Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security Awareness and Training: Security Reminders

Although an organization may have the means to purchase the best firewall technology, deploy the hardest encryption standards, and implement multi-factor authentication schemes, it still needs the complement of enlightened workforce members who understand what measures they can take to help reduce security risks. To help protect electronic protected health information (EPHI), employees need to understand what they can do to ensure the security of the information systems for which they are responsible. They also should ...

Copyright SANS Institute
Author Retains Full Rights

AD

Security Awareness and Training: Security Reminders

GIAC HIPAA Security Certificate
(GHSC)

Practical Assignment
(Option B – Procedure)

Version 1.0

December 13, 2004

Kevin D. Sackett

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract 1

Assignment 1 – Define the Environment 2

Assignment 2 – Explanation 4

Assignment 3 – Policy 7

- Overview 7
- Purpose 7
- Scope 7
- Policy 8
- Enforcement 10
- Definitions 10
- Revision History 10

Assignment 4 – Procedures (Option B) 11

List of References 21

© SANS Institute 2005, Author retains full rights

© SANS Institute 2005 Author retains full rights.

Abstract
Although an organization may have the means to purchase the best firewall technology, deploy the hardest encryption standards, and implement multi-factor authentication schemes, it still needs the complement of enlightened workforce members who understand what measures they can take to help reduce security risks. To help protect electronic protected health information (EPHI), employees need to understand what they can do to ensure the security of the information systems for which they are responsible. They also should understand their organization's security policies and procedures and the expectations surrounding them.

The HIPAA Security Rule[1] underscores the importance of employee participation under the Security Awareness and Training standard of the Administrative Safeguards. Under that is the addressable implementation specification of Security Reminders:

§164.308 Administrative Safeguards
(a) A covered entity must, in accordance with §164.306

(5)(i) Implement a security awareness and training program for all members of its workforce (including management).

(ii) Implementation specifications. Implement:

(A) Security reminders (Addressable). Periodic security updates.

This paper will discuss the importance of security reminders as part of an overall security awareness and training program. It will offer suggestions and venues for security reminders as well as a security reminder policy and procedure. It will do this for GIAC Health, a fictitious regional community mental health care provider and insurer.

[1] United States, Department of Health and Human Services, Health Insurance Reform: Security Standards. 45 CFR Part 164. (Washington: GPO, 2003) 270.

© SANS Institute 2005 Author retains full rights.

Assignment 1 – Define the Environment

GIAC Health is an independent governmental authority responsible for delivering mental health services to individuals living with mental retardation and developmental disabilities within the county. It is a prepaid health plan which conducts managed care functions such as maintaining member eligibility, authorizing services, managing provider contracts, and processing claims, receiving its funding from state and federal levels. It is also a direct provider of care and employs clinicians and psychiatrists.

The IS department consists of six individuals who support Authority reporting needs, helpdesk calls and user troubleshooting, computer training, network administration, database administration, and server maintenance. Recently all of GIAC Health's servers were upgraded to Windows Server 2003 and its clients to Windows XP (SP2). Its enterprise resource planning and decision support software database applications reside on a set of Dell PowerEdge servers configured for Internet architecture, backed up on a PowerVault220S External Storage device. A second set of Compaq servers maintain the Authority's Exchange email system, public shares, and network authentication. A dedicated PC serves as the Software Update Services server.

GIAC Health contracts its firewall and Internet email routing to a network administrator. The network contractor protects Internet email traffic using McAfee anti-virus software and GIAC Health IS staff maintains the same on all of its servers and email clients internally. The GIAC Health Network Administrator also ensures that critical patches for its Windows servers and clients are deployed across its domain automatically via Software Update Services. It uses Arcserve's tape back up solution and back ups occur nightly. Back up tapes are taken offsite weekly to its North Center location, where they are stored in a fire-proof safe behind a secure, fire-protected door.

GIAC Health maintains four sites: The Authority's main location downtown is connected via two T1s to its North Center using Cisco 1721 routers, with the T1s begin maintained by SBC, the local telco. GIAC Health also provides crisis mental health services after hours at the local hospital where it has two workstations placed for use by the after-hour workers. These two workstations are connected via VPN. The last site, South Center, is located many miles outside of the city in a rural location, and its workforce members are connected via VPN over a wireless, point-to-point Internet connection. VPN tunnels terminate inside the Authority's main location at a Cisco VPN 3000 device. GIAC Health also allows VPN connection for various providers for the purpose of entering assessments and billable activity directly into the main billing system.

© SANS Institute 2005 Author retains full rights.

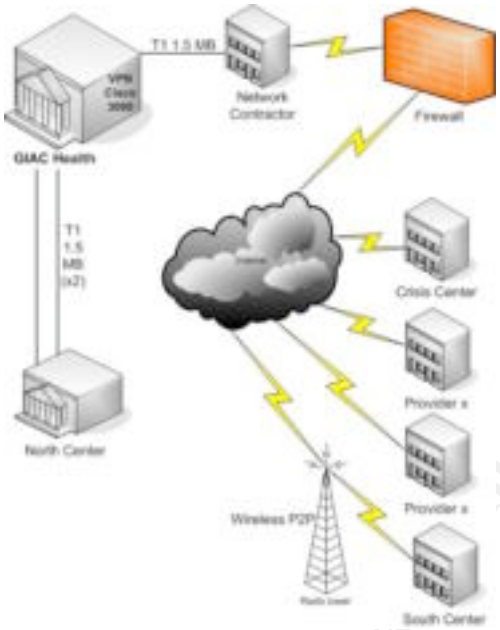

Figure 1. GIAC Health, Site Connection Overview

Between its staff of approximately 250 employees and hundreds of contracts with providers, GIAC Health operates in a complex funding environment serving approximately five thousand patients, or consumers, annually. Its direct staff is a diverse mix of managed care professionals and clinicians who are busy meeting monthly productivity goals and the requirements of multiple regulatory obligations and accrediting bodies for both sides of its business. The Authority is also responsible for overseeing that all of its contract providers meet Medicaid regulatory obligations as well and regularly audits providers.

Staff and contract providers comprise a network of care spread across a region of over a thousand square miles. They regularly use laptops in the field to record protected health information. For example, they often type progress notes which identify the consumer and the consumer's related health condition and treatment progress. Nurses also record vital signs on notes which identify the consumer on the laptop. The information is loaded in to the main database application after the clinician returns to GIAC Health's main location.

To communicate with its many constituents, GIAC Health uses internal and external newsletters and brochures, an Internet website (externally hosted), an Intranet webpage and email broadcasts. It posts announcements throughout its public areas, such as lobbies, corridors, and staff lounges. It also developed a training program and regularly conducts mandatory training on a wide range of topics for direct staff and contractors.

© SANS Institute 2005 Author retains full rights.

Assignment 2 – Explanation

Periodic security reminders is one of four addressable implementation specifications within the broader Security Awareness and Training standard at §164.308(a)(5)(i):

> "Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).
>
> (ii) Implementation specifications. Implement:
>
> (A) Security reminders (Addressable). Periodic security updates."

The HIPAA Security Rule intends for covered entities to train the "workforce as reasonable and appropriate to carry out their functions in the facility." Covered entities should regard security awareness training as critical to its workforce staff at the same time allowing covered entities flexibility and discretion in how they choose to implement awareness training.[2] On the topic of periodic security reminders the Rule elaborates, telling us covered entities have latitude in deciding the scope of "periodic" with the caveat that "training should be an on-going, evolving process in response to environmental and operational changes affecting the security of electronic protected health information". [3] It states that security training or awareness programs do not necessarily have to be elaborate, and suggests these become integrated into a covered entity's overall training and orientation program. It even offers a few examples of convenient venues, such as publishing pamphlets or distributing copies of security policies and procedures.[4]

Covered entities can take advantage of virtually any media within its means for deploying reminders. For example, they could be shared simply face-to-face in a meeting where reminders are a standing agenda item. The other extreme would be an automated security reminder deployment across the entire workforce, such as in Cosaint's Security Reminder Service (SRS). The SRS system is an automated email system and a part of its larger Learning Management System. The manager of the system has the ability to automatically generate and schedule email messages containing security awareness content. Topics that come with the program include password management skills, secure use of email, the importance of patching software and several other security topics. The system manager also has the option to add customized reminders. In between these two extremes are many technologies for deploying security reminders. The government suggests using email updates, articles in newsletters, messages on screensavers, postings in corridors or other public areas, intranet postings, training videos.[5] For continual reinforcement, the list is endless. There are as many ways to get the security reminders message out as there are ways to publish or messaging technologies.

---

[2] United States, Department of Health and Human Services, p. 96-98
[3] United States, Department of Health and Human Services, p. 101
[4] United States, Department of Health and Human Services, p. 100
[5] United States, Department of Commerce, National Institute of Standards and Technology Special Publication 800-66, An Introductory Resource Guide for Implementing the HIPAA Security Rule (DRAFT) (Washington: GPO, 2004) 26.

© SANS Institute 2005 Author retains full rights.

NIST publication 800-50 gives many good examples of security topics to address in a security awareness program and to integrate into periodic security reminders. For example, password management skills, spam, handheld devices, email etiquette, desktop security are only some of over two dozen security topics bulleted as ideas for covered entities to use.[6] But in addition to generic topics of security interest, covered entities will want to include changes which occur over time specific to their internal set of HIPAA Security policies and procedures. Note too that security reminders are a powerful vehicle for maintaining awareness on any topic, and can include privacy and other policy and procedure changes as well. Since the Privacy Rule requires training in privacy policies and procedures, one suggestion is to combine all HIPAA requirements in an overall HIPAA awareness program.[7]

Where can a covered entity locate sources of information for its security awareness program? Security awareness on these topics is not the same as security training. Training implies a more formal classroom setting where the course material has greater depth and breadth. Awareness, on the other hand, implies keeping content at less detail and in smaller sound bytes in a package which is attractive to the eye.[8] Periodic security reminders definitely fall into this latter category. Good sources for security awareness topics can be found in NIST 800-50 (p. 25). These include email advisories published by industry-specific news groups, academic institutions, professional organizations, online IT security daily news websites, periodicals, conferences and seminars.

Security awareness training should attempt to reach all workforce members of the covered entity, even those without access to the information system (for example, what should the janitor do if he or she finds a floppy disk in the garbage?). A reasonable minimum standard offered by Nebraska SNIP is to document workforce members (including contractors) who complete the initial security awareness and training program and also document who is updated with each periodic security reminder. A best practice might be to employ a sophisticated electronic system for deploying customized reminders to all workforce members by role, having them log in to retrieve them, conducting testing, and finally recording the transaction.[9]

Periodic security reminders are part of an overall security and awareness training program required for all workforce members, including management. Making periodic security reminders a requirement at GIAC Health guarantees security topics are reinforced among workforce members. Ultimately, the intent of these

[6] United States, Department of Commerce, National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program 24.
[7] Adler, Peter M, "Capitalize on Your Privacy Efforts to Get Started on Security Compliance," HIPAA Security Compliance Insider, July 2003: 6.
[8] United States, Department of Commerce, National Institute of Standards and Technology Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (Washington: GPO, 1998) 15.
[9] Nebraska Strategic National Implementation Process Task Group, Security Manual, 15 Nov 2004 <http://www.nesnip.org/securitychapter1.htm>.

© SANS Institute 2005 Author retains full rights.

efforts is to contribute to the availability, integrity and confidentiality of electronic protected health information.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Assignment 3 – Policy
This policy is designed to guide GIAC Health in its security reminders program by suggesting content and form and assigning responsibility. Other covered entities may find useful ideas here to apply for their own programs. However, please note that this policy should not be considered a standard. The topic of awareness and training methods is large in scope. Each covered entity should design a program to fit the unique needs of their business within the context of 45 CFR 164.308(a)(5)(ii)(A).

GIAC Health's Security Reminder Policy

1.0 Overview
Workforce members, including management, need to understand their responsibility for ensuring the availability, confidentiality and integrity of electronic protected health information on the management information system. They should practice good security habits at their workstations. Everyone should be mindful of GIAC Health's security policies and procedures.

After the initial security training, workforce members should be reminded periodically and these reminders should be part of an overall awareness program so that they are disseminated regularly and consistently, taking advantage of various venues or media available at GIAC Health. Periodic reminders will help remind and reinforce what workforce members learned in security training. They will also serve to alert workforce members to changes in security policies and procedures as well as to enlighten them about various security topics, such as password management skills, the importance of critical system patches, defenses against malicious software and web usage, to name a few.

2.0 Purpose
This policy sets GIAC Health's standard for providing periodic security reminders to its workforce members for the purpose of making workforce members aware of security policy or procedure changes and security topics. It suggests parameters for timing of messages, content and media. It also assigns responsibility for reviewing and approving content and for ensuring communication of security messages. Scope and applicability across the workforce are addressed as well.

3.0 Scope
This policy applies to all workforce members. The degree of applicability to workforce members will vary depending on a worker's role.

a) Workforce members who regularly use or disclose electronic protected health information will receive the greatest exposure to security reminders. Examples of roles in the category could include data analysts, system

© SANS Institute 2005 Author retains full rights.

administrators, administrative assistants, clinicians, claims processors, etc.

b) Workforce members who have network accounts but who do not regularly manage electronic protected health information will receive less exposure to security reminders. These roles could include those executives who receive aggregate data reports, mailroom clerks, HR specialists, payroll clerks and other support staff.

c) Workforce members who have no access to the information system at all will receive the least exposure to security reminders. Examples of these roles include maintenance staff, environmental services, and transportation.

4.0 Policy

4.1 The HIPAA Security Officer is responsible for the overall success of reminding workforce members of the principles of good security practices and reducing risks on GIAC Health's information systems.

4.2 The content of security reminders will be appropriate to the role of workforce members. Methods of providing information to workers will also be appropriate for a worker's role.

4.3 Security reminders must be disseminated regularly.

4.4 All workforce members of GIAC Health must receive periodic reminders, including management, workforce members at remote locations, and business associates. Providers and other contractors who are not defined as business associates of GIAC Health are not required to receive security reminder messages, unless otherwise stated by contract.

4.5 The content of security reminders must, at a minimum, reinforce the lessons learned in HIPAA Security training.

4.6 Suggested sources of content for security reminders should include, but are not restricted to:

- Specific HIPAA Security Rules topics (164.308(a)(5)(ii)(B-D):
  - Good password management skills.
  - Procedures workforce members can follow to reduce the risk of infection from malicious software and procedures GIAC Health's IS staff follow to protect information systems from malicious software.
  - Procedures GIAC Health uses for monitoring log-in attempts and reporting discrepancies.
  - Appropriate security measures to reduce the risk of improper access, uses, and disclosures of electronic protected health information.

© SANS Institute 2005 Author retains full rights.

- GIAC Health Security Policies and Procedures:
  - Additions, changes or deletions to GIAC Health's security policies and procedures.
- Security Topics from the following industry standard sources:
  - Principles of the HIPAA Security Rule.
  - NIST 800-50 Security Awareness Topics.
  - NIST 800-16 Security Awareness Terms and Concepts.

4.7 GIAC Health's security reminders should take advantage of as many activities and venues as possible. Possible methods include, but are not limited to, standing agenda items in departmental meetings (face-to-face), brochures or pamphlets, copies of security policies and procedures, employee training videos, email messages, posters, television monitor messages, regulatory training days, screen saver messages, newsletter articles, etc.

4.8 The security reminder awareness program may be incorporated into other existing training or awareness programs at GIAC Health, if it so desires.

4.9 The parameters for GIAC Health's security awareness and training program should be documented, along with documentation of security reminders in the form of a security reminder log. Specifically, elements which should be documented in a security reminder log include, but are not restricted to:

- Date security reminder published.
- Method by which security reminder published.
- Date security reminder lapsed.
- Intended audience.
- Security reminder topic.
- Follow up testing (Y/N).

4.10 The Information Security Officer is responsible for evaluating the overall effectiveness of security reminders, bearing in mind that the measure of a successful awareness program "creates the [employee's] sensitivity to the threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them."[10]

[10] United States, Department of Commerce, National Institute of Standards and Technology Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (Washington: GPO, 1998) 15.

© SANS Institute 2005 Author retains full rights.

5.0 Enforcement

5.1 This policy and any procedures related to it must be reviewed and evaluated regularly for quality assurance purposes, per GIAC Health's Compliance and Policy Committee standards.

5.2 The Information Security Officer is responsible for evaluating the overall effectiveness of the security training and awareness program, including security reminders

5.3 All GIAC Health employees must receive training in this policy as part of the HIPAA Security Training and Awareness Program.

5.4 Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or cessation of contract.

6.0 Definitions

6.1 Workforce member – Employees, volunteers, and other persons whose conduct, in the performance of work for GIAC Health, is under the direct control of GIAC Health, whether or not they are paid by GIAC Health. This includes full and part time employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to GIAC Health.[11]

6.3 Electronic protected health information – Individually identifiable health information that is transmitted by electronic media or maintained in electronic media.[12]

6.2 Malicious Software – Any software designed to damage or disrupt a system.[13] Examples of malicious software or code are viruses, worms, or Trojan horses.

7.0 Revision History

7.1 Version 1 of this policy was published in December 2004.

7.2 This policy will be reviewed annually.

[11] HIPAA Security Policies Templates Suite for Healthcare Provider Organizations (Phoenix Health Systems).
[12] Ibid
[13] United States, Department of Health and Human Services, p. 263.

© SANS Institute 2005 Author retains full rights.

Assignment 4 – Procedures (Option B)
The following procedure details what GIAC Health can do to ensure compliance with the security reminders policy above, based on the HIPAA Security Rule at 45 CFR 164.308(a)(5)(ii)(A). The procedures define specific activities departments, managers and various technical staff can follow for ensuring the regular deployment of security reminders to all workforce members, internally and remotely, and including management. As stated previously, GIAC Health operates in a complex funding environment and is obligated to many constituencies at the local, state and federal levels, across a wide geography. Getting the security message to workforce members in diverse locations will require interdepartmental cooperation and the use of multiple channels of communication.

Through the process of risk analysis, GIAC Health's HIPAA Security team concluded that the following set of procedures would provide adequate periodic security updates to its workforce. This set of procedures, along with the policy, will be presented to the Compliance and Policy committee for final approval and acceptance.

1. The HIPAA Security Office will submit an Information Services Request For Assistance Form to enable screen savers for security reminders. So that all workstations are used for this purpose, GIAC Health will use Windows Server 2003 group policy to enforce a screen saver for all clients connected to its network. The screen saver will call a Macromedia Flash shockwave file containing security update information provided by the HIPAA Security Office. The content will be appropriate for all workforce members who use a workstation. The IS department technical team will:
    a. Create a new sub domain for giachealth.org named screensaver.giachealth.org.
    b. Create a Macromedia Flash application based on the provided content and compile the security reminder to shockwave format file (.swf).
    c. Create a screensaver executable containing web controls in MS Visual C# .Net, giving it the name "screensaver.scr". The executable should contain a fixed reference to the sub domain named above.
    d. Embed the following key HTML code in a file named screensaver.htm. This will drive the shockwave (here the example uses a file named after the content, in this case on the topic of password management):
        i. <embed src="passwordmanagement.swf" quality="high" pluginspage="http://www.macromedia.com/go/getflashplayer" type="application/x-shockwave-flash" width="550" height="400"></embed></object>

© SANS Institute 2005 Author retains full rights.

e. In Active Directory, add the MSI package for deploying Microsoft .NET Framework:

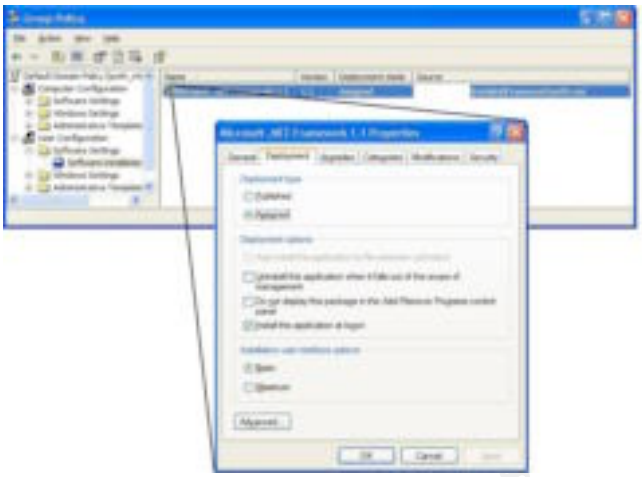

Figure 2, GIAC Health .NET Framework Software Installation MSI Deployment Group Policy settings.

f. In GIAC Health's client network logon .bat file, logon.bat, insert the following commands to install the necessary executables and DLLs on client workstations:

- COPY \\SCMH_NT01\Programs$\ScreenSaver.scr C:\Windows\System32 /Y
- COPY \\SCMH_NT01\Programs$\AxInterop.SHDocVw.dll C:\Windows\System32 /Y
- COPY \\SCMH_NT01\Programs$\Interop.SHDocVw.dll C:\Windows\System32 /Y

© SANS Institute 2005 Author retains full rights.

g. In Active Directory, using the Group Policy editor, configure the screen saver policy under User Configuration/Administrative Templates/Control Panel/Display and enable the screen saver after ten minutes of inactivity.

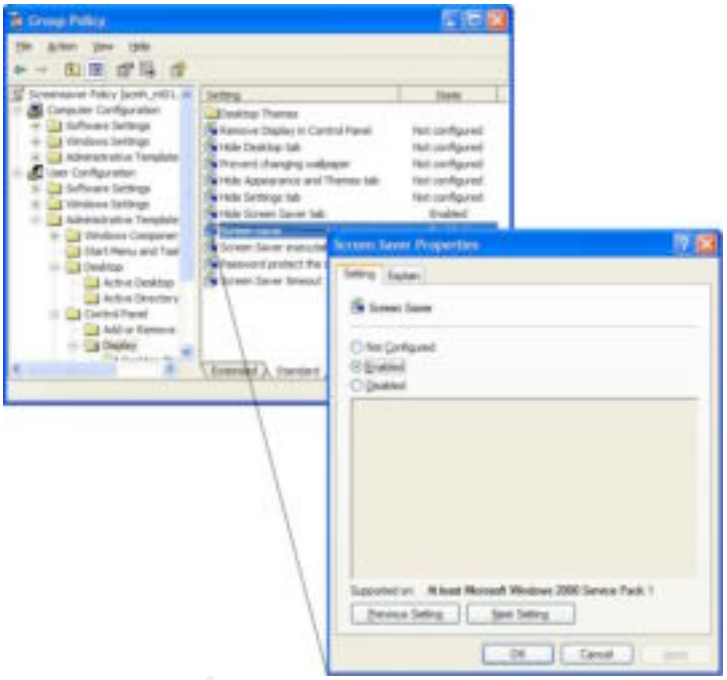

Figure 3, GIAC Health Screen Saver Group Policy settings

© SANS Institute 2005

© SANS Institute 2005 Author retains full rights.

h. Point the screen saver executable to “screensaver.scr” in the Screen Saver Executable Name group policy.

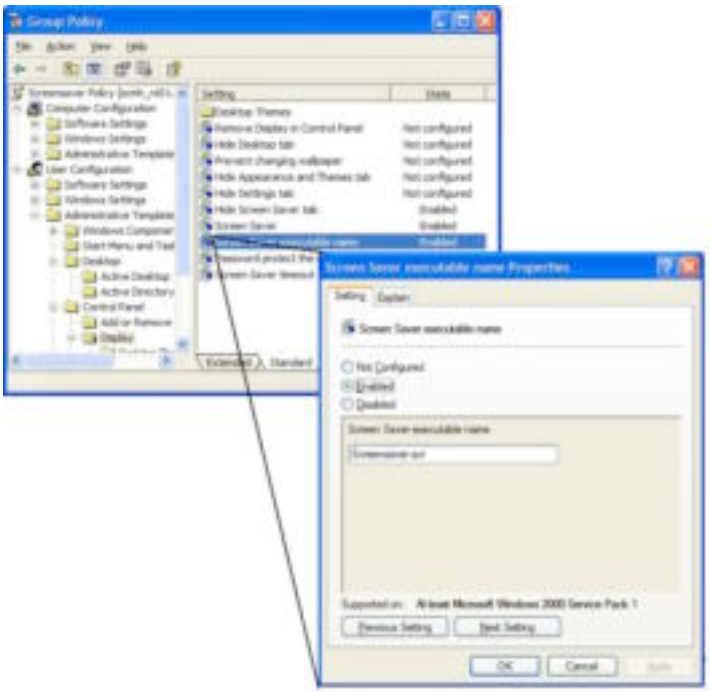

Figure 4, GIAC Health Screen Saver Executable Name Group Policy settings.

i. Configure the screen saver timeout to ten minutes (600 seconds) in the Screen Saver Timeout group policy.

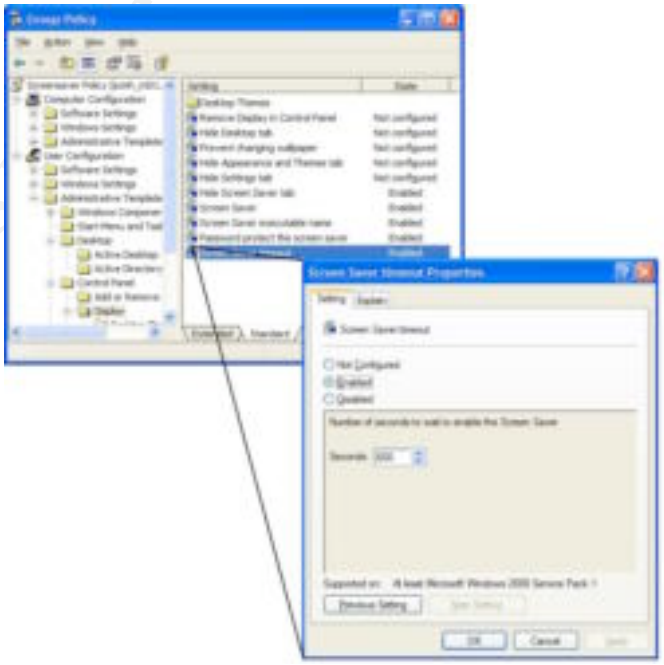

Figure 5, GIAC Health Screen Saver Timeout Group Policy settings.

© SANS Institute 2005 Author retains full rights.

j. To summarize, once all files and group policies are tested, deployed and enforced, the following should take place:
   i. After ten minutes of inactivity, group policy forces the screen saver to execute on the client workstation, calling the screen saver located at c:\windows\system32\screensaver.scr.
   ii. The screen saver calls the sub domain of screensaver.giachealth.org.
   iii. IIS sends back screensaver.htm.
   iv. Security update content is rendered on the client workstation.

k. Change content and design monthly so that the security reminders are fresh, reducing the likelihood that users will "tune out". Make content and design simple enough to convey a message at a glance.

Figure 6, Example of screen saver rendering after following this procedure.

2. Use email messages to broadcast security articles to workforce members, including clinicians. Use the web interface functionality in MS FrontPage to complete the following:
   a. The HIPAA Security Office will ask for contributions on a monthly basis from the network security administrator, IS Director, Compliance Officer, Authority Attorney and other management

© SANS Institute 2005 Author retains full rights.

team members as appropriate. Rotating contributions among several different individuals in leadership positions will make HIPAA Security appear as an organizational priority. Contributions will involve topics of HIPAA Security, security policy and procedures changes, and other relevant security topics as listed in the Security Reminder policy. The content will be broad enough to apply to all workforce members, remotely or internally, with an email account. Email messages will be posted in employee lounges for the benefit of those without an email account.

b. The HIPAA Security Office will, upon receipt of the email article, write a short, multiple choice post quiz and submit it to the IS Department for posting to the Intranet website at the following location:

   i. intranet.giachealth.com/hipaa/security/quiz

c. The HIPAA Security Office will insert a link to the post quiz at the bottom of the email pointing to the link named above.

d. The HIPAA Security Office will broadcast the email message with the link to the quiz. Email recipients of this email message, after reading the content, should click on the link and take the short post quiz which presents. Once the quiz is completed, click on the "Submit" button at the bottom of the page.

e. The quiz results are saved to a database. A macro corrects the quiz results and logs the user as having completed the security update in the agency's training database.

f. The training department will submit a list of those workforce members who failed the quiz or didn't take the quiz, for remedial action or sanctions.

3. Contribute articles on relevant security related topics in the agency's monthly internal newsletter, "The GIAC Health Times".

   a. The HIPAA Security Office will contribute a security related topic for every other issue. The newsletter article will be titled "GIAC Health Employee HIPAA Security Update."

   b. Contributions will be submitted to the HR department for approval and inclusion to the newsletter.

   c. Article content will be broad enough to apply to all regular employees of GIAC Health.

4. Contribute articles on relevant security related topics in the agency's external provider network newsletter, "The GIAC Health Provider Network Newsletter."

© SANS Institute 2005 Author retains full rights.

a. The HIPAA Security Office will contribute a security related topic for every other issue. The newsletter article will be titled "GIAC Health Provider Network HIPAA Security Update."

b. Contributions will be submitted to the Network Services department for approval and inclusion to the newsletter.

c. Article content will be tailored to the distinct needs of GIAC Health's providers, who are generally less technology enabled than GIAC Health itself and who look to GIAC Health for guidance in business matters. Topics will include GIAC Health's stance on PHI in email communications, risks of using floppy disks and other portable media with regard to electronic protected health information, importance of system back ups, recommendations for system or network security, good PC security practices, and other pertinent subjects relevant to small providers.

5. Display posters on security topics.

   a. Posters displaying topics on system and workstation security will be displayed in the following areas which manage electronic protected health information heavily :

      i. Finance Department

      ii. IS Department

      iii. PC lab

      iv. Administration

   b. Poster content will be approved by the HIPAA Security Office and purchased through the Purchasing Department.

6. Contribute oral updates to the Management Team at Management Team Meetings.

   a. GIAC Health Management Team meets every six weeks. The HIPAA Security Officer will contribute HIPAA Security content relative to the administrators of GIAC Health at every other meeting (every twelve weeks).

   b. Periodic security update content suggestions may include reporting virus incidents, security policy and procedure updates, staffing issues surrounding implementation of security measures, security sanction policies, security incident reporting, principles of disaster recovery, safeguard cost justifications and any of the security topics identified in the HIPAA Security Reminder Policy which may be relevant at the administrator level.

7. Provide technical security updates to IS data analysts, network administrators and other IS technical staff involved in batching, transmitting, authorizing access to electronic protected health information.

© SANS Institute 2005 Author retains full rights.

a. The network administrator will take the lead for content relative to managing and aggregating data and disseminating that information to technical staff.

b. Suggested topics include policy and procedure reminders in the areas of establishing unique user IDs, the how of emergency access procedures, reviewing IS termination procedures, ensuring automatic log off, auditing for appropriate use of MIS, access authorization, authentication (integrity) mechanisms, and any other security topic relevant to workforce members at a technical level.

c. Security reminders to IS technical staff can be presented at brown bag lunch case study walk through sessions, face to face, for the opportunity for staff question and answer sessions to work through some of the more complex technical issues. These should occur monthly.

8. Provide simple security updates to non-system staff.

   a. The HIPAA Security Office will prepare a list of security topics appropriate for non-system staff, including maintenance, janitorial services, van and bus drivers, mail room clerks, and security guards.

   b. Examples of topics to start with may include expectations with regard to moving IS equipment, what to do when discovering portable media loose (i.e., floppy disk or CD in garbage or on floor, etc.), IS concerns, policies and procedures regarding facility security to the MIS, and their involvement in GIAC Health's disaster recovery plan.

   c. The HIPAA Security Officer can present the reminder orally at these non-system staff meetings every other month in order to answer questions or review concerns.

9. Update business associates.

   a. All contractors defined as business associates will be mailed a standard brochure describing GIAC Health's security policy and procedures for business associates.

   b. A cover letter and copy of the brochure will be placed in each business associate's contract file in the Network Services department.

   c. Each letter will be sent with a return receipt request.

   d. The return receipt will be filed in the business associate's contract file.

10. Create a booth display complete with reference materials and quizzes for the Regulatory Training Days fair for all workforce members.

© SANS Institute 2005 Author retains full rights.

a. The HIPAA Security Office will prepare an informational booth outlining security reminders based on the initial security training content. The booth will display information using colorful graphics, games, and humor to engage workforce members in the material.

b. The both is intended for all workforce members, including management and internal and remote employees and contractors.

c. The informational booth will be submitted to the training department which has responsibility for coordinating the fair, for approval and set up. The training department will be responsible for collecting quizzes, grading them, and logging results in to the training database. The training department will also assure that all workforce members attending the fair are properly signed in.

d. The training department will submit a list to those workforce members who failed the quiz, didn't take the quiz, or didn't show up to the fair, for remedial or sanction measures.

11. Provide specialized reminders to traveling clinicians using laptops.

    a. Clinicians managing electronic protected health information on laptops should receive specialized training in how to properly manage their assigned laptops to protect laptop data.

    b. After the training, clinicians will receive periodic reminders on proper laptop management to reinforce the training received. Training topics to be reinforced must include, at a minimum, how to manage laptop encryption features, how to secure laptops, ensuring laptops are checked out appropriately (accountability), how to protect laptops from weather extremes, how to download laptop data into the main clinical system, in addition to general instructions for using and managing laptops.

    c. GIAC Health IS staff will distribute these reminders in the form of a brochure provided inside each laptop case.

    d. The HIPAA Security Office will assess competence and adherence to laptop procedures for clinicians using the procedure outlined below in Step 13.

12. All security reminder update events described above will be logged in a spreadsheet. The spreadsheet will record the security content topic, audience, medium, date delivered, date lapsed (if applicable), whether or not a quiz was required, pass/fail status of the quiz, and who took the quiz (if applicable). The HIPAA Security Officer will be responsible for tracking the security reminder update events in the spreadsheet. The HIPAA Security Officer will submit a security reminder update event report to the Compliance Officer quarterly.

13. Information security managers need to receive feedback on the safeguards implemented for security risk reduction. The HIPAA Security

© SANS Institute 2005 Author retains full rights.

Rule asks for this at several places: 164.308 (a)(a)(D): Information system activity review, 164.308 (a)(6): Security incident procedures, 164.308 (a)(8): Evaluation, and 164.312 (b): Audit Controls.[14] Obviously, employee awareness assists in risk reduction, but only if the awareness program is effective, is doing its job. Therefore, GIAC Health should take the following measures for measuring compliance with this procedure and for evaluating effectiveness:

a. This procedure will be submitted to GIAC Health's Compliance and Policy Committee for review and acceptance.
b. The Compliance Officer will be responsible for measuring compliance with this procedure and submitting feedback to the HIPAA Security Officer, according to the compliance monitoring procedures developed in the Office of Regulatory Compliance.
c. Compliance evaluations will occur annually and be conducted by the Compliance Officer.
d. The HIPAA Security Officer will conduct random walk throughs of different departments, asking staff questions on recently published security topics, for a subjective analysis of general staff security awareness.
e. The HIPAA Security Officer will also have the authority to assess adherence to the content presented in security updates. For example, if a security update is published about good password management skills, the HIPAA Security Officer will check for passwords written down around workstations or under keyboards or run auditing tools to check for sharing of passwords. As another example, if a security update is published reminding staff about positioning monitors in public places for maximum privacy, the HIPAA Security Officer will conduct inspections afterward to ensure compliance.
f. When non-compliance is found after publishing security updates, or workforce members fail security updates, the HIPAA Security Officer will follow up with the management of the affected workforce member for remedial action or sanctions.

[14] Julie Baumler, et al., HIPAA Security Implementation (SANS, 2004) 253.

© SANS Institute 2005 Author retains full rights.

List of References

Adler, Peter M. "Capitalize on Your Privacy Efforts to Get Started on Security Compliance." HIPAA Security Compliance Insider July 2003.

Baumler, Julie, et al. HIPAA Security Implementation. SANS, 2004.

Nebraska. Nebraska Health and Human Services System. Security Manual. 15 Nov. 2004 <http://www.nesnip.org/securitychapter1.htm>.

HIPAA Security Policies Templates Suite for Healthcare Provider Organizations. Phoenix Health Systems, 2004.

United States. Department of Health and Human Services. Health Insurance Reform: Security Standards. 45 CFR Part 164. Washington: GPO, 2003.

United States. Department of Commerce. National Institute of Standards and Technology Special Publication 800-66, An Introductory Resource Guide for Implementing the HIPAA Security Rule (DRAFT) Washington: GPO, 2004.

United States. Department of Commerce. National Institute of Standards and Technology Special Publication 800-16, Information Technology Security Training Requirements: A Rose- and Performance-Based Model Washington: GPO, 1998.

United States. Department of Commerce. National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program Washington: GPO, 2003.

© SANS Institute 2005 Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced