SearchHealthIT.com

How the HITECH Act changes HIPAA compliance

In addition to introducing the concept of meaningful use, the Health Information Technology for Economic and Clinical Health (HITECH) Act made significant changes to the Health Information Portability and Accountability Act (HIPAA) of 1996.

The biggest change to HIPAA compliance is the significant toughening of data breach notification laws, which now not only impose larger fines and require more extensive public notifications when data is lost, but also apply to a health care provider's business associates. Additional updates to HIPAA compliance affect the way providers are authorized to use personal health information for marketing and communication purposes.

The chart below summarizes the major changes made to the HIPAA Privacy and HIPAA Security rules by the HITECH Act. The Department of Health & Human Services outlined these changes in its proposed rule on HIPAA compliance modifications under the HITECH Act, although it should be noted that some of the modifications within that rule are independent of the HITECH Act.

Much of this information comes courtesy of the American Association of Oral and Maxillofacial Surgeons, whose research on HIPAA compliance was passed along by Christopher Paidhrin, security compliance officer for the Southwest Washington Medical Center in Vancouver.

Issue	HIPAA	HITECH Act
Definition of CE	Health plan, clearinghouse or provider involved in the disclosure of PHI	Expanded to include HIE, RHIO, e-prescribing gateway and subcontractor
Is a BA a CE?	No	Yes -- subject to HIPAA Privacy and HIPAA Security rules
Data breach notification	No direct obligation, though state laws vary	Notification required if more than 500 patients affected
Data breach enforcement	Collaborative investigation involving HHS and CE	HHS investigation to determine willful neglect[1]; expanded to include individual employees at CE and BA
Data breach penalties	Minimum of $100, maximum of $25,000	$100 to $50,000 per violation, with yearly maximum of $25,000 to $1.5 million and mandatory penalties for willful neglect

Sale of PHI	Allowed	Prohibited by CEs and BAs without valid authorization, save for certain conditions[2]
Use of PHI in marketing communications	Authorization required, with three exceptions -- CE services, treatment, case management/alternative treatment	Expanded to ban direct or indirect payment for communications; now applies to BAs
Dissemination of PHI to patients	Only if readily available	Must be provided, preferably in electronic format; fee cannot exceed labor cost
Fundraising opt-out	If patients opt out, CE must make "reasonable efforts" to stop	If patients opt out, CE must stop
Definition of electronic media	Limited to storage media, such as tape and disk	Expanded to reference Internet and VoIP technology

Key to acronyms

BA = business associate
CE = covered entity
HHS = Department of Health & Human Services
HIE = health information exchange
PHI = personal health information
RHIO = regional health information organization

[1]The "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated"

[2]Public health activities; research; treatment; services rendered by a BA; or "the sale, transfer, merger, or consolidation of all or part of a CE"

Let us know what you think about this story; email editor@searchhealthit.com.

25 Aug 2010