Greenway Marketplace

Hear from GSG Compliance & White Plume

November 14, 2013
To enhance the Greenway customer user experience by offering innovative, forward-thinking technologies to assist in providing the most advanced healthcare possible.
Where are we today

- **82** signed partners
- **55** solutions listed
- **60+** partners in pipeline
<table>
<thead>
<tr>
<th>Category</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Engagement</td>
<td>17</td>
</tr>
<tr>
<td>Care Coordination</td>
<td>12</td>
</tr>
<tr>
<td>Document Management</td>
<td>9</td>
</tr>
</tbody>
</table>
GSG Compliance has not only helped practices but also some of the largest and most prestigious health systems in the country. They're often brought in by the largest law firms in the country to help their clients through OCR investigations.

For the private practice, they offer the ability to accurately address HIPAA compliance in a cost-effective, simplistic and thorough manner.
HIPAA Security Compliance for Physician Practices

Presented by
Bill Steuer and Todd Greenberg
Who is GSG Compliance?

GSG Compliance partners with firms that have the credentials, long history in healthcare, and have not only helped practices but also they consult with some of the largest and most prestigious health systems in the country. They're often brought in by the largest law firms in the country to help their clients through OCR investigations. For the private practice, we offer you the ability to accurately address HIPAA Compliance in a cost effective, simplistic, but thorough manner.

The Delivery: MEDITOLOGY

• An average of 15+ years of combined “Big 4” healthcare IT security and compliance leadership experience
• Team has directly relevant operational experience (health system CISO and IT Operations leaders)
• Published authors and sought after conference speakers on healthcare security and privacy
• Certifications include: CISSP, HITRUST (CCSFP), PMP, CCNA, CPHIMS, CISA, and CNSS
• Dozens of clients ranging in size and complexity from community hospitals & 2000+ bed multi-facility academic medical centers, to the small private practice.
• Leaders in development of HITRUST, ANSI and HIMSS standards
BREACH FINDINGS
Healthcare Breach Data

What is a Breach? The acquisition, access, use or disclosure of PHI that violates HIPAA and compromises the privacy or security of that information.

- The Breach Notification Rule made reporting breaches a requirement in September 2009
- The average cost is $194 per record breached (Ponemon Institute)
- Since July 2011, Physician Practices have become the most breached organization type and 2nd most breached overall from 2009-2013 (HITRUST Alliance. A Look Back: U.S. Healthcare Data Breach Trends)

Most Breached from 2009-2013
- Hospital/Health Systems (32%)
- Physician Practices (28%)
Behind the Numbers

Top Breach Types
- Theft: 54%
- Loss: 12%
- Unauthorized access: 11%
- Incorrect mailing: 6%
- Improper disposal: 5%
- Hacking: 6%

Breach Locations
The chart to the right portrays where breaches have occurred.

NOTE: The percentages were taken from HITRUST’s “A Look Back: U.S. Healthcare Data Breach Trends” and the HHS breach notification report.
Physician Practice Data

Biggest Losses
- Stolen devices (laptops)
- Business associates (third parties)
  - Healthcare industry overall according to a recent HITRUST report
    1
    - Total breaches implicating a BA: 21%
    - Total records breached implicating a BA: 58%
  - 30% of Physician Practice breaches involved a BA

Smaller Practices are Targets
- The largest source of breaches occur in small Physician Practices
  - 1-10 physician-sized practice
    - Accounted for 39% of breaches coming from Physician Practices

In the Headlines
- The 2nd largest breach to date is from a physician group practice
  - Over 4 million patient records breached due to theft of 4 computers (Advocate Medical Group)

REGULATORY IMPACT:
WHAT’S NEW WITH HIPAA OMNIBUS
Overview: Omnibus Rule Impact

The HIPAA Omnibus Rule was EFFECTIVE March 23, 2013 and is now ENFORCEABLE beginning September 23, 2013 (last Monday)

Updates made by the HIPAA Omnibus Rule can be broken down into 3 areas that impact physician practices. In summary:

1. Modifications to prior HIPAA privacy and security regulations, including:
   a. Business Associates and Sub-contractors
   b. Notice of Privacy Practices
   c. Individual Rights
   d. Use and Disclosure

2. Clarification on breach notification and reportable breaches

3. Increased and tiered penalties
Omnibus Rule Impacts

**Business Associates & Sub-contractors**

- Business Associates (BA) are now regulated by HIPAA and must comply with:
  - The HIPAA Security Rule
  - Breach Notification Rules
  - Privacy Rule’s Use and Disclosure provisions
- BAs are liable for compliance and violations
- Physicians are liable for the actions of their BAs who are agents (acting on their behalf)
Example BA Organizations

Who You Need to Sign an Updated BA Agreement

• IT Service Providers
  o Tech support, EHR partner, Personal Health Record (PHR) vendors

• Claims Processing, Billing, Shredding, Copier and Lab companies

• Data Hosting Services
  o Google services (email), DropBox, Box, Amazon data hosting

• Health Information Organizations
  o E-prescribing gateways or health information exchanges that transmit or maintain PHI

• Attorneys, consultants

Not…

• Payers, hospitals, other physicians or employees
• Conduits such as couriers (FedEx, UPS, etc.)
Omnibus Rule Impacts

Notice of Privacy Practices
- Requires updates and modification
  - Post & start using new version now (no requirement to redistribute to all patients)
  - View updates at: http://www.healthit.gov/providers-professionals/model-notices-privacy-practices

Individual Rights
- Right to request and receive electronic copies of their health information
  - Request must be granted or denied within 30 days
- Right to restrict disclosures to health plans for services paid for out-of-pocket

PHI Uses and Disclosures
- Limitations on using PHI for marketing and fundraising
- Prohibits the sale of PHI without individual authorization
- Emailing PHI unencrypted
Omnibus Rule Impacts

**Penalties**
Violations of an identical compliance requirement occurring in the same calendar year can cost an organization up to $1.5M

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>Repeat Violations/ Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 – $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 – $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful Neglect—<strong>Corrected</strong></td>
<td>$10,000 – $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>(within 30 days)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willful Neglect—<strong>Not corrected</strong></td>
<td>At least $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>(within 30 days)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WHAT ARE THE REGULATORS LOOKING FOR?

What you need to know about OCR investigations and audits
OCR Audits

2 Types of OCR Audits

1. Proactive or “Mock” Audit

2. OCR Investigation
Top Security Issues

OCR Audit Results: Audit Issues by Area

Below are the top HIPAA Security issues identified during OCR’s mock audits.

1. User Activity Monitoring
2. Contingency Planning
3. Authentication / Integrity
4. Media Reuse and Destruction
5. Conduct Risk Assessment
6. Grant, modify user access
7. Incident Response
8. Encryption
9. Physical Access Controls
OCR Investigation

Lessons Learned

• Documentation
  o Document everything—evidence

• Better late than never

• Willful neglect
  o “The Addressable HIPAA requirements are unreasonable to ask of a physician practice”
  o Do not be in denial, “willful neglect” will catch up to you
PHYSICIAN PRACTICE SECURITY

Mitigating security and compliance risks
What We See at Our Clients

Smaller Physician Practice Advantages

• Low exposure to internet risks (less network complexity)
• Lower opportunity for insider threats (intentional/ malicious)
• Hosted IT environments

Physician Practice Challenges

• Resource Availability
  o Limited budget for expensive technologies
  o No dedicated security role and not enough head count to cover security responsibilities

• Lack of Awareness
  o Little understanding of the financial implications of a breach
    - Up front new technology costs
Cover Your Bases

Executive Support
• Alert upper management of increased compliance requirements and possibility of an audit.

Two D’s of HIPAA Compliance
Demonstrate you’ve Taken the Necessary Steps
• Identify your risks, create a remediation plan/ CAP and begin corrective actions now.

Documentation
• Ensure that documentation is accessible and organized.
  o Auditor perspective—if it’s not documented, it didn’t occur.
# Security Compliance Checklist

## Administrative and Physical Safeguards

- **Risk Analysis:** Comprehensive security risk assessment
- **Risk Management:** Risk assessment corrective action plan (CAP)
- **Policies:** Up-to-date policies and procedures
- **Responsibility:** Delegate a role responsible for security oversight
- **Training:** All staff members have been provided training and awareness within the last year
- **Media Destruction:** Adequate number of shredders or shred bins; employee awareness on secure paper disposal; re-use of electronic media
- **Business Associates** (BA) have signed an updated BA contract
- **Access Control and Monitoring:** Minimum necessary access rights; periodic monitoring of access (3-6 months)
# Security Compliance Checklist

## Technical Safeguards

- **Encryption**: Encrypt laptops, back-up media and flash drives with ePHI
- **Email Encryption**: Encrypt all email messages that contain PHI (e.g., 3rd party solution)
- **Anti-Virus**: Install on all workstations
- **Vulnerability Management (technical scanning)**: Conduct a vulnerability scan on a periodic basis to identify security gaps in technologies (minimum every 6 months to 1 year)
- **Mobile Device Management**: Centrally manage, encrypt and wipe data on mobile devices
- **Monitoring**: Set up EHR alerts for user activity (e.g., suspicious activity)
Questions?

Bill Steuer
GSG Compliance, LLC
bsteuer@gsgcompliance.com

Todd Greenberg
GSG Compliance, LLC
tgreenberg@gsgcompliance.com

Thank You for Your Time and Attention
Matthew Menendez has worked with White Plume for 10 years and currently serves as the Vice President of Sales and Marketing.

Matthew and his wife Emily both graduated from Vanderbilt University and now live in Birmingham, AL with their 3 children.

Matthew Menendez
Vice President of Sales and Marketing
White Plume
White Plume Background

• Founded in 1999
• Privately Held
• 6,000 Physician Clients
White Plume Areas of Focus

- Protect Physician Productivity in ICD-10
- Protects Revenue Cycle Efficiency in ICD-10
- Closed Loop Denial Prevention

- White Plume can best help practices with:
  - Paper Superbills
  - High Encounter Volumes
  - Complicated Coding Requirements
AccelaPASS™
For charges passed from Progress Note

AccelaSMART™ HL7

GREENWAY

ePASS™ Electronic Practice Acceleration Solution Suite
White Plume Workflow with PrimeSUITE

– Physician Saves and Signs the Progress Note in PrimeSuite.
  – Superbill Status changes to Superbill Ready

– Checkout/billing employee clicks on Superbill Summary.
– Checkout/billing employee clicks on Charge Edits button.
  • Custom Edits:
    – DX, CPT and Insurance
– Checkout/billing employee reviews results and corrections are made.
– Checkout/billing employee clicks Post and charges are posted in PrimeSuite.

– Checkout/billing employee assembles a batch in AccelaSMART.
– Checkout/billing employee clicks on Validate button.
  • Custom Edits:
    – DX, CPT and Insurance
    – Modifiers, units, locations, providers, etc
– Checkout/billing employee reviews results and corrections are made.
– Checkout/billing employee clicks Complete and charges are posted in PrimeSuite.
Adjudicating Claims in ICD-10

- CPT codes must have an appropriate dx for reimbursement
- Cat and Mouse game with insurance companies
- Non-uniformity across payers
- ICD-10 is massive one day earthquake that will disrupt this equilibrium
- Aftershocks of changes to reimbursement for 3, 6, 12 months of rapid change
- The volume of changes will be significant.
  - What, who, how will you manage?
  - What happens if you don’t?
Closed Loop Denial Prevention

Denied Claim / New Policy

Closed Loop Denial Prevention

New Rule Built

Rule fires for all employees every time
White Plume Areas of Focus

• Protect Physician Productivity in ICD-10
• Protects Revenue Cycle Efficiency in ICD-10
• Closed Loop Denial Prevention

• White Plume can best help practices with:
  – Paper Superbills
  – High Encounter Volumes
  – Complicated Coding Requirements
AccelaPASS™
For charges passed from Progress Note

AccelaSMART™ HL7

AccelaCAPTURE™
An electronic superbill
White Plume Areas of Focus

- Protect Physician Productivity in ICD-10
- Protects Revenue Cycle Efficiency in ICD-10
- Closed Loop Denial Prevention

- White Plume can best help practices with:
  - Paper Superbills
  - High Encounter Volumes
  - Complicated Coding Requirements
Questions?

• Learn more about available solutions by requesting more information from the partner on the Greenway Marketplace site: http://marketplace.greenwaymedical.com/

• Submit potential partners, solutions and development ideas that would benefit Greenway customers: http://marketplace.greenwaymedical.com/inex_vendorform
Thank you

http://marketplace.greenwaymedical.com

GREENWAY
Smarter solutions for smarter healthcare®