




HIPAA Compliance Case Study: Establishing and Implementing a Program to Audit HIPAA Compliance



Drew Hunt
Network Security Analyst
Valley Medical Center

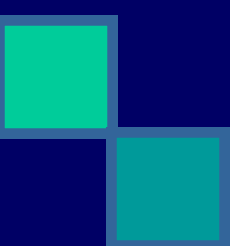



Disclaimers & Definitions:

- **Disclaimer:** The focus of this presentation is based on the auditing process which we will follow to ensure Valley Medical Center is HIPPA compliant. This process will include auditing people, procedures and security logs. This is a journey not a task!
 - **Compliance-** At Valley Medical Center we are tying privacy and security into one coherent plan rather than building separate silos of concern. This is recommended for hospitals that already deal with JCAHO in order to create a more viable long term strategy. For us at Valley, privacy and security have complementary goals.
 - For further technical guidelines or questions, email me at drew@valleymed.org.
- 

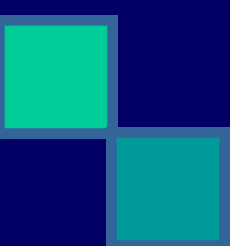



Security Quote

- 
- Maybe you don't have any security problems because no one is looking at security.
 - Your security weakness will not be at the system level- it will be a breakdown at the human level. –Drew
- 




How do I start?

- 
- Get on the path!
 - Review the HIPPA regulations and follow the necessary requirements.
 - Create a checklist that combines your policies and the HIPAA/JCAHO/State regulations for validation.
 - Update policies to include the HIPPA regulations.
 - Incorporate management and Administration
 - Set up a schedule to periodically report to management and continue staff development
- 




Okay, then what?

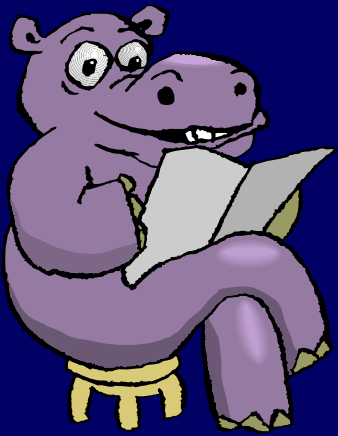
- Use the “top-down” strategy approach.
 - Manage expectations
 - “Make it so!”
 - “Are we done yet?”
 - Keep administration and staff informed and involved. Remember security is everyone’s responsibility.
- 



§ 164.306 Security standards: General rules.

(a) General requirements. Covered entities must do the following:

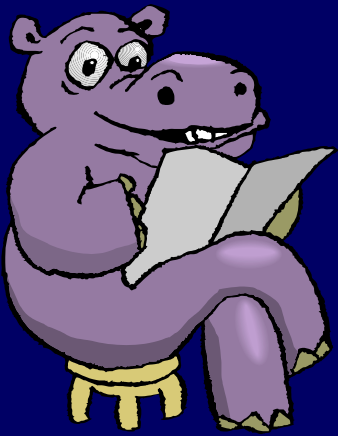
- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
 - (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
 - (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
 - (4) Ensure compliance with this subpart by its workforce.
- 



§ 164.306 Security standards: General rules.

(d) Implementation specifications

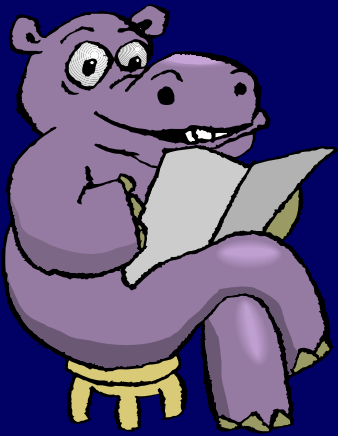
- (i) Assess whether each implementation specification is a reasonable and appropriate...and
- (ii) As applicable to the entity--
 - (A) Implement the specification; or
 - (B) If implementing the implementation specification is not reasonable and appropriate--
 - (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and
 - (2) Implement an equivalent alternative measure if reasonable and appropriate.

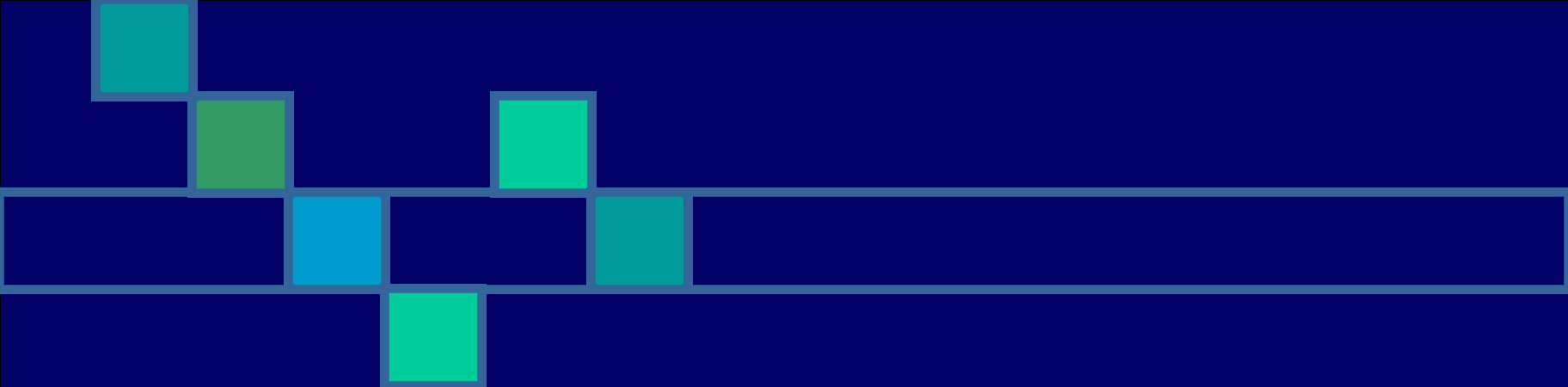


§ 164.308 Administrative safeguards

(ii) Implementation specifications:

- ...(D) Information system activity review.
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.






System Auditing Notes



In god we trust, All others we audit.



Audit Privacy & Security together

- What are the potential gaps?
 - Lack of Procedures or lack of implementation
 - Lack of Education
 - Lack of understanding
 - Lack of awareness
 - Vulnerability to social engineering –Be careful
 - Lack of consistency
 - Will every department have the same policies?
No....and that is not a bad thing.
- 




Auditing Basics



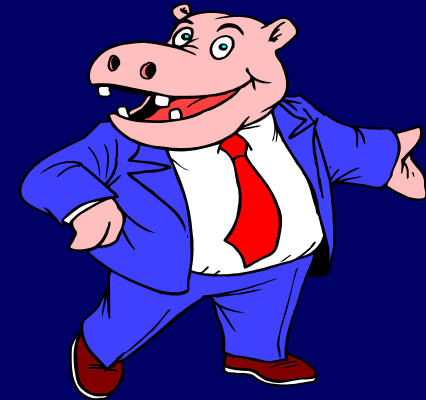
- How often
- Who is involved
- Who do we report to
- What are the objectives
- Where do we store logs, reports and incidents



What am I auditing for?

- Policy awareness understanding and implementation.
 - Client computer configuration-
 - Anti-Virus, Installed software, Screen Saver, Patches,
 - Users knowledge on reporting privacy and security incidents
 - Users knowledge of the PHI disposal policy
 - Physical Security
 - Authentication requests
 - Failed login attempts
 - System logging is only one half of it-one must actually parse the logs for the logs to be useful.
- 

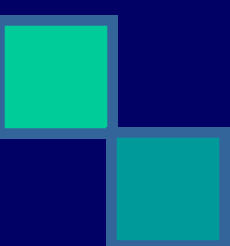

Walkthrough Info



- Use Checklists
- Give manager checklist- before and after
- Talk with staff not just to ding them but to educate them
 - Let them know that it is personally important to you but you are not a fanatic
- Make managers and staff accountable for security. You are there to spot check. Managers should enforce P & P.
 - Did I mention that you have to have a mandate from Administration




Quarterly Computer Audit

- 
- Separation of duties
 - Least privilege
 - Patches
 - Account changes
 - Log review
 - Firewall review
- 




Auditing tools and links



- Privacy Auditor
 - Event Comb
 - <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/secwin2k/default.asp>
 - Syslog
 - Swatch/logwatch
 - Log Parser
 - <http://www.microsoft.com/windows2000/downloads/tools/logparser/default.asp>
 - Elogdmp.exe resource kit tool
- 




Quarterly Awareness Campaign (for staff)

- Topics may include
 - Top 5 Privacy FAQ's
 - Virus Awareness
 - Acceptable Use
 - Password Policies
 - How to report incidents
 - Weird facts
- 



Quarterly report to Compliance Committee

- Make it meaningful
 - Make it clear
 - Be specific
 - Have a plan
- 



Questions???

- 
- Walk the path, don't just know the path!

