



How to Conduct an Investigation and Use the Results for Continual Process Improvement

Piecing it Together

HIPAA Summit Thirteen

Tuesday, September 26, 2006

Sharon A. Budman, BBA, MS. Ed, CIPP

Ishwar Ramsingh, MBA, CISSP, CISM, CISA

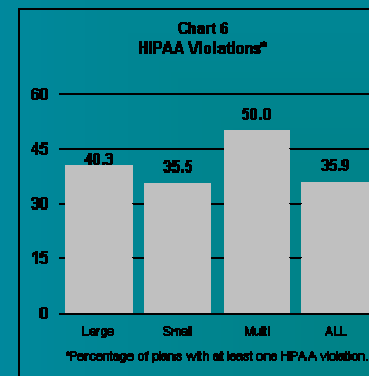
Organizational Cultural Awareness

- Create and maintain a culture of compliance
- Define a standardized process for reporting potential incidents
- Train the masses on the process
- Encourage the reporting of issues
- Reinforce the need for continual improvement
- Stress the concept of teamwork as it is an important element of compliance from an institutional perspective



Sources of Incidents

- Employees
 - Departments (Security, Guest Relations)
 - Patients
 - Documentation/Files, Forms and Records
 - Direct Observation and Monitoring
- Audit and Oversight



Types of Incidents

- **Misuse of system access**

- Accessing information inappropriately
 - Celebrity or VIP accounts and/or medical records
 - Co-worker accounts and/or medical records
 - Family member accounts and/or medical records
 - Sharing or posting passwords



- **Inappropriate Disclosure**

- Providing PHI to unauthorized individuals
- Insufficient authorization or completed release forms
- Posting PHI on unsecured web sites

- **Loss of data**

- Missing files or records
- Lost equipment containing PHI
- Storing unencrypted PHI on removable computer media



Tue Dec 10 21:01:59

Receiving/Obtaining the Data

- Allow for multiple methods of reporting
 - In-person
 - Via Telephone
 - Via Email, Fax, or mail
 - Post contact information on relevant web site and Notice of Privacy Practices
- Communicate the methods to the employees as they are the eyes and ears of the organization
 - Essential component of privacy and security training
 - Emphasize no retaliation for reporting potential violations



The Process

- Document and review the data received
- Analyze the data to determine whether a potential violation occurred
 - Nature of violation
 - Severity of violation
 - Potential impact
- Determine the best manner to investigate each particular incident
 - Direct Observation/Walk-through
 - Personal Interviews (when particular staff have been implicated)
 - Formal Audit
 - Involvement of other internal departments/areas
 - Involvement of external authorities



The Process Cont'd

- Obtain or run system/audit reports to validate information, if applicable
- Contact Human Resources to:
 - Notify them of potential employee violation
 - Conduct a joint personal interview of the employee (s) involved
 - Involve the direct supervisor and/or departmental administrator of the implicated employee, as necessary



Evidentiary Information



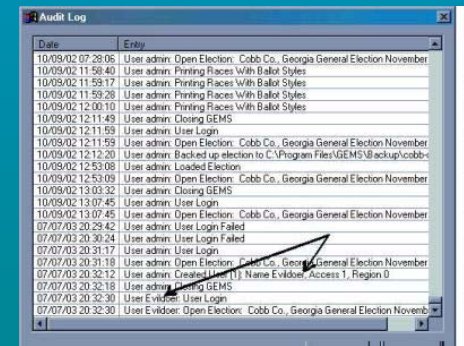
- Obtaining and documenting solid evidence as proof of what has occurred is the key to any successful investigation
- Maintain objectivity – one cannot assume that the truth is what is being provided
- Validating information using system reports, pictures, personal statements, etc. is important for credibility and integrity
- **NOTE:** Most incidents involve the use of computer systems
 - Audit trails and system logs (properly configured) often provide indisputable evidence of system misuse

Audit Trails /System Logs

- Not just for the “techies”
- Should be managed as a legal record
 - Complete
 - Accurate
 - Verifiable
- Provide the digital evidence that can prove malicious and/or deliberate intent or knowledge
 - Defense that intrusion/attempt was accidental
 - “I didn’t know I was doing something wrong”
 - Logs show repeated attempts at 1 am
 - Ignorance defense is exposed as a “sham”

System Generated Reports

- Systems containing PHI should provide unique User-IDs to all system users
- Audit Trails/Logs should provide
 - Username
 - Time
 - Date
 - Application or module accessed
 - Highly desirable to include workstation name and/or IP address
- Ideally reports should be run by an area/group independent of IT Operations



Date	Entry
10/09/02 07:28:06	User admin: Open Election: Cobb Co., Georgia General Election November
10/09/02 11:59:40	User admin: Printing Places With Ballot Styles
10/09/02 11:59:17	User admin: Printing Places With Ballot Styles
10/09/02 11:59:28	User admin: Printing Places With Ballot Styles
10/09/02 12:00:10	User admin: Printing Places With Ballot Styles
10/09/02 12:11:49	User admin: Closing GEMS
10/09/02 12:11:59	User admin: User Login
10/09/02 12:11:59	User admin: Open Election: Cobb Co., Georgia General Election November
10/09/02 12:12:20	User admin: Backed up election to C:\Program Files\GEMS\Backup\cobb-
10/09/02 12:53:09	User admin: Loaded Election
10/09/02 12:53:09	User admin: Open Election: Cobb Co., Georgia General Election November
10/09/02 13:03:32	User admin: Closing GEMS
10/09/02 13:07:45	User admin: User Login
10/09/02 13:07:45	User admin: Open Election: Cobb Co., Georgia General Election November
07/07/03 20:29:42	User admin: User Login Failed
07/07/03 20:30:24	User admin: User Login Failed
07/07/03 20:31:17	User admin: User Login
07/07/03 20:31:18	User admin: Open Election: Cobb Co., Georgia General Election November
07/07/03 20:32:12	User admin: Created User (11) Name Evidoor, Access 1, Region 0
07/07/03 20:32:18	User admin: Closing GEMS
07/07/03 20:32:30	User Evidoor: User Login
07/07/03 20:32:30	User Evidoor: Open Election: Cobb Co., Georgia General Election Novemb

Evaluating the Evidence



- Does the data support the accusation?
- Is there adequate evidence?
- Does the violation specifically map to a policy or direct section of the regulation (this is important when documenting the violation)?
 - If so, was the implicated employee forthright in the investigation?
 - Direct admission of guilt
 - Admission of the possibility
 - Flat out denial of the accusation despite the data

Scenarios

- Employee admits guilt
- Employee admits partial guilt
 - Admits wrong-doing/inappropriate behavior for only some of the evidence presented
 - Determine if admission of partial guilt is sufficient for HR
 - Sometimes the time and effort required to conduct further investigation is not worth the cost
- Employee denies wrong-doing



Employee denies wrong-doing



- Someone else used my username and password
- If this seems credible, then further evidence/audit logs may need to be investigated
- Remember – employee may be telling the truth
- Are there network access logs that identify workstation name and /or IP address?
- Are there building access logs/security camera film that firmly establishes employee location at time of incident?



Employee denies wrong-doing Cont'd



- Evidence of employee telling truth
 - IP address or workstation name is not one that employee has access to
 - Employee was not in building at time of access
 - Assumes you have means of distinguishing remote access and local access
 - Check logs when employee was sick or on vacation/leave
 - Was username active during these dates?
 - Strong evidence that some one else, at the very least, knows user's ID and password
- Assumption that you are not using SSO system with two factor authentication
 - 2nd factor is a physical token or biometric scan

Employee denies wrong-doing Cont'd

- Determine if you want to go after the real culprit
 - May need to involve
 - Application Security
 - System (O.S.) Support
 - Network Infrastructure
 - Physical Security
- Opportunity to reinforce to the “accused” the importance of guarding authentication credentials
- Best practices
 - Have a policy that requires regular change of passwords
 - Enforce that policy by application/system settings
 - i.e. force the users to change passwords “regularly”
 - Unique password requirements
 - Password complexity



Application of Sanctions in Employee Implicated Incidents

- Is a sanction warranted?
- Does the sanction fit the violation?
 - Nature
 - Severity
 - Intentional or unintentional
 - Pattern of improper use or disclosure
- Consistency is paramount to the application of sanctions within the organization
 - Sanctions may range from verbal warning to termination



Creating Reports



- Develop a template to document each violation
- Prepare a confidential report to document the investigation
- Report should be comprehensive and include all aspects of the investigation
- Distribute the report to Human Resources, if applicable
- Reports should be on file in the HIPAA Compliance area as documentation
- Documentation is paramount in every investigation

Documentation and Trends



- Record all incidents in a database
- Close all items found to be incidents and document their resolution
- Document via report all incidents found to be true violations
- Create files maintaining support documentation
 - Backup and secure (practice what you preach)
- Trend the data to determine corporate categories of Incidents/Violations

Continual Process Improvement



- Provide reports to leadership outlining the trends
 - E.g. complaints with user accounts and passwords may provide justification for expense of SSO
- Use the incidents trends to continually educate and enlighten the staff
- Create training materials that focus directly on areas of deficiencies across the organization
- Target specific areas and departments with recurring issues
- Provide regular reminders and awareness tips to the employee community
 - New threats/issues are continuously arising

Continual Process Improvement



Impress upon the staff the importance of maintaining a culture of Privacy with respect to patient information

- Provide opportunities for training reinforcement through any media
- Continue to monitor and assess areas of deficiencies via direct observation and formal auditing, if necessary
- Revisit and modify policies and procedures on a regular as well as needed basis

Building Patient Trust & Increasing Quality of Care

Security protects protected health information



Healthcare organizations build patient trust by protecting protected health information



Trust between provider and patient thereby improves quality of patient care





Questions?

Sharon A. Budman, MS. Ed, CIPP

Director of HIPAA Privacy & Security

University of Miami Miller School of Medicine

sbudman@med.miami.edu

305-243-5000

Ishwar Ramsingh, MBA, CISSP, CISM, CISA

HIPAA Information Security Administrator

University of Miami Miller School of Medicine

iramsingh@miami.edu

305-243-5000