



## HITECH Implications

©2009, The Long Term Care Consortium (LTCC). These materials may be reproduced and used only by long-term health care providers and their health care affiliates for their internal use, in connection with their efforts to comply with relevant legal rules and regulations. All other reproduction, transfer and use is prohibited without the express written consent of the LTCC. Neither the LTCC nor its members make any representation that use of these materials will ensure legal compliance.

Section	Title	Description	Action	Timing	Comments
13400	Definitions	Establishes a federal breach law, in addition to state security breach laws.	Comply with both federal breach and state security breach notification laws if applicable.		(Doesn't discuss the hybrid record (paper & electronic) just speaks to electronic health records.)
		Definition of breach is expanded from the state breach definitions to include Protected Health Information in hardcopy versus just sensitive information as defined in state breach laws.	Update security breach policy to include protected health information in hard copy form as a security breach.		
		Exceptions to breach include: unintentional or inadvertent and not further use of disclosed.			
13401	Security and Penalty provisions	Security rule and commensurate penalties now also apply to Business Associates as defined 45CFR160.103.	Review business associate agreements for proper language.	Effective date is 12 months from enactment - February 17, 2010.	Prior to ARRA, a BA was subject to the Security Rule contractually through a BA Agreement.
		Secretary of HHS will issue annual guidance re: the use and carrying out appropriate technical safeguards.	Review annual report recommendations when available and compare to current security controls.		Annual guidance could mean annual changes to policies and procedures.

Section	Title	Description	Action	Timing	Comments
13402	Notification of Breach	Covered Entity must notify individuals of a breach. <ul style="list-style-type: none"> <li>• Notification to affected individuals must occur timely, w/in 60 days of discovery</li> <li>• If &gt;10 w/ insufficient or incorrect address must make conspicuous posting as alternate notification.</li> <li>• If &gt;500 media and HHS web posting required</li> <li>• &gt;500 immediate HHS notification</li> <li>• &lt;500 maintain and submit log of breaches to HHS annually</li> </ul>	Update policies to reflect breach notification requirements. Implement an ongoing Breach Log.	Interim Final Rule w/in 180 days - actions will apply to breaches discovered on or after 30 days of interim final rule publication. Possible effective date September 15, 2009.	Providers will have to comply with State and Federal breach notification requirements. It is possible to have a federal breach that is not a breach under state law. May want to specify in BA Agreements that the BA will have the responsibility of notifying affected individuals when it is the BA's breach.
		Breach by BA requires BA to notify Covered Entity.	May need to update BA Agreements to include this requirement.		
		A safe harbors occurs when PHI is secured through encryption or other methods which render the information unreadable, unusable or indecipherable.	Review HHS guidance.	HHS guidance on technologies and methods to secure information was published and is effective as of April 17, 2009. HHS is accepting comments on the guidance until May 21, 2009 and will release an updated guidance if it accepts any stakeholder comments.	
13403	Education on Health Information Privacy	HHS to educate covered entities, business associates and individuals regarding rights and responsibilities for privacy and security of PHI.	Review company education for thoroughness, update as necessary.	Appointment of regional educator for HHS w/in 6 months of enactment - August 2009.	
		Education to public to increase awareness of how their information may be used and their rights.	Consider education to "our public" – residents and families on safeguards to reduce angst.	Education to public within 12 months of enactment - February 17, 2010.	
13404	Privacy Provisions and Penalties - Business Associates	Privacy Rule and penalties apply to business associates. Language related to requirements must be present in contract.	Amend or revise Business Associate Agreements.	Effective date is 12 months from enactment - February 17, 2010.	Prior to ARRA, a BA was subject to the Privacy Rule contractually through a BA Agreement.

Section	Title	Description	Action	Timing	Comments
13405	Restrictions on disclosures; sales of PHI; accounting of disclosures; access to electronic information.	Covered entities must comply with an individual's request to restrict disclosures of information if the disclosure is to a health plan and is related to payment or health care operations only and the entity has been paid in full out of pocket.	Update request for restrictions policy and procedure.	Effective date is 12 months from enactment - February 17, 2010.	
		Minimum necessary disclosure -minimum determined by the covered entity or business associate.	Monitor for updated interpretation from the HHS on what constitutes "minimum necessary"	Minimum necessary guidance expected with in 18 months - August 2010.	
		If a covered entity uses or maintains an Electronic Health Record (EHR), an accounting of disclosures must now include disclosures for treatment, payment, and operations. Must be able to account for treatment, payment, and operations disclosures for 3 years prior to the date of the request.	Work with EHR vendor to ensure software can capture and account for disclosures for treatment, payment and health care operations purposes. Accounting of Disclosure policies and procedures may have to be updated.	If you have an EHR as of 01/01/2009, the compliance date is 01/01/2014. However, if you acquire an EHR after 01/01/2009, the compliance date is 01/01/2011.	There is some question as to what exactly constitutes an EHR. Many providers have electronic systems for billing and MDS purposes - are these systems considered an EHR?  This new requirement differs from Privacy Rule which generally requires a covered entity to account for disclosures up to 6 years prior to the request.
		Accounting of disclosures may include disclosures by the covered entity and the business associate (BA). The covered entity may account for their disclosures and provide the name and contact info of the BA. If requested by the individual, the BA must then account for their disclosures under separate cover.			It appears that the disclosures are trackable only through the EHR.
		Prohibits sale of EHR or PHI directly or indirectly w/o valid authorization. See Act for exceptions.	Review policies and procedures for compliance.	Effective date for this section is a maximum of 24 months from enactment (final rule within 18 months plus 6 months). Possible effective date - February 2011.	
		If a covered entity uses an EHR, individuals have the right to obtain a copy in an electronic format or request transmission to another designated entity or person. Covered entity may impose a charge not to exceed the covered entity's labor cost.	When considering conversion to EHR, consider ease of providing an electronic copy, hardware to do so, and transmission options.	Effective date for this section is 12 months from enactment - February 17, 2010.	

Section	Title	Description	Action	Timing	Comments
13406	Conditions on certain contacts as part of health care operations	Marketing - a communication by a covered entity or business associate about a product or service that is designed to encourage the recipient to purchase or use the product or services is not considered health care operations (except as defined by the Privacy Rule).	Applicability to LTC should be determined based on communications that may come from our business associates (i.e. pharmacy, DME, etc)	Applies to written communications occurring after 12 months from enactment - February 17, 2010.	
		If the covered entity or business associate receives payment for marketing (as described in the Privacy Rule) then the communication is not considered health care operations with some exceptions. <b>The term payment does NOT include payment for treatment.</b>			
		Recipient may opt-out" of receiving fundraising communications. Option must be presented clearly and conspicuously.	May need to update Fundraising policies and procedures.		
13407	Temporary Breach Notification requirement for vendors of PHR and other non-HIPAA covered entities	Applies to a vendor of Personal Health Records (PHR) and other non-HIPAA entities.	Applies only to non-HIPAA covered entities.	FTC must publish an Interim Final Rule w/in 180 days - actions will apply to breaches discovered on or after 30 days of interim final rule publication. Possible effective date September 15, 2009.	
		Requires notification of the individual whose unsecured information was acquired by an unauthorized person due to a security breach. Specific mention is made that it applies to resident or citizen of the US.			
		Also requires notification to the Federal Trade Commission (FTC). FTC is the enforcement agency.			
13408	Business Associate contracts required for certain entities	Vendors that contract with a covered entity to offer a PHR are required to enter into a contract and shall be treated as a business associate.	May widen what type of vendors are considered business associates for the purpose of privacy and security.	As of date of enactment - February 17, 2009.	
		Applicability to Health Information Exchange Organizations and Regional Health Information Organizations, E-prescribing Gateway organizations.			
13409	Clarification of application of wrongful disclosures criminal penalties	Updates the Social Security Act (SSA) to specify that criminal penalties apply to individuals and employees of a covered entity who disclose individually identifiable health information maintained by the covered entity without proper authorization. Such wrongful disclosure would constitute a HIPAA violation.	Consider additional education to notify employees of penalties that may be applied to them should they wrongfully disclose individually identifiable health information.	Effective date for this section is 12 months from enactment - February 17, 2010.	

Section	Title	Description	Action	Timing	Comments
13410	Improved Enforcement	<b>Adds a section to SSA section 1177 to include willful neglect as a violation.</b>	Update definition of a violation to include "willful neglect" and train staff on examples of "willful neglect".	Applies to penalties imposed on or after 24 months after the date of enactment - February 17, 2011. HHS shall promulgate regulations to implement the amendments no later than 18 months after enactment - August 2010.	
		Requires HHS to formally investigate a complaint if a preliminary investigation indicates a possible violation due to willful neglect. A violation due to willful neglect is subject to enforcement and penalties.			
		Individuals harmed by a violation may receive a percentage of the Civil Monetary Penalties (CMPs) collected.		Methodology for distribution of collected CMPs to harmed individuals to be established within 3 years of enactment.	
		<b>Tiers of penalties are defined.</b> <a href="http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&amp;docid=f:h1enr.txt.pdf">http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&amp;docid=f:h1enr.txt.pdf</a> (pp. H-R-1- 159)	Update training to include the increased penalties.	Applies to violations occurring after the date of enactment - February 17, 2009.	
		Increases penalties and differentiates by amount the penalty for reasonable cause vs. willful neglect to a yearly maximum of \$1,500,000 for all violations of an identical requirement or prohibition.			
		<b>State Attorney Generals can bring civil suits on behalf of residents of a state against any person for harm due to a violation.</b>		Applies to violations occurring after the date of enactment - February 17, 2009.	
		Adds language of the SSA with regard to statute of limitations and State action while Federal action is pending.		Applies to violations occurring after the date of enactment - February 17, 2009.	
13411	Audits	HHS shall provide for periodic audits of covered entities and business associates.		Effective as of the date of enactment - February 17, 2009.	Prior to ARRA, enforcement was complaint driven.
Part 2 13421	Relationship to other laws	HIPAA remains in effect to the extent it is consistent with new privacy and security requirements.	Implement updated provisions as necessary. Upgrade training where applicable.		HHS will amend federal regulations as required to make the Privacy and Security Rules consistent with this Act.
13423	Effective date	If not otherwise specified, effective date is 12 months after enactment.			
13424	Studies, Reports, Guidance	HHS is required to report on HIPAA covered entities' compliance to Congress annually. HHS with the FTC will conduct a study on the applicability to non-HIPAA covered entities. And provide implementation specification guidance to de-identify PHI.		12 months from date of enactment - February 17, 2010.	