailed review of the HIPAA Security Rule, visit www.cms.hhs.gov and follow the link under "Regulations and Guidance."

Important 2007 Updates to Medicare's Diabetes-related and Other Preventive Services

In 2005, Medicare coverage for preventive services was expanded to include diabetes screening.

Starting January 1, 2007, Medicare began providing more coverage for services that affect people with diabetes, including the following changes:

- Medicare will increase payments to physicians for office visits in which maintenance and promotion of patient health and wellness are discussed. Medicare encourages referrals of eligible patients to existing preventive services such as diabetes outpatient self-management training and medical nutrition therapy, which will be covered services included in the Federally Qualified Health Center benefit. For more information on Federally Qualified Health Centers, visit www.cms.hhs.gov/center/fqhc.asp.
- Medicare is expanding access to rural and underserved areas.

Medicare is also updating other preventive services, including adding a new abdominal aortic aneurysm screening to the "Welcome to Medicare" physical exam and excluding colorectal cancer screening from the Part B deductible.

For a complete list and details of Medicare's preventive services, see: www.medicare.gov and "Preventive Services" or get a free copy of "Guide to Medicare's Preventive Services." MPM