

HIPAA PCI Compliance

2010 HEALTHCARE BIZTECH FORUM
Thursday, May 20, 2010

HIPAA Impact
Presenter: Grant Peterson, J.D. – HIPAA Privacy & Security Consultant

1

Speaker

About the Speaker –

Grant is a HIPAA privacy and security consultant specializing in the American Recovery and Reinvestment Act's (ARRA) HITECH ACT, HIPAA privacy and security audits and implementations, strategic compliance planning, and HIPAA training and awareness programs.

Grant holds a B.S. degree in Public Administration from Minnesota State University, and a Juris Doctor (J.D.) law degree from Hamline University School of Law

Grant Peterson, J.D.
HIPAA Privacy & Security Consultant
DGPeterson, LLC

Questions and comments about the presentation: grant@dgpetererson.com

2

HIPAA PCI Compliance

Welcome

- Program Notes
- HIPAA, HITECH
- PCI Harmony with HIPAA
- Red Flags Rule
- Q & A

3

HIPAA PCI Compliance

HIPAA History and Timeline

HIPAA Privacy Rule	April 2003
HIPAA Security Rule	April 2005
HIPSA (Senate Bill)	July 2007
HITECH Act	February 2009

4

HIPAA PCI Compliance

HIPAA Privacy: Framework for Handling PHI

Uses and Disclosures Restrictions	
General	§ 164.502 (a)
Minimum Necessary	§ 164.502 (b)
Verification	§ 164.514 (h)
De-identified	§ 164.514
Permitted – Agree or Object	§ 164.510
Permitted – Obtaining Consent Voluntary	§ 164.506
Permitted – Authorization Required	§ 164.508
Permitted –Social Responsibility disclosures	§ 164.512
Marketing or Fundraising	§ 164.512 (e) (1)
Required Disclosures	§ 164.502 (a) (2)

5

HIPAA PCI Compliance

HIPAA Privacy – Framework for Patient Rights

Individual Rights	
Individual Rights to request restrictions/ Right to alternative means of communication	§ 164.522
Right to Notice of Privacy Practices	§ 164.520
Right to Access or Copy	§ 164.524
Right to Amend	§ 164.526
Right to an Accounting of disclosures	§ 164.528
Waiver of rights not allowed	§ 164.530 (h)
Right to request restrictions regarding disclosures	§ 164.502 (c) § 164.522 (a)

6

HIPAA PCI Compliance

HIPAA Privacy – Framework for Administration of HIPAA

Administrative Requirements		
General Privacy Standard		§ 162.530 (l) (1)
Documentation: Policies and Procedures; and Document retention of HIPAA forms		§ 164.530 (l)
Designate Privacy Official		§ 164.530 (a);
Train workforce		§ 164.530 (b)
Workforce sanctions for non-compliance		§ 164.530 (e)
Business Associates		§ 164.502 (e); § 164.504 (e)
Safeguards, Security and Destruction		§ 164.530(c);
Remedies and Penalties		
Complaints – Internal		§ 164.530 (d)
Complaints – Other		§ 160.306
Enforcement and Sanctions		HIPAA (the law) 42 USC 1320 (d)

7

HIPAA Impact

HIPAA Security – Framework for Administrative Safeguards of HIPAA

Standards	Sections	Implementation Specifications (R) – Required, (A) – Addressable
Administrative Safeguards		
Security Management process	164.308(b)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R)
Assigned Security Responsibility	164.308(b)(2)	(R)
Workforce Security	164.308(b)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(b)(4)	Isolation Health care Clearinghouse Function (R) Access Authorization (A)
Security Awareness and Training	164.308(b)(7)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(b)(6)	Response and Reporting (R)
Contingency Plan	164.308(b)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(b)(8)	(R)
Business Associate Contracts	164.308(b)(1)	Written Contract or Other Arrangements (R)

8

HIPAA Impact

HIPAA Security – Framework for Physical Safeguards of HIPAA

Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

9

HIPAA Impact

HIPAA Security – Framework for Technical Safeguards of HIPAA

Technical Safeguards		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

10

HIPAA PCI Compliance

HITECH Act Amendments – Framework Adjustments to HIPAA

HITECH Act	
13401	Application of Security Provisions and Penalties to Business Associates + HHS Annual Guidance
13402	Notification in the Case of Breach
13403	Education on Health Information Privacy
13404	Application of Privacy Provisions to Business Associates of Covered Entities
13405	Restrictions on Certain Disclosures and Sales of Health Information, Accounting of Certain PHI Disclosures, Access of Certain Information in Electronic Format

11

HIPAA PCI Compliance

HITECH Act Amendments – Framework Adjustments to HIPAA

HITECH Act	
13406	Conditions on Certain Contracts as Part of Health Care Operations
13407	Temporary Breach Notification for Vendors of PHR and other Non-HIPAA Covered Entities
13408	Business Associate Contracts Required for Certain Entities
13409	Clarification of Application of Wrongful Disclosures Criminal Penalties
13410	Improved Enforcement
13411	Audits

12

HIPAA PCI Compliance

PCI Framework in Harmony with HIPAA

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data

MANUFACTURERS: PCI PTS (PIN Transaction Security)
SOFTWARE DEVELOPERS: PCI PA-DSS (Payment Application Security)
MERCHANTS & PROCESSORS: PCI DSS (Data Security Standard)
PCI SECURITY STANDARDS & COMPLIANCE

Ecosystem of payment devices, applications, infrastructure and users

13

HIPAA PCI Compliance

PCI Framework in Harmony with HIPAA

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

14

HIPAA PCI Compliance

Red Flags Rule: Protecting PHI Outside HIPAA

- The Identity Theft Red Flags Rule was promulgated under the Fair and Accurate Credit Transactions Act, in which Congress directed the Commission and other agencies to develop regulations requiring "creditors" and "financial institutions" to address the risk of identity theft.
- Health care providers who periodically allow patients to pay for medical services over time through a series of payments should have written policies that identify the "red flags" or indicators of possible identity theft they may come across in the course of business, establish procedures to detect those red flags and to respond appropriately to mitigate and prevent harm, and develop procedures for training staff and keeping applicable policies current. Health care providers should also have procedures in place to ensure that their vendors are in compliance with the Red Flag Rules and amend existing business associate agreements or asking for copies of the vendors' Red Flag policies.
- The Federal Trade Commission is delaying enforcement of the "Red Flags" Rule until June 1, 2010, for financial institutions and creditors subject to enforcement by the FTC

15

Question & Answer

For additional questions or comments on this presentation: grant@DGPeterson.com

16

Notice

This presentation should not be considered as, or as a substitute for, legal advice and is not intended to nor does it create an attorney-client relationship. Because the presentation is general, the materials may not apply to your individual legal or factual circumstances. You should not take (or refrain from taking) any action based on the information you obtain from this presentation without first obtaining professional counsel.

17
