



HITECH Act and GINA Update

What the New HIPAA Rules Mean for Health Plans

Experience Infinisource

Copyright © 2009

www.infinisource.net



Interim Final HITECH Act Rule



www.infinisource.net



Interim Final HITECH Act Rule

- Overview
 - Provides safe harbor for securing protected health information (PHI)
 - Details notification process for breaches of unsecured PHI
- Key Dates
 - Published on August 24, 2009 by Health and Human Services (HHS) Department
 - Office for Civil Rights (OCR) is in charge of enforcement

www.infinisource.net



Interim Final HITECH Act Rule

- Key Dates
 - Breach notification rules take effect on September 23, 2009
 - Comments due to OCR by October 23, 2009
 - Moratorium on sanctions until February 22, 2010

www.infinisource.net



Interim Final HITECH Act Rule

- Review of familiar key terms
 - Business Associate
 - Covered Entity
 - Privacy Rule
 - Security Rule
 - PHI

www.infinisource.net



Interim Final HITECH Act Rule

- Review of unfamiliar key terms
 - Unsecured PHI
 - Not encrypted
 - Not destroyed
 - Redaction and PHI security
 - Less secure means are acceptable for complying with HIPAA Security Rule

www.infinisource.net



Interim Final HITECH Act Rule

- Review of unfamiliar key terms
 - Breach of unsecured PHI
 - “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information”*

www.infinisource.net



Interim Final HITECH Act Rule

- Review of unfamiliar key terms
 - Exceptions to breaches of unsecured PHI
 - Unintentional acquisition, access or use by workforce member or authorized individual
 - Inadvertent disclosure to authorized individual
 - Good faith belief that unauthorized person would not reasonably retain PHI



www.infinisource.net




Interim Final HITECH Act Rule

- Review of unfamiliar key terms
 - Unauthorized
 - “impermissible use or disclosure of PHI”*
 - Compromise
 - “poses a significant risk of financial, reputational, or other harm to the individual”*


www.infinisource.net


Breach Notification Map

www.infinisource.net


Breach Notification Map

- Step One:
 - Analyze whether use or disclosure involved PHI
- Step Two:
 - Determine if an actual breach occurred or if an exception exists

www.infinisource.net


Breach Notification Map

- Step Three:
 - Who discovered the breach?
 - If Covered Entity, go to Step Five
 - If Business Associate, go to Step Four
- Step Four:
 - Notify Covered Entity
 - Without unreasonable delay
 - No later than 60 days after breach is or should have been discovered

www.infinisource.net



Breach Notification Map

- Step Four:
 - Content of Business Associate Notice to Covered Entity
 - Identity of all affected individuals
 - Any other information needed by Covered Entity to meet its notice requirements
 - Prompt notification required when new information becomes available

www.infinisource.net



Breach Notification Map

- Step Five:
 - Notify the affected individuals in writing
 - Content of Covered Entity Notice to Individuals
 - Brief description of what happened
 - Date of breach
 - Date of discovery
 - Description of types of unsecured PHI involved

www.infinisource.net



Breach Notification Map

- Step Five:
 - Content of Covered Entity Notice to Individuals
 - Steps individuals should take to protect themselves
 - Brief description of Covered Entity's steps
 - Investigation of breach
 - Mitigation of harm
 - Protection against future breaches

www.infinisource.net



Breach Notification Map

- Step Five:
 - Content of Covered Entity Notice to Individuals
 - Contact information, i.e., one or more of the following:
 - Toll-free number
 - Email address
 - Website
 - Postal address

www.infinisource.net



Breach Notification Map

- Step Six:
 - Sort out miscellaneous notice issues
 - Dead individuals
 - Next of kin
 - Personal representative

www.infinisource.net



Breach Notification Map

- Step Six:
 - Sort out individual notice issues
 - Insufficient contact information
 - Fewer than 10: phone, other means
 - 10 or more: toll-free number and...
 - » Conspicuous posting on home page for 90 days, or
 - » Conspicuous notice in major print or broadcast media where individuals might reside

www.infinisource.net



Breach Notification Map

- Step Seven:
 - Establish how to contact HHS
 - 500 or more
 - No later than 60 days after discovery
 - Less than 500
 - Record in breach log
 - Provide log within 60 days after end of calendar year

www.infinisource.net



Breach Notification Map

- Step Eight:
 - Determine if media notification is required
 - 500 residents of state or jurisdiction (e.g., county, city or town)
 - Based on breach count for Covered Entity, not Business Associate
 - No later than 60 days after discovery

www.infinisource.net



Breach Notification Map

- Related notification issues
 - Notices must use plain language
 - Law enforcement can delay notifications
 - Burden of proof is on Covered Entity and Business Associate

www.infinisource.net

Breach Notification Map

- Related notification issues
 - Covered Entity requirements
 - Training
 - Complaint process
 - Sanctions policy
 - No intimidation, retaliation or waivers
 - Documentation
 - Business Associate requirements will be the same on February 17, 2010

Final FTC Rule on Privacy



Final FTC Rule on Privacy

- Overview
 - Called the “Health Breach Notification Rule”
 - Governs security breaches of individually identifiable health information for non-HIPAA entities
 - Personal health record vendors
 - Entities offering applications for personal health records



Final FTC Rule on Privacy

- Key Dates
 - Published on August 25, 2009 by FTC
 - FTC is in charge of enforcement
 - Breach notification rules take effect on September 24, 2009
 - Moratorium on sanctions until February 22, 2010

www.infinisource.net



Final FTC Rule on Privacy

- Major provisions
 - Generally mirrors HITECH Act HIPAA Rule
 - Written notification without unreasonable delay (no later than 60 days) after discovery
 - Notification to prominent media outlets if 500 or more affected in state or jurisdiction
 - FTC notification
 - 500 or more
 - » No later than 10 business days after discovery
 - Less than 500
 - » Record in breach log
 - » Provide log within 60 days after end of calendar year

www.infinisource.net



Other HITECH Act Rules



www.infinisource.net



Other HITECH Act Rules

- Changes already in effect
 - New penalty scheme
 - Tier A (unknown violations): \$100 each, up to \$25,000 per year
 - Tier B (reasonable cause violations): \$1,000 each, up to \$100,000 per year
 - Tier C (willful neglect, corrected): \$10,000 each, up to \$250,000 per year
 - Tier D (willful neglect, uncorrected): \$50,000 each, up to \$1,500,000 per year
 - 30-day correction period for Tiers A and B

www.infinisource.net



Other HITECH Act Rules

- Changes already in effect
 - State Attorneys General can sue

www.infinisource.net



Other HITECH Act Rules

- Changes effective February 17, 2010
 - Business Associates are subject to Covered Entity requirements
 - Privacy
 - Security
 - HITECH Act
 - Minimum Necessary rules
 - Requests for disclosure/access restrictions

www.infinisource.net



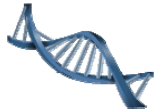
Other HITECH Act Rules

- Changes effective February 17, 2010
 - PHI marketing restrictions
 - Prohibition on sale of PHI
 - Plan for periodic HIPAA audits
- Changes effective in 2012-2016
 - Accounting of E-Health Record disclosures
 - Allocation of penalty money to individuals

www.infinisource.net



GINA Update



www.infinisource.net



GINA Update

- Two parts of GINA
 - Title I: Health insurance (health plans, carriers)
 - Enforced by HHS, Treasury and Department of Labor
 - Title II: Employment (employers)
 - Enforced by Equal Opportunity Employment Commission (EEOC)
- Overall effective date: November 21, 2009

www.infinisource.net



GINA Update

- Regulations Update
 - Title I: Health insurance
 - Regulations were due on May 21, 2009 (not yet published)
 - Title II: Employment
 - Proposed Regulations published on March 2, 2009
 - Final Regulations were due on May 21, 2009 (not yet published)

www.infinisource.net



GINA Update

- Key terms
 - Genetic information
 - Genetic tests
 - Genetic services
 - Family medical history
 - Family: up to fourth-degree relatives

www.infinisource.net



GINA Update

- Major provisions
 - Title I (health insurance) prohibitions
 - No adjusting group premium or contribution amounts
 - No requesting or requiring genetic testing
 - No requesting, requiring, or purchasing genetic information for underwriting purposes
 - No preexisting condition exclusions, absent diagnosis of condition

www.infinisource.net

GINA Update

- Major provisions
 - Title II (employment) prohibitions
 - No discrimination in all areas of employment
 - No requests, requiring, purchases with exceptions
 - FMLA
 - Wellness programs
 - No breach of confidentiality

Action Plan



Action Plan

- For HITECH Act compliance...
 - Create breach notification procedures and documents
 - Maintain and report breach log
 - Revisit Business Associate Agreements
 - Train workforce members
 - Update Privacy and Security procedures
 - Review Security risk assessment and risk analysis

Action Plan

- For GINA compliance...
 - Examine PCE clauses
 - Review underwriting procedures

Additional Resources



Additional Resources

- HHS Final Interim Rule
 - <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>
- HHS news release
 - www.hhs.gov/news/press/2009pres/08/20090819f.html



Additional Resources

- FTC Rule
 - www.ftc.gov/os/2009/08/R911002hbn.pdf
- FTC news release
 - www.ftc.gov/opa/2009/08/hbn.shtm
- FTC breach notification form
 - www.ftc.gov/os/2009/08/R911002hbnform.pdf

www.infinisource.net



Additional Resources

- News & Review article, major guidance, seminars and webinars
 - www.infinisource.net

www.infinisource.net



Final Thoughts



www.infinisource.net



Final Thoughts

- HITECH Act rules up the ante on HIPAA compliance
- Mere correction is no longer sufficient
- Notification requirements are detailed and specific
- Penalty/publicity scheme make HIPAA compliance more important than ever

www.infinisource.net
