

EFFECT OF THE HITECH ACT ON HIPAA

Topic	Existing Law	HITECH ACT	Effective Date	Comments
Criminal Penalties for Individuals	On June 1, 2005, the DOJ Office of Legal Counsel issued a position paper stating that only covered entities could be directly liable for criminal violations of HIPAA. While this memo was not followed by all federal prosecutors, it may have limited the number of cases brought against individuals.	Under Section 13409, individuals can now be criminally liable for violations of HIPAA. Section 13409 adds the following language to HIPAA: "[A] person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1180(b)(3)) and the individual obtained or disclosed such information without authorization."	Feb. 17, 2010	This provision gives new leverage to individuals or entities seeking redress for privacy violations.
Enhanced Enforcement	Before the HITECH Act, civil monetary penalties for HIPAA violations were limited to \$100 per violation, with a maximum of \$25,000 for all violations of an identical requirement in a single year.	<p>Section 13410(a) states that HHS <u>must</u> investigate any complaint that may have resulted from "willful neglect" by a covered entity or business associate.</p> <p>Section 13410(c) states that a methodology will be developed by which victims of privacy violations may receive a share of penalties that are collected.</p> <p>Section 13410(d) establishes significant, tiered civil monetary penalties for HIPAA violations. Fines start at \$100 per violation (maximum \$25,000 per year) and go to \$50,000 per violation (maximum \$1,500,000 per year).</p> <p>Section 13410(e) provides that state attorneys general may bring a civil action to enjoin privacy or security violations or obtain damages on behalf of state residents for such violations. Damages in</p>	<p>"Willful neglect" provision – Feb. 17, 2011</p> <p>Compensation methodology – Feb. 17, 2012</p> <p>Tiered penalties – Feb. 17, 2009</p> <p>Attorney general enforcement – Feb. 17, 2009</p>	This provision increases the penalties for privacy violations and the likelihood that such penalties will be imposed.

Topic	Existing Law	HITECH ACT	Effective Date	Comments
		such actions are limited to \$100 per violation, up to a maximum of \$25,000 for violations of the same requirement.		
<p>Notification to Patient and Others in Case of Breach of Confidentiality</p>	<p>HIPAA does not directly require covered entities to notify patients or others if PHI is improperly disclosed. (The closest HIPAA comes is requiring covered entities to take steps to mitigate damages resulting from a breach.) Many states have breach notification laws, but these are often of limited effect.</p>	<p>Under Section 13402, covered entities must notify individuals whose "<u>unsecured</u> protected health information" has been accessed or disclosed as a result of a "<u>breach</u>." Similarly, a business associate must notify a covered entity of a breach (with the covered entity then notifying the individual).</p> <p>Generally, PHI is "unsecured" when it is not secured by a technology that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals. HHS has issued guidance describing the specific methodologies that satisfy this standard (such as certain encryption technologies).</p> <p>A "breach" only occurs if, among other things, an improper use or disclosure of PHI "poses a significant risk of financial, reputational, or other harm to the individual." Thus, covered entities must conduct a case-by-case analysis to determine if patient notification is required.</p> <p>If notice is required, it must be provided in writing via first-class mail within 60 days of discovery of the breach. Among other things, the notice must tell individuals what happened and what they can do to protect themselves.</p> <p>If the breach involves more than 500 individuals, notice must also be provided</p>	<p>The breach notification provisions apply to breaches that occur on or after September 23, 2009. HHS has stated that it will not impose sanctions for violations of the breach notification provisions until February 22, 2010. HHS expects compliance before February 22, 2010, and will work with covered entities to achieve it, but will not impose sanctions for violations during that time frame.</p>	<p>The breach notification provisions only apply to "unsecured protected health information." Thus, covered entities have a significant incentive to encrypt PHI or take other steps to ensure it is not "unsecured."</p>

Topic	Existing Law	HITECH ACT	Effective Date	Comments
		immediately to HHS and to "prominent media outlets" in the area. Moreover, HHS must be informed of all breaches on at least an annual basis.		
Application of Privacy Rule to Business Associates	Business associates are not directly bound by the Privacy Rule, and are not subject to civil or criminal penalties for improper disclosures of PHI. Instead, business associates are indirectly regulated through business associate agreements.	<p>Under Section 13404, a business associate may only use or disclose PHI in a manner that complies with 45 C.F.R. § 164.504(e) (which describes the requirements for business associate agreements). Thus, business associates will now be regulated directly through a statutory requirement rather than indirectly through a contract. Business associates also must comply with the applicable provisions of the HITECH Act.</p> <p>Business associates will be subject to civil and criminal penalties if they violate these provisions.</p>	Feb. 17, 2010	<p>Business associate agreements will have to be revised. The federal government has stated that it will provide additional guidance regarding business associate agreements by the end of 2009.</p> <p>If business associates have been complying with existing business associate agreements, Section 13404 should not result in significant additional work. However, the consequences of a privacy violation will increase significantly.</p>
Application of Security Rule to Business Associates	Business associates are not directly bound by the Security Rule, and are not subject to civil or criminal penalties for improper disclosures of PHI. Instead, business associates are indirectly regulated through business associate agreements.	<p>Under Section 13401, business associates will be required to comply with provisions of the HITECH Act, and with the following provisions of the Security Rule:</p> <p>§ 164.308 (Administrative Safeguards);</p> <p>§ 164.310 (Physical Safeguards);</p> <p>§ 164.312 (Technical Safeguards);</p> <p>§ 164.316 (Policies and Procedures).</p> <p>Business associates will also be subject to civil and criminal penalties if they violate these provisions.</p>	Feb. 17, 2010	Business associates must implement standards and "required" implementation specifications set forth in the Security Rule. They must also analyze whether to adopt "addressable" implementation specifications and, if not, must document their rationale. Business associates will have to expend considerable time and money to satisfy these requirements. Also, business associate agreements will have to be revised.

Topic	Existing Law	HITECH ACT	Effective Date	Comments
<p>Disclosures Limited to the "Minimum Necessary" or a "Limited Data Set"</p>	<p>A covered entity is generally required to limit its request, use or disclosure of PHI to the "minimum necessary" to accomplish the purpose of the request, use or disclosure. However, this requirement does not apply to treatment and certain other situations.</p>	<p>Under Section 13405(b), the "minimum necessary" requirement will only be satisfied if a covered entity or business associate uses a "limited data set," provided, however, that if using a limited data set is not "practicable," then the "minimum necessary" may still be used. This rule will no longer be in effect once HHS issues additional guidance as to what constitutes the "minimum necessary" for purposes of the Privacy Rule. This guidance is to be issued by August 17, 2010. This section also clarifies that the covered entity or business associate disclosing PHI is the one who determines the "minimum necessary."</p>	<p>Feb. 17, 2010</p>	<p>This provision could significantly increase the administrative burden on covered entities. For example, if medical records are to be sent to an external reviewer, there is no reason a limited data set could not be used. Thus, only a limited data set would satisfy the minimum necessary requirement.</p>
<p>Accounting of Disclosures</p>	<p>An individual may request an accounting of the disclosures of that individual's PHI. However, covered entities do not have to account for disclosures made for treatment, payment or health care operations.</p>	<p>Under Section 13405(c), covered entities that use electronic health records must account for disclosures of PHI even for treatment, payment or health care operations. HHS will publish regulations as to the type of information that has to be provided in an accounting.</p>	<p>Jan. 1, 2014, if the covered entity had an electronic health record ("EHR") as of Jan. 1, 2009.</p> <p>The later of Jan. 1, 2011 or the date on which a covered entity acquires an EHR, for covered entities that did not have an EHR as of Jan. 1, 2009.</p>	<p>The significance of this provision will depend partly on the regulations that HHS adopts to implement it. Presumably, users of an electronic health record will be prompted to identify the purpose of a disclosure any time PHI is to be printed or e-mailed. It is unclear how disclosures will be logged for hospitals that allow medical staff members to gain remote access to their electronic health records.</p>
<p>Prohibition on Sale of EHRs or PHI</p>	<p>There is currently no prohibition on a covered entity or business associate being paid for disclosing PHI for authorized purposes. With respect to sales of PHI for marketing, the Privacy Rule currently states "[i]f the marketing</p>	<p>Under Section 13405(d), a covered entity or business associate may not receive remuneration in exchange for PHI unless the individual has signed an authorization which states that remuneration will be paid. However, there are numerous exceptions, including those for public</p>	<p>No later than Aug. 16, 2010, HHS is required to issue regulations to implement this provision. This provision will</p>	

Topic	Existing Law	HITECH ACT	Effective Date	Comments
	involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved." 45 C.F.R. § 164.508(a)(3)(ii).	health, research, treatment, sales or mergers, payments to a business associate for services performed for the covered entity, payments by an individual to obtain a copy of that individual's records, or other exchanges set forth by HHS in a regulation.	become effective six months after those regulations are issued.	
Restrictions on Certain Disclosures	Individuals must be permitted to request restrictions on the use or disclosure of their PHI for treatment, payment or health care operations. However, the covered entity is not required to grant such requests.	Under Section 13405(a), a covered entity must grant a request for a restriction if (1) the disclosure is to a health plan for purposes of either payment or health care operations, and (2) the PHI pertains to a service for which the patient paid in full out-of-pocket.	Feb. 17, 2010	
Access to PHI in Electronic Format	Individuals have the right to obtain a copy of their PHI maintained in a designated record set.	Under Section 13405(e), individuals have the right to obtain a copy of their PHI in electronic format if the covered entity uses an EHR.	Feb. 17, 2010	This provision should have minimal effect on covered entities.
Marketing	A covered entity generally must obtain an authorization for any use or disclosure of PHI for marketing purposes. The definition of "marketing" set forth at 45 C.F.R. § 164.501(1) does not include (i) descriptions of health-related products or services offered by the covered entity, (ii) communications for treatment purposes, or (iii) communications for care coordination or to suggest alternative therapies.	Under Section 13406(a), a communication continues to be excluded from the definition of "marketing" in 45 C.F.R. § 164.501(1) if it meets the requirements of subsections (i), (ii), or (iii), <u>unless</u> the covered entity receives direct or indirect remuneration for the communication. If payment is made, the communication <u>is</u> marketing unless: (1) the communication describes a drug or biologic and any payment made is reasonable; or (2) the communication is made by the covered entity and the covered entity obtains an authorization from the patient; or	Feb. 17, 2010	

Topic	Existing Law	HITECH ACT	Effective Date	Comments
		<p>(3) the communication is made by a business associate pursuant to a business associate agreement.</p> <p>For purposes of these provisions, the term "direct or indirect" payment does not include any payment for treatment.</p>		
<p>Fundraising</p>	<p>The Privacy Rule currently states:</p> <p>(ii) The covered entity must include in any fundraising materials it sends to an individual under this paragraph a description of how the individual may opt out of receiving any further fundraising communications.</p> <p>(iii) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.</p> <p>45 C.F.R. § 164.514(f)(2).</p>	<p>Section 13406(b) states that HHS "shall by rule provide that any written fundraising communication that is a healthcare operation . . . shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication."</p>	<p>Feb. 17, 2010</p>	<p>The HITECH Act makes the opt-out provisions for fundraising a statutory requirement, as opposed to only a regulatory requirement.</p>