HITECH Act (H.R. 1)
Summary of HIPAA Privacy & Security Provisions
Enacted 2/17/09

by Christy Tinnes, Groom Law Group

Section	Topic	H.R. 1
13401	**HIPAA Security Standards apply to Business Associates**	• HIPAA Security Standards apply to business associate in same manner as covered entity. • HIPAA civil and criminal administrative simplification penalties apply to business associate in same manner as covered entity. • New security requirements in bill must be incorporated into business associate contracts. • Secretary of HHS to issue annual guidance on most effective and appropriate technical safeguards.
13402(a)	**Notification of Breach**	• In case of "breach," covered entity 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. • "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.
13402(b)	**Duty to Notify:** **When Breach is by Business Associate**	Business associate must notify covered entity of breach, including identification of each individual whose information was breached.
13402(c)	**Duty to Notify:** **When Breach is Considered "Discovered"**	Breach is "discovered" when entity knew or reasonably should have known breach occurred.

Section	Topic	H.R. 1
13402(d)	**Duty to Notify:** **Timing of Notification**	Notice must be made "without unreasonable delay," but no later than 60 calendar days after discovery.
13402(e), (g)	**Duty to Notify:** **Method of Notification**	• Individual notice to be made by first-class mail to last known address. • May be made by electronic mail "if specified as a preference by the individual." • If contact information is insufficient or out of date, must provide substitute form of notice. If 10 or more individuals have insufficient or out-of-date contact information, covered entity must conspicuously post notice on home page for period determined by Secretary or provide notice in major print or broadcast media in geographic regions where individuals likely to reside. Posting must include toll-free contact number. • 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. • If more than 500 residents of a State or jurisdiction affected, must provide notice to "prominent media outlets" serving that State or jurisdiction (jurisdiction not defined). • Must give notice of breach to Secretary. If 500 or more individuals affected, must give notice immediately. Otherwise, may maintain log of breaches and annually submit to Secretary. • Secretary to list covered entities with breaches affecting more than 500 individuals on HHS website. • Notice may be delayed for law enforcement purposes, consistent with rules for delay of accounting under HIPAA Privacy Rules.

Section	Topic	H.R. 1
13402(f)	**Duty to Notify:** **Content of Notification**	Content of notice: • Brief description of what happened, including date of breach and date of discovery. • Types of PHI involved (*e.g.*, name, SSN, address). • Steps individuals should take to protect themselves from potential harm. • Brief description of steps covered entity is taking to investigate, mitigate losses, and protect against further breaches. • Contact information, including toll-free telephone number, email address, website, or postal address.
13402(h)	**Duty to Notify:** **Applicable only to Breaches of "Unsecured PHI"**	• 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. • Within 60 days of enactment and annually thereafter, Secretary must issue guidance specifying technologies that meet this standard. • If Secretary 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.
13402(j)	**Duty to Notify:** **Regulations / Effective Date**	• Secretary to issue interim final regulations within 180 days of enactment. • 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.
13403	**Education**	• Within 6 months of enactment, Secretary shall designate individuals in each regional office to offer guidance and education on privacy and security rules. • Within 12 months of enactment, HHS must develop national education initiative.

Section	Topic	H.R. 1
13404	**HIPAA Privacy Rules apply to Business Associates**	• HIPAA Privacy Rules, as set out in business associate contract, apply directly to business associate (no longer just contractual obligation). • HIPAA civil and criminal administrative simplification penalties apply to business associate in same manner as covered entity.
13405(a)	**Right to Restrict**	• If individual requests restriction of disclosure of PHI to health plan for purposes of payment or health care operations, covered entity must comply. • Only applies where provider has been paid out of pocket in full.
13405(b)	**Minimum Necessary**	• Secretary to issue guidance on what constitutes "minimum necessary" within 18 months of enactment. • Until guidance is issued, covered entity must limit use and disclosure of PHI, to the extent practicable, to information under limited data set rules. (Under these rules, limited data set information must exclude direct identifiers, such as name, address, SSN, ID numbers.) • Disclosing covered entity or business associate to make determination as to what constitutes minimum necessary PHI. • Exceptions under current minimum necessary rule continue to apply (*e.g.*, for treatment, to individual, pursuant to authorization, required by law).

Section	Topic	H.R. 1
13405(c)	**Accounting**	• If covered entity or business associate maintains an "electronic health record," must account for disclosures even for treatment, payment, or health care operations (TPO) (currently excepted from accounting rule). • TPO accounting limited to past 3 years (6 years in current accounting rule). Secretary to provide guidance on what information must be collected. • Covered entity either can provide accounting of its TPO electronic disclosures, along with that of business associates', or may provide its own accounting and list contact information for all business associates. • "Electronic health record" defined as an electronic record or health-related information on an individual that is created, gathered, managed, or consulted by authorized health care clinicians and staff. <u>Effective Dates</u>: • For electronic health records held by covered entity as of 1/1/09, accounting requirement applies to TPO disclosures on or after 1/1/14. • For electronic health records acquired by covered entity after 1/1/09, accounting requirement applies to TPO disclosures after 1/1/11. • Secretary may set later effective date if determined to be "necessary," but must be by 2016 (for electronic health information held as of 1/1/09) and 2013 (for electronic health information acquired after 1/1/09).
13405(d)	**Remuneration for PHI**	• Neither covered entity nor business associate may receive direct or indirect remuneration in exchange for PHI, except where individual authorizes. • Authorization must specify whether PHI can be further exchanged for remuneration. • Exceptions – Remuneration permitted if PHI exchanged for public health activities, research, treatment, sale of covered entity, services under business associate contract, providing individual with copy of PHI, or as determined by Secretary in regulations. • Secretary must issue regulations within 18 months of enactment. • Effective Date - Applies to exchanges on or after 6 months after date of final regulations.

Section	Topic	H.R. 1
13405(e)	**Access to EPHI**	• Where covered entity uses or maintains "electronic health record," individual may request right to access information in electronic format (in addition to current right to access PHI). • Individual also may direct covered entity to transmit a copy of electronic health record directly to an entity or person designated by the individual, provided that direction is clear, conspicuous, and specific. • Fee charged by covered entity limited to labor costs in responding to request.
13406	**Marketing / Fundraising**	• Communication about a product or service that encourages recipient to purchase or use product or service only will be considered "health care operations" if covered entity does not receive direct or indirect remuneration in exchange for the communication and the communication meets certain exceptions under "marketing" definition: (i) to describe health-related product or service included in plan of benefits, such as entities participating in network, replacement of or enhancements to health plan, and services or products that add value to, but are not part of, plan of benefits; (ii) for treatment; or (iii) for case management or care coordination, or to direct alternative treatments, providers, or settings of care. • Remuneration permitted if communication only describes drug or biologic currently being prescribed and payment is reasonable or if individual authorizes. • In order to fall under definition of "health care operations," any written fundraising communication by covered entity shall, in clear and conspicuous manner, provide recipient opportunity to opt out of further communications. Opt out is treated as a revocation of authorization. Secretary to issue additional rules.

Section	Topic	H.R. 1
13407	**Duty to Notify of Breach by Vendors of Personal Health Records**	• 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. • FTC to notify Secretary of HHS. • 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). • "Breach" is defined as acquisition of information without the authorization of the individual. A breach is considered discovered when entity knew or reasonably should have known breach occurred. • Notification subject to same delivery, timing, and content requirements as for covered entity notification (above). • Violation of this section treated as unfair and deceptive act or practice under Federal Trade Commission Act. • Notification requirement only applies to breach of "unsecured" PHR, defined as PHR not secured through use of a technology or methodology specified by Secretary. Secretary to issue guidance under same requirements for covered entity notification (above). • FTC to issue interim final regulations within 180 days of enactment. • 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.
13408	**PHR Vendors Considered Business Associates**	• Any organization providing data transmission services to covered entity or business associate is considered business associate. • Applies to vendor that contracts with covered entity to allow covered entity to offer PHRs. • Applies to Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway.
13409 / 13410	**Enforcement - Criminal Penalties**	• Extends criminal penalties under HIPAA to any individual (whether or not an employee of the covered entity) who obtains or discloses information without authorization. • Secretary may bring civil or criminal penalties (current law limits criminal enforcement to DOJ).

Section	Topic	H.R. 1
13410	**Enforcement – Civil Penalties**	• A civil penalty may be imposed, except where a criminal penalty actually has been imposed (formerly, a civil penalty could not be imposed if the violation merely was punishable as a criminal penalty). • Secretary is required to impose a civil penalty if there is a violation due to willful neglect. If a preliminary investigation of a complaint indicates possible violations due to willful neglect, the Secretary is required to formally investigate. • Above provisions apply to penalties imposed on or after 24 months from enactment; Secretary to issue regulations within 18 months of enactment. • Increase in penalties (in determining amount, Secretary to assess nature, extent, and harm of violation) - - Where person does not know (and by exercising due diligence would not have known) of violation, minimum penalty is $100 per violation, with a cap of $25,000 for violations of an identical requirement during a calendar year; maximum penalty is $50,000 per violation, with a cap of $1.5 million for violations of an identical requirement during a calendar year; - Where violation is due to "reasonable cause," minimum penalty is $1,000 per violation, with a cap of $100,000 for violations of an identical requirement during a calendar year; maximum penalty is $50,000 per violation, with a cap of $1.5 million for violations of an identical requirement during a calendar year; and - Where violation is due to "willful neglect," minimum penalty is $10,000 per violation, with a cap of $250,000 for violations of an identical requirement during a calendar year; maximum penalty is $50,000 per violation, with a cap of $1.5 million for violations of an identical requirement during a calendar year. • Above penalties not applicable if corrected within 30 days after person knew (or by exercising reasonable diligence should have known) of violation. Applicable to violations occurring after date of enactment. • Any civil penalty collected shall be transferred to Office of Civil Rights (HHS) for purposes of enforcement. Within 18 months of enactment, GAO to submit recommendations for methodology under which harmed individuals may receive percentage of civil penalties. Secretary must establish such methodology within 3 years of enactment. • Nothing in the bill to be construed as preventing HHS from using corrective action without penalty where the person did not know (and by exercising due diligence would not have known) of the violation.

Section	Topic	H.R. 1
13410	**Enforcement – State Attorneys General**	• State Attorneys General may bring civil action on behalf of residents in district court to enjoin violations and obtain damages on behalf of state's residents of up to $100 per violation, with a cap of $25,000 for violations of an identical requirement during a calendar year. May not bring if Secretary already has instituted action. Applies to violations occurring after the date of enactment.
13411	**Audits**	The Secretary shall periodically audit covered entities and business associates regarding compliance with the HIPAA Privacy and Security rules.
13423	**Effective Date**	Unless otherwise noted, effective date is 12 months after date of enactment.
13424	**Reports / Additional Guidance**	• Secretary to submit annual report to Congress regarding enforcement, including number/amount of complaints, audits, subpoenas, and penalties imposed. • Secretary and FTC to submit report to Congress within one year of enactment regarding compliance by non-covered entities. • Secretary to issue additional guidance on "de-identified" information within 12 months of enactment. • GAO to submit report to Congress within one year of enactment about best practices for disclosures among providers for treatment purposes. • GAO to submit report to Congress within 5 years of enactment on impact of Act on health insurance premiums, health care costs, adoption of EHRs by providers, and reduction in medical errors and quality improvements. • Secretary to issue regulations to revise definition of "psychotherapy notes."

Contact: Christy Tinnes

We will provide updates on further developments. In the meantime, if you have any questions, please contact your regular Groom attorney or any of the Health and Welfare Practice Group attorneys listed below:

Jon W. Breyfogle	jwb@groom.com	(202) 861-6641
Jenifer A. Cromwell	jac@groom.com	(202) 861-6329
Thomas F. Fitzgerald	tff@groom.com	(202) 861-6621
Debbie G. Leung	dgl@groom.com	(202) 861-2601
Christine L. Keller	clk@groom.com	(202) 861-9371
Heather E. Meade	hem@groom.com	(202) 861-0179
Christy A. Tinnes	cat@groom.com	(202) 861-6603
Donald G. Willis	dgw@groom.com	(202) 861-6332