TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
New "Defined" Terms	Not Applicable	Breach; Electronic health record (different from electronic PHI); Personal Health Record (different from PHI); Vendor of Personal Health Records; Unsecured PHI		
Electronic Health Record	Not Defined	Electronic Health Record (EHR) means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. Section 13400(5)	2/18/2009	Term used through the ARRA to describe rights and responsibilities pertaining to EHR
Unsecure PHI	Not Defined	PHI (in any medium, i.e., electronic, paper or oral) that is not secured through use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals. If Secretary of HHS does not issue guidance by 4/18/09 (with annual updates), the statute defaults to ANSI standards. Section 13402(h) NOTE: Limited Data Sets and de-identified PHI is not PHI and would not be subject to this provision.	Issued 4/17/09; 74 Fed. Reg. 19006; Applies to breaches 30 days AFTER publication of interim final regs. Interim final reg 8/19/09 . See also: http://www.hhs.gov/ocr/privacy/ (updated guidance document from the regs)	Addresses 4 "states of data:" Data in Motion; Data at Rest; Data in Use; or Data Disposed. Two methods identified to render PHI unusable, unreadable, or indcipherable to unauthorized individuals: (i) Encryption, as specified in the Security Rule and (ii) Destruction of paper or electronic records. Redaction of paper records is INSUFFICIENT unless it results in NO PHI (i.e, de-identified).

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
Breach	Not Defined	Unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI, except: (1): unauthorized disclosures to an unauthorized person who would not reasonably have been able to retain such information; (2) unintentional acquisition, access, use by CE's or BA's employees/agents; and (3) inadvertent disclosures among a CE or BA's employees/agents. Section 13402 Per the regulation, the exceptions will not apply if there is further use or disclosure in violation of the Privacy rule.	45 CFR Part D (issued 8/19/09); expands definition to clarify when privacy or security of PHI is compromised and definition of other terms. The term "unauthorized" is an impermissible use or disclosure of PHI under 45 CFR 164, Part E	Need to define in our HIPAA policies where relevant. First step - Does a use or disclosure (which incldues access and acquisition) violate the Privacy Rule? Second, does the violation compromise the security or privacy of PHI (i.e., pose a significant risk of financial, reputational or other harm to the individual)? If both are "Yes", then there is a Breach.
Unauthorized		45 CFR Part 164, Part D; defined as "impermissable use or disclosure of PHI under 45 CFR 164, Part E		
Willful Neglect (Penalty Provisions)	Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.	No statutory change - may be changed by regulations issued under ARRA	8/18/2010	Impact on imposition of penalties - See below

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
Breach Notification	Covered Entity (CE) must mitigate, to the extent practicable, any harmful effect that is known to the CE of an unauthorized use or disclosure of Protected Health Information (PHI) by the CE or its Business Associates (BA); 45 CFR 164.530(f) Include in Accountings of Disclosures and report to the individual under a Request for Accounting Disclosure. 45 CFR 164.528	CE must provide notice to persons whose unsecured PHI has been accesssed, acquired, or disclosed as a result of a breach discovered by the CE. (BA has same notice requirement to the CE). Section 13402(a) and (b) Regulations added "used" to the list of actions for which notification is required. 45 CFR 164.404(a)(1) In addition to including all breaches in the accountings of disclosures, the CE must provide annual notice to Secretary of HHS of all breaches occuring during that year. Section 13402(e)(3)	Interim final rule issued 8/19/09; 45 CFR 164, Part D	Must develop a form notification along with a process to provide the required notification, including the annual notice to the Secretary of HHS. See new 45 CFR 164.404(a)(1)
Discovery of Breach	Not Applicable	45 CFR 164.404(a)(2) - a breach is treated as discovered as of the first day the breach is known to the CE or should have been known by the CE exercising reasonable diligence. A breach is deemed to be known to a CE if its workforce member/agent (other than the person committing the breach) knew or should have known of the breach.		Liability to TTUHSC if it should of known of a breach, but failed to identify it.

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
Notice of Breach Requirements	Not Applicable	1. Notice must be given without unreasonable delay, but no later than 60 days after discovery. Section 13402(d)		Important to identify when a breach has occurred (ties into the "discovery of breach"
		2. Individual Notice for those with known contact information (address or e-mail). Section 13402(e)	8/19/09; 45 CFR 164.404, effective 30 days from rule publication; enforcement delay for 180 days after	Written form by 1st class mail or electronic, if agreed to by the individual.
		3. Substitute Notice (10 or more individuals with out-of-date contact information) posted on the CE's website or major print or broadcast media (required if more than 500 individuals affected by breach), to include a toll-free phone number where the individual can get more information		Establish separate toll-free number for IPO and ISO. The regulations allow use of a prominent hyperlink from TTUHSC's home web site to access the substitute note.
		4. Notice to Secretary of HHS if the breach involved PHI of 500 or more individuals		
		5. Annual Notice to Secretary of HHS of Breaches. Not clear whether this is mandatory.	45 CFR 164.408	
Notice Content	Not Applicable	45 CFR 404 (c)	8/19/2009	Notice includes types of information, not a listing of the actual PHI compromised; written in plain language; may require translation to satisfy LEP (i.e., Spanish) or ADA.
Business Associates	BA is contractually obligated, through a written BA agreement to comply with certain provisions of the Privacy and Security rules when performing certain functions on behalf of the CE. 45 CFR 164.502(e)	BAs now subject to all provisions of HIPAA Security. Now all provisions of the Privacy rule apply to BAs and must be incorporated into the BA agreement, such as accounting of disclosures and breach notifications. Also subject to same civil penalties as CEs.	2/18/2010	Current and Future BA Agreements. TTUHSC is also a BA in some cases.

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
Requested Restrictions on Disclosures of PHI	Individuals can request that disclosure of PHI be restricted as to use or disclosure, however a CE must affirmatively agree to such restriction otherwise the CE is not required to comply. 45 CFR 164.522(a)	CE must comply with request to restrict disclosure of PHI to a health plan for payment or health care operations IF the PHI pertains to health care items or services which were paid in full out of pocket by the patient or his/her representatives	2/18/2010	Will need functionality within the EHR to segregate this type of PHI when a request is made. Need further clarification on what to do if patient provides that PHI in the history during a future visit.
Minimum Necessary Disclosures	Subject to certain exceptions, a CE must limit uses and disclosures of PHI to the "minimum necessary" to accompliance the purpose of the use or disclosure. 45 CFR 154.502(b)	Secretary of HHS must publish guidance on what constitutes "minimum necessary" for use or disclosure of PHI. Until the guidance is published, CE must, to the extent practicable, limit use, disclosure or request of PHI to the "limited data set" (defined as PHI without the name, address, telephone/fax, e-mail, SSN, MRN and 9 other identifiers) or, if needed, the minimum necessary to accomplish the intended purpose. Section 13405(b)	8/18/2010	This does not impact disclosures for Treatment or pursuant to an Authorization, among other exceptions.
Accounting of Disclosures	CE does not have to account for disclosures of PHI for Payment, Treatment or Healthcare Operations for purposes of the Accounting of Disclosure Requirement. Accountings limited to disclosures outside Payment, Treatment and Healthcare Operations that are not made pursuant to a Written Authorization and the accountings can only go back 6 years. 45 CFR 164.528	CE must account for ALL disclosures of PHI made through EHR by the CE (and BA or provide contact information for BA), including those related to Treatment, Payment and Healthcare Operations. Accountings limited to 3 year time period. Section 13405(c)	Regulations 6/18/10; 1. EHR acquired as of 1/1/09 - compliance is 1/1/14; 2. EHR acquired after 1/1/09, the later of 1/1/11 or date of acquisition.	TTUHSC EMRs, Centricity (and other Billing systems) must be able to provide the required accounting on the respective compliance dates based on recommendations from the HIT Policy Committee established under Section 13101 of the ARRA.

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
Sale of PHI	Absent specific authorization from the individual, a CE cannot directly or indirectly receive remuneration in exchange for that individual's PHI, including marketing activities. 45 CRF 164.508	Prohibits receipt, directly or indirectly, of any payment in exchange for an PHI unless there is a valid authorization. The authorization must include information about whether the PHI can be further exchanged for remuneration by the recipient of the PHI. An authorization is not required for public health activities, research (if the price charged reflects the actual costs of preparation and transmittal of the data), treatment, health care entity mergers, payments for services provided by a BA, releases subject to an individual's authorization, or other activities authorized by regulation. Section 13405	Regulations by 8/18/10, which become effective 6 months after final regulations are published.	None - TTUHSC does not sell PHI without an authorization. Will allow limited exchanges without an authorization, which is not addressed in current regulations.
Patient Access to PHI	Subject to limited exclusions, an individual has a right to access and copy PHI in a designated record set, in the form or format requested by the individual, if it is readily producible in such form or format, or, if not, in a readable hard copy form or as otherwise agreed to. 45 CFR 164.524	If the CE uses or maintains an EHR, the individual has the right to obtain a copy of his/her PHI in electronic from and direct the CE to transmit such copy diretly to an entity or person the individual designates, if such direction is clear, concise and specific. Fee shall not be greater than the labor costs to provide the copy. Section 13405(e) Key item for INTEROPERABILITY OF EHRs.	2/18/2010	TTUHSC EMRs, Centricity and other billing systems must be able to provide the required copy when requested by the individual and securely transmit it to a designated entity or individual.

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
Marketing	Marketing is defined as a communication about a product or service that encourages people to purchase or use the product. It does not include communications for treatment, case management, coordination of care or to direct or recommend alternative treatments or therapies. 45 CFR 145.501 A written authorization is required for marketing EXCEPT where the communication is face-to-face between a CE and individual or a promotional gift of nominal value provided by a CE. 45 CFR 164.508(a)(3)	Marketing now includes communications for treatment, case management, coordination of care or to direct or recommend alternative treatments IF the CE receives or has received direct or indirect payment in exchange for the communication. Section 13406. Communications with direct or indirect payment is not marketing IF it describes a drug or biologic that is currently being prescribed for the recipient of the communication and the payment is reasonable in amount. Communications with direct or indirect payment is not marketing IF the CE makes the communication and has a valid written authorization, or the communication is by a BA and is consistent with the written agreement between the BA and CE.	2/18/2010	Future marketing activities to TTUHSC patients.
Fundraising	A CE must include in all fundraising materials a description of how the individual may opt out of receiving any further fundraising communications, and the CE must make reasonable efforts to honor such request. 45 CFR 164.514(f)	Expands the "opt-out" requirements under the current law to fundraising communications that may have been considered healthcare operations under current law. Must provide a clear and conspicuous opportunity for the recipient to elect not to receive any further fundraising communications. Once an election to opt out is made, no fundraising communications can be made to that individual. Section 13406(b)	2/18/2010	Expands opt-out" to all fundraising using TTUHSC patient data.

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
Criminal Penalties	Imposes criminal penalty of up to $250,000 and up to 10 years in prison against a person (limited to the CE and not its employees or agents) who discloses or obtains PHI with intent to sell, transfer or use for commercial advantage, personal gain or malicious harm. 42 USC 1320d-6	Criminal penalties can now be imposed against a CE's employees or any other individual who obtains or discloses, without authorization, PHI maintained by a CE. Section 13409	2/18/2010	
Civil Penalties	Secretary of HHS may impose a CMP for failure to comply with HIPAA, with a maximum civil fine of $100/violation and to $25,000 for all violations of an identical nature during a calendar year. Civil penalties not imposed if (a) criminal penalties apply; (b) there was not actual or constructive knowledge of the violation; or (c) the violation was due to reasonable cause and not willful neglect and is cured within 30 days. 42 USC 1320-5(a)(1)	Tiered Penalty Provision: 1. Violations where CE did not know of the violation are $100-$50K/occurrence, not to exceed $25K-1.5mil/year for similar violations during that year; 2. Violations due to reasonable cause and not willful neglect are $1,000-50K/violation, not to exceed $100K-1.5mil/annually for similar violations. 3. Violations due to wilful neglect that are cured within 30 days are subject o $10K-50K/violation, up to a max. of $250K-1.5mil/annually for similar violations. 4. Violations due to wilful neglect that are not cured within 30 days are subject to $50K/violation up to a max. of $1.5 mil/year for similar violations. Section 13410(d)	2/18/10 - regulations are due; Penalties apply to violations occurring after 2/18/09; Penalities for willful neglect will be imposed after 2/18/11	Since we are required to annually report to the Secretary each breach of unsecured PHI (HIPAA violation), it is likely that we will then be asked to pay a civil penalty for each breach reported based on the new tiered penalty provisions.
Required Investigations	None currently required.	Secretary of HHS must investigate any complaint where a preliminary investigation indicates the conduct constituted wilful neglect. Section 13410	2/18/2011	

TTUHSC HIPAA Privacy Changes - HITECH Act
August 28, 2009

Provision	HIPAA as of Feb. 2006	ARRA Changes to HIPAA (2/17/09) - Statutory	Regs Due/Effective Date	Impact
State AG Authority	Not Applicable	Attorney General has authority to bring action on behalf of residents in their state to stop violations and/or obtain damages of $100/violation not to exceed $25,000/year for similar violations. State may be able to recover attorneys fees in any civil action to collect damages.	2/18/2009	
Audits	None currently required.	Secretary of HHS must conduct periodic audits of CE and BA. Section 13411	2/18/2010	
Security Safeguard Guidance	Currently the HIPAA security regulations do not mandate use of any particular technical system or safeguards. 45 CFR 164, Subpart C	Each year the Secretary of HHS shall issue guidance on the most effective and appropriate technical safeguards related to security of PHI	2/18/10 and annual thereafter	Guidance may impact EMR and other electronic storage devices. If TTUHSC chooses to not follow the guidance, then must justify their choice of tehcnical systems.