

“Mecklenburg mental health director resigns in wake of scandal”

***“Providence Health Pays
\$100,000 for HIPAA
Violations”***

***“Alabama man gets six years
for HIPAA violations”***

***“HHS Imposes \$4.3M
Penalty Against Cignet for
HIPAA Violations”***

***“Behavioral counseling
company owner sentenced
to prison for fraud scheme”***

***“Former non-profit owner to
serve 12 years for fraud scheme”***

***“Gentiva to pay \$12.5M
to settle Medicare fraud
claims”***

***“Patient recruiter convicted
of defrauding Medicare over
hurricane-damaged
wheelchairs”***

***“Merck affiliate to pay
\$44M to settle false
claims charges”***

*“Staff members at UMC
Tucson fired for
inappropriately accessing
medical records”*

“MGH pays \$1M and enters into a CAP to settle potential HIPAA violations”

Don't Be A Headline!

Program Integrity Tools and Resources for Providers

Quarterly Webinar Event

June 17th, 2011

Presented by:

Susan Mitchell

Compliance Director

ValueOptions[®] of Tennessee



Welcome!

So Why Are We Here?

- Compliance is largely about managing risks in a heavily-regulated environment.
- Two of the biggest risks in health care compliance are:
 - 1) Privacy
 - 2) Fraud

First, A Little History: Privacy

- Before 2003: Part 2 (substance and alcohol abuse information) and a scattering of state laws
- 2003: HIPAA Privacy Rule, followed closely by the HIPAA Security Rule. Lots of excitement, activity, and even changes at the state level.
- Through early 2009: Attention to privacy seen to wane a bit. Little enforcement activity, competing issues within health care organizations.

First, A Little History, continued...

- 2009: The HITECH Act places more emphasis on enforcement, and the affiliated regulations begin changing some of the long-standing HIPAA Privacy and Security provisions
 - For example, breach notification, business associate responsibilities, enforcement by state attorneys general, minimum necessary.
 - Many final provisions have not been released yet.

What Have We Seen So Far?

- Mass. Gen. Hosp. - \$1 million settlement after employee left patient records on subway
- CIGNET Health - \$4.3 millions for not providing patients access to their records (and not cooperating with the investigation)
- HealthNet: \$375K for loss of a disk drive AND a \$55K state fine for delaying notifications.
- Employees fired at several hospitals for “snooping”

What Do We See Going Forward?

- Continued modifications to the rules
- Transition from paper to electronic records
- Increase in “non-traditional” risks (e.g., hacking, electronic identity theft, large-scale breaches due to the storage capacities of small devices)
- More enforcement by the states, in addition to the feds

Ensuring Compliance when Sharing Information Electronically

How Secure is your Email?

What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. It has been shown that 87% of the population in the United States is likely to be uniquely identified by only gender, date of birth and ZIP code.

[Latanya Sweeney, Ph.D. Standards of Privacy of Individually Identifiable Health Information.](#) April 2002.

What is Protected Health Information (PHI)?

Under HIPAA, PHI is confidential, personal, identifiable health information about individuals that is created or received by a health plan, provider, or health care clearinghouse and is transmitted or maintained in any form. "Identifiable" means that a person reading this information could reasonably use it to identify an individual.

Below are some (but not all) of the elements that make a piece of health-related information PHI:

- name
- address
- e-mail address
- birth date (except year)
- Social Security number
- employee number
- federal and state tax information
- financials
- criminal/court related information
- claim number
- health plan beneficiary number

PHI includes written documents, electronic files, and verbal information. Even information from an informal conversation can be considered PHI. Examples of PHI include completed health care claim forms, detailed claim reports, explanations of benefits (EOBs), and notes documenting discussions with plan participants

What is encryption?

Under the HIPAA Security Rule, encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. In other words, algorithmic schemes encode plain text into a non-readable form or cyphertext, providing privacy. The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form.

Why is encryption important?

As concerns mount over data breaches, state governments and regulatory bodies are taking action. In October 2008, Nevada passed a law requiring all businesses, no matter their size or nature, to secure confidential customer information if it's transmitted electronically. In Massachusetts, effective January 1, 2010, companies are required to encrypt all personal information of state residents transmitted electronically or wirelessly. The safeguarding of private data, especially in regard to the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), has become a major concern.

Under section 13402(h) of the new HITECH privacy act “unsecured protected health information” is defined as “protected health information that is not secured through the use of a technology or methodology specified by the Secretary of Health and Human Services”. Covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in the event of a breach of such information—that is, the information is not considered “unsecured” in such cases. The Secretary has listed and described encryption and destruction as the two technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

Unless Secured, Email Can Be Intercepted and Read During Transit and Still Reach the Intended Recipient

...among the more common analogies used to describe an email sent across the internet is that it is like a message on a postcard that anyone can read along the way. The internet is an open worldwide network that relies on many intermediary computers and networks to direct traffic. Messages or files sent in plain text can be intercepted, read, copied and sometimes modified at these intermediary junctions by using traffic monitors or packet sniffers that look for keywords and other content of particular interest.

- Osterman Research, Inc. The Critical Need for Encrypted Email and File Transfer Solutions. July 2009.

Faxes sent across the internet are not secure, either, unless the fax setup includes some form of fax encryption technology. For example, if the fax is sent to an email address such as 7033905555@Joesfaxserver.com, then between ValueOptions® and Joesfaxserver, the email is going over the internet. If the fax is sent via a standard telephone line connected to a fax machine or fax server then the transmission is an analog transmission sent over land lines and does not need any type of encryption. If you are unsure about whether or not an email fax setup includes encryption, contact your information technology department.

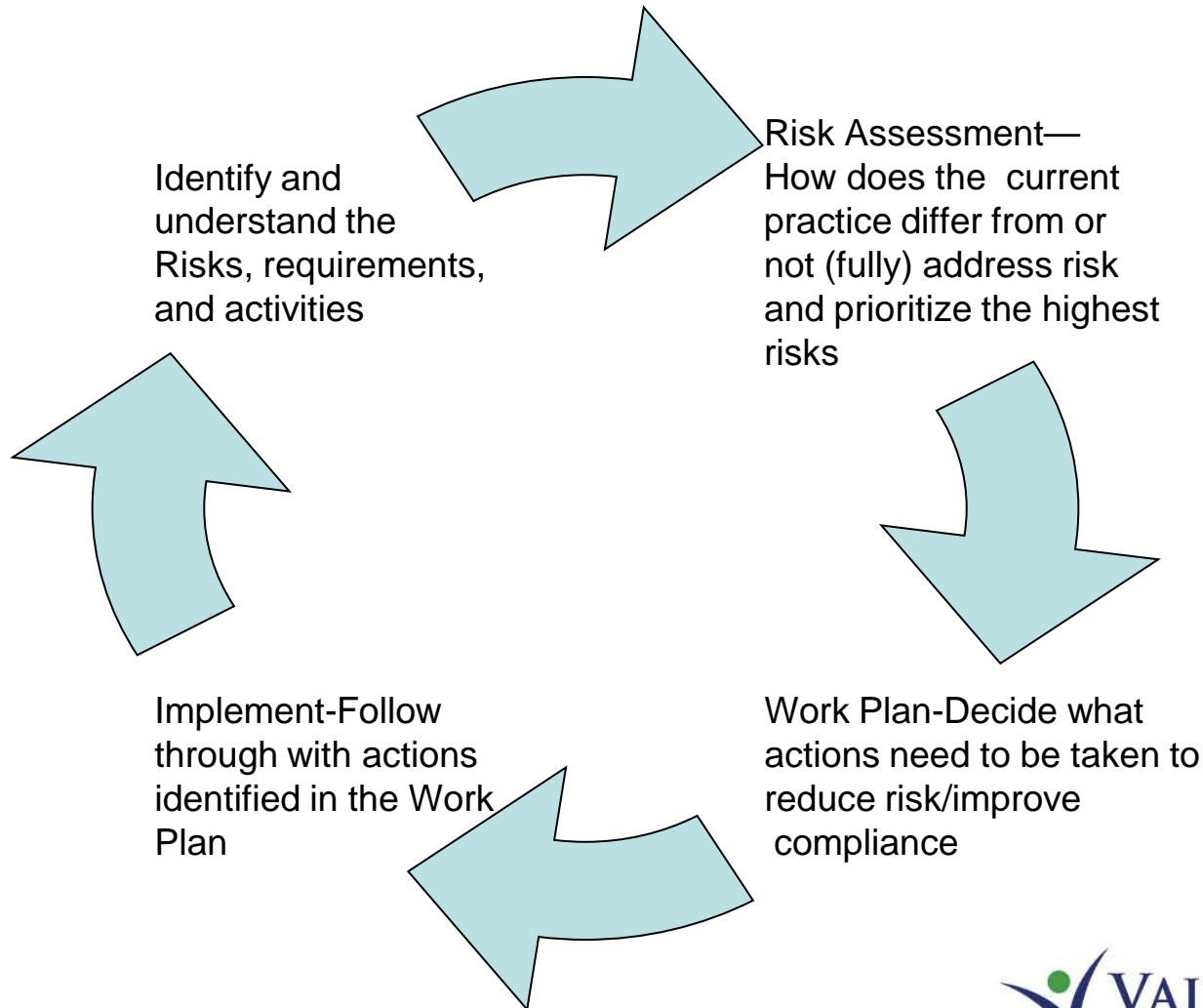
Scenarios

HIPAA Compliant?

- Provider sends an email to the ValueOptions[®] provider representative which contains PHI or PII.
- Provider responds directly to an encrypted email from ValueOptions[®].
- Provider sends an email with a spreadsheet which contains PHI/PII and sends the password in a separate email.
- Provider uses a free encryption program to send an email which contains PHI/PII.

Implementing an Effective Compliance Program: Conducting a Risk Assessment

Implementing an Effective Compliance Program



Two Keys of Risk Assessments:

- Risk assessments should be on-going
- Results of risk assessments should influence the design & implementation of the compliance program in order to be effective

3 Steps to Conducting a Risk Assessment

- Identify the Risks
 - Don't Over-Complicate the Process
 - Don't get ahead of yourself: focus on identifying risks, not current performance
- Assess the Current Activities
- Evaluate/Prioritize the Risks

Step 1: Identifying Risk-Definitions

Formal Definition: Risk is “any event that can adversely affect the achievement of your objectives.”

Detailed Definition: Risk is “the potential for loss or harm – or the diminished opportunity for gain – that can adversely affect the achievement of an organization’s objectives.”

Simple Definition: Risk is “the possibility of something bad happening or something good not happening.”

Step 1: Identify the Risks (cont.)

- Compliance Requirements
 - Culture & Responsibility of Entity Leadership
 - Is compliance a priority of management?
 - Are employees aware of your compliance program & their responsibility for compliance?
 - Does your compliance lead have a high level of authority within the service center and access to senior management?
 - Does the compliance lead report to the CEO?
 - How often does the compliance lead report to the CEO on implementation & effectiveness of compliance efforts?

Step 1: Identify the Risks (cont.)

- Effective Communication of Standards & Training
 - Has training been offered on the compliance program annually?
 - Is there documentation to show that every employee has been trained?
 - Has job-specific compliance training been provided?
 - Has your training been effective?
- Monitoring, Auditing & Evaluation
 - Do you have a written monitoring & audit plan?
 - Do you have a documented method to identify potential fraud, waste & abuse (i.e. data-mining)?
 - Do you have a documented response plan for privacy/security breaches?
 - Do you have written corrective action plans?
 - What are your effectiveness measures?

Step 1: Identify the Risks (cont.)

- Reporting Systems
 - Are employees aware of how to report compliance violations?
 - Do you promote an anonymous mechanism to report?
- Accountability & Remediation
 - Are compliance violations dealt with consistently? Are individuals held accountable? Are disciplinary actions taken at all levels?
 - Do you have a procedure in place to address handling of violations?
 - Does the procedure include evaluation & modification of the compliance plan?

Step 1: Identify the Risks (cont.)

- Other Risks
 - Have you reviewed all relevant documents, including:
 - Contract, Amendments, RFP and Proposal
 - Regulations
 - Letters of Directions from Client/State
 - Policies and Procedures
 - Manuals
 - Review the key performance indicators
 - What keeps you awake at night
 - What do you hear in the hallways
 - What do hear from other satellite locations, organizations, trainings, seminars, and the news

Step 2: Assessing Current Activities

What are you currently doing to meet the requirements?

Are departments communicating and coordinating activities related to overlapping risks?

How are these activities documented?

- What evidence or documentation would you use to prove you are compliant?; or
- What evidence or documentation would you use to prove you've improved compliance or initiated corrective measures that will be tracked for future improvement?
- Where is the evidence/documentation tracked and stored?

Step 3: Evaluate/Prioritize the Risks

Which risks are the most critical and pose the biggest threat to your organization?

- Severity and type of consequence:
 - Legal-criminal or civil
 - Financial
 - Reputational
 - Exclusion
- Likelihood of occurrence

Coordinate with & include all operational areas (inter-departmental coordination) re: evaluation & prioritization of risks

Next Steps: Using the Risk Assessment to Develop a Work Plan & Implement Change

- Develop a work plan with assigned responsibilities & prioritized tasks based on risk assessment findings
- Implement work plan through inter-departmental efforts
- Document all efforts to remedy non-compliance or reduce risks
- Periodically review risk assessments & work plans to ensure progress on compliance improvements
- Update the risk assessment & work plan as necessary

Benefits of Risk Assessments

- Contractual & Regulatory Compliance
- Compliance with Federal Requirements
- Program Improvements
- State/Federal Audit Preparation
- Inter-departmental Coordination
- **Can Demonstrate Effectiveness**

PROGRAM INTEGRITY TIPS

Do we have in place and can we support with appropriate documentation all 7 elements of an effective compliance program (as adopted by CMS and OIG):

Yes No

Written policies and procedures;

Compliance officer and Compliance committee;

Effective training and education;

Effective lines of communication between the compliance officer, board, executive management and staff, including an anonymous reporting function;

Internal monitoring and auditing;

Disciplinary enforcement;

Mechanisms for responding to detected problems.

Do we have in place and can we support with appropriate documentation the proposed 8th element of a compliance program:

Yes No

Is our program effective (i.e., can we show that we are preventing, detecting and resolving fraud, waste and abuse)?



Does our program consist of the following:

Yes No

- | | | |
|--------------------------|--------------------------|---|
| <input type="checkbox"/> | <input type="checkbox"/> | Documentation, consistently maintained, of all policies, procedures, program integrity activities, audits, investigations, etc.? |
| <input type="checkbox"/> | <input type="checkbox"/> | Procedures to ensure that our contractual and regulatory requirements are fully met? |
| <input type="checkbox"/> | <input type="checkbox"/> | Tool to assess the company's risk and compliance with contractual and regulatory requirements? |
| <input type="checkbox"/> | <input type="checkbox"/> | Work plan to prioritize the identified compliance risk assessment activities and resources? |
| <input type="checkbox"/> | <input type="checkbox"/> | Training and education of staff on how to recognize fraud waste and abuse as well as how to prevent, detect and report it? |
| <input type="checkbox"/> | <input type="checkbox"/> | Process to audit medical records to ensure documentation accurately supports claims submitted for payment and that the documentation meets standards? |
| <input type="checkbox"/> | <input type="checkbox"/> | System in place to identify when an employee has lost his/her credentials (due to expiration, revocation, disbarment, etc.) |
| <input type="checkbox"/> | <input type="checkbox"/> | Link between treatment provided and the billing function to ensure accurate billing of the funding source? |
| <input type="checkbox"/> | <input type="checkbox"/> | Process to return all erroneously paid claims to the appropriate funding programs and correct all identified errors? |
| <input type="checkbox"/> | <input type="checkbox"/> | Process to proactively seek evidence of fraud, waste and abuse, such as data-mining? |
| <input type="checkbox"/> | <input type="checkbox"/> | Process to report all fraud, waste and abuse issues to the appropriate contracted, state and/or federal agency? |

Program Integrity Links

- Code of Federal Regulation
 - TITLE 42-Public Health, Chapter IV-CMS, DHHS, SUBCHAPTER C-Medical Assistance Programs, Part 455-Program Integrity: Medicaid
www.gpoaccess.gov/cfr/index.html
- Office of Inspector General (OIG):
 - www.oig.hhs.gov/fraud.asp
- Center for Medicare and Medicaid Services (CMS):
 - www.cms.gov/MedicaidIntegrityProgram/
- National Association of Medicaid Fraud Control Units (NAMFCU):
 - www.namfcu.net/

ValueOptions® Contact & Reporting Info:

- Susan Mitchell, Compliance Director – Tennessee
 - 423-535-6330
- Ron Melzer, Ph.D., Director of Quality Management – Tennessee
 - 1-347-821-8553
- ValueOptions® Ethics Hotline
 - 1-888-293-3027
- Report Concerns to Your Organization's Compliance Office, ValueOptions® directly, or via ValueOptions' Ethics Hotline
 - Remember: You May Report Anonymously and Retaliation is Prohibited When You Report a Concern in Good Faith
 - Reporting All Instances of Suspected Fraud, Waste and/or Abuse is an Expectation and Responsibility for Everyone
- Tennessee (OIG) Fraud Division
 - <http://www.tn.gov./tnoig/ReportTennCareFraud.html>
 - Fraud Toll Free Hotline @ 1-800-433-3982

Questions?