



CHART YOUR HIPAA COURSE . . .

**HITECH Act  
 Security Breach Notification Requirement**

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>Scope – HIPAA Covered Entities</b>	<ul style="list-style-type: none"> <li>• In case of "breach," HIPAA covered entity (health plan, provider, clearinghouse) must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of the breach.</li> <li>• Business associate also must notify covered entity of breach, including identification of each individual whose information was breached.</li> <li>• "Breach" means unauthorized acquisition, access, use, or disclosure of PHI which compromises security, privacy, or integrity of PHI. Does not include unintentional disclosures if made in good faith and within course and scope of employment or business associate relationship, and PHI not further acquired, accessed, used or disclosed.</li> <li>• Violation of this section treated as violation of HIPAA privacy and security rules.</li> </ul>	<ul style="list-style-type: none"> <li>• HHS to issue interim final regulations governing HIPAA covered entities no later than 180 days from enactment (by 8/16/09).</li> </ul>

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>Scope – PHR Vendors</b>	<ul style="list-style-type: none"> <li>• If vendor of personal health records (PHR) discovers breach of unsecured PHR identifiable health information, must notify each individual who is a US citizen or resident and Federal Trade Commission (FTC) that PHR was acquired by unauthorized person.</li> <li>• Also applies to entities offering products or services through a PHR vendor's or covered entity's website or an entity that accesses or sends information to a PHR ( as well as third party service providers).</li> <li>• Notification subject to same delivery, timing, and content requirements as for covered entity notification.</li> <li>• FTC to notify Secretary of HHS.</li> <li>• Violation of this section treated as unfair and deceptive act or practice under Federal Trade Commission Act.</li> </ul>	<ul style="list-style-type: none"> <li>• PHR vendor is an entity (other than a HIPAA covered entity or business associate of a covered entity) that offers or maintains PHRs.</li> <li>• PHR related entity is an entity (other than a HIPAA covered entity or business associate of a covered entity) that offers products or services through the website of a PHR vendor or a covered entity, or an entity that accesses information in a PHR or sends information to a PHR.</li> <li>• Preamble says that examples of a PHR related entity include:             <ul style="list-style-type: none"> <li>- Web-based application that helps consumers manage medications.</li> <li>- Website offering an online personalized health checklist.</li> <li>- Brick and mortar company advertising dietary supplements online.</li> <li>- Online application through which individuals connect their blood pressure cuffs, blood glucose monitors, or other devices so that results can be tracked through a PHR.</li> <li>- Online medication or weight tracking program that pulls information from a PHR.</li> </ul> </li> </ul>

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>Applicable only to Breaches of "Unsecured PHI"</b>	<ul style="list-style-type: none"> <li>• Notification requirement only applies to a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses "unsecured PHI" - defined as PHI not secured through use of a technology or methodology specified by Secretary.</li> <li>• Within 60 days of enactment and annually thereafter, HHS must issue guidance specifying technologies that meet this standard.</li> <li>• If HHS does not issue guidance, required technology standard shall be one developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.</li> </ul>	<ul style="list-style-type: none"> <li>• Definition of "secure PHI" not part of FTC guidance.</li> <li>• HHS issued guidance on "secure PHI" on April 27, 2009. Comments on HHS guidance due 5/21/09.</li> <li>• HHS described two technologies that will be considered "secure" and exempt from security breach notification requirement – (1) Encryption, and (2) Destruction.</li> <li>• (1) <u>Encryption</u> – PHI will be considered rendered unusable, unreadable, or indecipherable if it has been encrypted by an algorithmic process to transform data into a form where there is low probability of assigning meaning without use of a confidential process or key, and such confidential process or key has not been breached. HHS identified specific encryption process.</li> <li>• (2) <u>Destruction</u> – PHI also will be considered unusable, unreadable, or indecipherable if it has been shredded or destroyed such that it cannot be read or otherwise reconstructed (for paper or hard copy) or has been cleared, purged, or destroyed consistent with specific NIST standards (for electronic media).</li> </ul>

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>Breach – PHR Vendors</b>	<ul style="list-style-type: none"> <li>• “Breach” is defined as acquisition of information without the authorization of the individual.</li> </ul>	<ul style="list-style-type: none"> <li>• Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless PHR vendor has reliable evidence showing there has not been, or could not reasonably have been, unauthorized acquisition.</li> <li>• Preamble says examples of "breach" include theft of laptop, theft of hard copies, unauthorized downloading or electronic break-in of data, and remote copying of records by hacker.</li> <li>• Preamble gives example of rebuttable presumption: If entity's employee loses laptop with unsecured PHI, entity can rebut presumption of unauthorized acquisition by showing laptop was recovered and forensic analysis reveals no files were compromised.</li> <li>• Preamble notes that "PHR identifiable health information" subject to the breach notification requirement includes the fact that someone has an account with a PHR vendor, where the product or service offered by the vendor relates to a particular health condition. Also would include the breach of a database containing names and credit card information, even if no other information was included.</li> </ul>

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>When Breach is Considered "Discovered"</b>	Breach is "discovered" when entity knew or reasonably should have known breach occurred.	<ul style="list-style-type: none"> <li>• Breach will be considered "discovered" on the first day it is known to the PHR vendor or third party service provider, or reasonably should have been known.</li> <li>• Burden is on the PHR vendor to demonstrate that all notifications are made.</li> <li>• When third party service provider discovers breach, must provide notice of breach to senior official at PHR vendor and obtain acknowledgement that notice was received.</li> <li>• Preamble states that if the PHR vendor discovers a breach by a service provider, the PHR vendor should treat the breach as "discovered" at that time, and should not wait to receive notice from the service provider to begin taking steps to address the breach.</li> </ul>
<b>Timing of Notification</b>	Notice must be made "without unreasonable delay," but no later than 60 calendar days after discovery.	<ul style="list-style-type: none"> <li>• Preamble clarifies that the 60-day period is the "outer limit" and, in some cases, it may be "unreasonable" to wait the full 60 days.</li> </ul>

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>Notification to Individual</b>	<ul style="list-style-type: none"> <li>Individual notice to be made by first-class mail to last known address.</li> <li>May be made by electronic mail "if specified as a preference by the individual."</li> <li>If breach deemed by covered entity to require urgency due to possible imminent misuse of unsecured PHI, may provide notice by telephone or other means, as appropriate.</li> <li>Notice may be delayed for law enforcement purposes, consistent with rules for delay of accounting under HIPAA Privacy Rules.</li> </ul>	<ul style="list-style-type: none"> <li>In order to provide electronic notice, individual must give "express affirmative consent."</li> <li>Preamble states that entities may obtain such consent by asking individuals whether they would prefer to receive notice by email when they create an account.</li> <li>Preamble says that FTC does not regard "pre-checked boxes" or "disclosures that are buried in a privacy policy or terms of service agreement" to be sufficient.</li> </ul>
<b>Substitute Notice to Individual</b>	<ul style="list-style-type: none"> <li>If contact information is insufficient or out of date, must provide substitute form of notice.</li> <li>If 10 or more individuals have insufficient or out-of-date contact information, covered entity must (1) conspicuously post notice on home page for period determined by Secretary; or (2) provide notice in major print or broadcast media in geographic regions where individuals likely to reside. Posting must include toll-free contact number.</li> </ul>	<ul style="list-style-type: none"> <li>Substitute form of notice, in the event of insufficient or out-of-date contact information, may be in the form of the individual's less preferred method or by telephone.</li> <li>Where 10 or more individuals are involved, an entity is required to either (1) post notice on its home page for six months or (2) provide notice to major print or broadcast media in the geographic area where affected individuals are likely to reside.</li> <li>Preamble says website notice should be provided on the homepage and "landing" page for existing account holders and should be prominent.</li> <li>Preamble says that, for media notice, PHR vendor should take into account the number of individuals involved, their location, and the reach of the particular media. Preamble says the notice should be "clear and conspicuous," which means that it should "be stated in plain language, be prominent, and run multiple times."</li> </ul>

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>Notification to HHS / FTC</b>	<ul style="list-style-type: none"> <li>• Must give notice of breach to Secretary.</li> <li>• If 500 or more individuals affected, must give notice immediately.</li> <li>• Otherwise, may maintain log of breaches and annually submit to Secretary.</li> <li>• Secretary to list covered entities with breaches affecting more than 500 individuals on HHS website.</li> </ul>	<ul style="list-style-type: none"> <li>• Where a breach involves 500 or more individuals, notice must be given to the FTC "as soon as possible," but no later than 5 business days following discovery of the breach.</li> <li>• Preamble says FTC will post a form on its website that PHR vendors can use to report security breaches.</li> </ul>
<b>Notification to Media</b>	<ul style="list-style-type: none"> <li>• Substitute Media Notice - If 10 or more individuals have insufficient or out-of-date contact information, covered entity may provide substitute notice through media (or may post on homepage). Must provide notice in major print or broadcast media in geographic regions where individuals likely to reside.</li> <li>• Notice When More Than 500 People Involved - If more than 500 residents of a State or jurisdiction affected, must provide notice to "prominent media outlets" serving that State or jurisdiction</li> </ul>	<ul style="list-style-type: none"> <li>• Media notice should include all of the content requirements of the notice to individuals.</li> <li>• Substitute Media Notice - For substitute media notice, Preamble says scope of substitute media notice depends on number of individuals involved, location, and reach of particular media. For example, if hacker obtains a million records with no contact information available, notice should run multiple times in national print and on network and cable TV. If online weight management application loses customer list and can reach all but 20 individuals in a particular city, notice can be limited to advertisement in local media.</li> <li>• Notice When More Than 500 People Involved - Preamble says, at a minimum, a press release should be disseminated to the media outlets in the areas affected by the breach. For example, if breach affects individuals from a particular locality, the press release could be sent to the relevant division or department (e.g., health, technology, or business) of a number of state or local print publications, network and cable news shows, and radio stations.</li> </ul>

Issue	HITECH Act (Stimulus Bill) Enacted 2/17/09	Additional Clarifications from FTC Proposed Regulations (except where noted, FTC adopts language of statute) <b>**Comments Due 6/1/09 - See end of chart for FTC questions.</b>
<b>Content of Notification</b>	<ul style="list-style-type: none"> <li>Brief description of what happened, including date of breach and date of discovery.</li> <li>Types of PHI involved (e.g., name, SSN, address).</li> <li>Steps individuals should take to protect themselves from potential harm.</li> <li>Brief description of steps covered entity is taking to investigate, mitigate losses, and protect against further breaches.</li> <li>Contact information, including toll-free telephone number, email address, website, or postal address.</li> </ul>	<ul style="list-style-type: none"> <li>Preamble notes that the breach notification should not include a request for personal or financial information in order to avoid concerns about "phishing."</li> <li>Preamble provides examples of steps an entity can suggest that individuals take to protect themselves – such as reviewing copies of medical files or explanations of benefits, reviewing credit reports, and monitoring other accounts and bills.</li> </ul>
<b>Regulations / Effective Date</b>	<ul style="list-style-type: none"> <li>HHS / FTC to issue interim final regulations within 180 days of enactment.</li> <li>Effective Date - This section applies to breaches that are discovered on or after the date that is 30 days after the date of publication of these interim final regulations.</li> </ul>	<ul style="list-style-type: none"> <li>FTC issued proposed regulations 4/20/09. Comments due 6/1/09.</li> </ul>

**\*\*Comments on the FTC proposed regulations are due June 1, 2009. See 74 Fed. Reg. 17915 (April 20, 2009).**

The FTC specifically requested comment on the following items:

- The nature of entities to which its proposed rule would apply and the particular products and services they offer.
- The extent to which PHR vendors, PHR-related entities, and third party service providers may be HIPAA-covered entities or business associates of HIPAA covered entities.

- Whether some PHR vendors may have a dual role as a business associate of a HIPAA covered entity and a direct provider of PHRs to the public.
- Circumstances in which such a dual role might lead to a consumers' receiving multiple breach notices or receiving breach notices from an unexpected entity, and whether and how the rule should address such circumstances.
- The standard that should apply to substitute media notices.
- How to address when some email notifications may be screened by consumers' spam filters.
- The standards and criteria that should apply in determining the adequacy of media notices.

\* \* \*