

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.




# HIPAA Gap Analysis

## GIAC Certified Security Consultant (GCSC)
## Practical Assignment - Version 1.0
## Challenge

**T. Brian Granier**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract ..... 3
Part 1: Methodology and Process ..... 4
Business Structure ..... 4
Target Client Base ..... 4
General Methodology ..... 4
GIAC Enterprises ..... 6
Part 2: Proposal and Pitch ..... 7
Proposal ..... 7
Cover Letter/Executive Summary ..... 7
Proposal/Scope of Work ..... 8
Pitch ..... 11
Part 3: Project Performance ..... 12
Project Plan ..... 12
Overview ..... 12
Objectives ..... 12
Phase I ..... 14
Phase II ..... 16
Phase III ..... 18
Budget Details – Estimate ..... 20
Meeting/Interview Facilitation ..... 21
Introduction ..... 21
Identifying Keys to Success ..... 22
Information Gathering ..... 22
Conclusion and Recap: ..... 23
Potential Pitfalls ..... 24
Value Add – Ongoing Business ..... 24
Part 4: Final Deliverables ..... 26
Section A ..... 26
Executive Summary ..... 26
Summary of Results ..... 27
Administrative Safeguards: Details ..... 29
Physical Safeguards: Details ..... 39
Technical Safeguards: Details ..... 44
Appendices ..... 47
References ..... 49

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## Abstract

This practical is written for the GIAC GCSC v 1.0 practical assignment. This covers the lifecycle of a single engagement for a HIPAA Security Rule Gap Analysis. GIAC Enterprises is a small clinic that is contracting with Circron Consulting to perform the Gap Analysis and provide a remediation plan. This paper will provide a basic explanation of the two organizations, the scope of work and sales methodology. Next, is information about completing the project, including a more detailed project plan, sample questions, and potential pitfalls. Finally, a sample deliverable is provided.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

# Part 1: Methodology and Process

## *Business Structure*

Circron Consulting Corporation is a small consulting firm based in Houston, Texas consisting of two highly trained consultants, three moderately skilled general technicians and an administrative person that provides accounting, sales and management responsibilities. Established in 1995, Circron has found a niche market in consulting to legal and medical clientele with a focus on medium to small practices. Typical services include complete management of server systems such as email, antivirus, firewalls, file servers and business critical application servers. The founding lead consultant has 12 years of experience with primary strengths in networking, IT security, Microsoft products and four years of experience focusing on HIPAA compliance. The second lead consultant has 20 years of experience with primary strengths in UNIX administration, web development, and technical infrastructure design and is currently a certified Paralegal in Texas. The administrative lead spent the majority of her career selling DEC and later Compaq mainframe systems to large oil firms. The technicians provide standard services and support as directed by the two lead consultants and are responsible for ongoing maintenance. One of the technicians previously worked as a nurse for a large hospital before changing careers and joining Circron three years ago. Circron was originally an LLC, but growth needs have required reorganizing into a C Corporation. Fortunately, being based in Texas has limited the additional costs associated with this change in status due to lack of state taxes.

## *Target Client Base*

While Circron's clientele include both medical and legal firms, Circron is currently focused on growing their medical business. With HIPAA legislation, there has been an increase in demand for consulting services, especially for small to medium companies that are targeted by Circron. The administrative lead has focused her attention on private practices, clearinghouses, third party administrators and other organizations that can be classified as a Covered Entity under HIPAA legislation. The smallest customer in this target market is a five-employee dentist office and the largest is a 500-employee third party administrator.

## *General Methodology*

Circron distinguishes itself from competitors through involvement in the industry and certification programs. Employees are encouraged to pursue certifications on their own time through a bonus incentive program. A company library of technical books is provided to all employees and new books are purchased, within reason, upon request. If an employee is able to find a way to pay for a certification class, whether through volunteering at SANS, from their own money or other methods, they are granted the time to do the class and Circron will provide airfare, hotel


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and a daily stipend to adequately cover travel expenses once per year. This offer is dependant upon scheduling in advance in order to manage the timing of projects with clients. Certification exams are covered by Circron, provided that the test is passed. All technical personnel are tasked with writing a published article or book review for at least one trade magazine each year with an incentive program to reward employees who publish more than three articles in a year.

Each employee is expected to participate as an active member in at least one professional organization. This includes ISSA, AITP, Infragard, Techxans, ANIA, AMIA and the Houston Bar Association. Other professional organizations can be substituted, but it must be submitted for review and approval. The goal is to cover memberships with a representative sample of legal, medical, computing and IT security. The networking that is established in these associations is used as the primary source from which leads are taken. Employees are trained by the administrative lead on how to network and to identify potential opportunities. Circron pays membership dues and meeting fees. To encourage the sales role that employees take as they participate in these organizations, commissions are awarded to any employee that identifies a successful opportunity to the administrative lead.

While a substantial amount of revenue is generated from one-time projects, the focus remains on signing support agreements with three or more year terms in order to establish a dependable source of ongoing income. Approximately 75% of all one-time projects end with some type of ongoing support agreement that provides a monthly source of revenue, however small. This provides the “bread and butter” that helps Circron to survive when the larger projects are light. Technical employees are paid a base salary plus bonuses from the above incentive programs. Additional overtime and holiday pay is given as the situation warrants. The administrative lead generates the vast majority of her salary from commissions, but is also given a small base salary to cover the non-sales functions that she fulfills.

Circron has established a partner relationship with one of its longest standing clients. This partnership is with a law firm who is familiar with regulatory compliance needs. Circron barters its services in exchange for meeting the technical needs of the law office. In exchange, Circron receives legal counsel and other required legal work, such as contract reviews. This partnership is predominantly leveraged with regards to HIPAA related projects as Circron refers any necessary legal work and often receives referrals to perform technical work towards HIPAA compliance. It is clear that this relationship produces a potential environment for a conflict of interest if legal issues arise between Circron and a mutual client with the partnered law firm. However, this has been more beneficial than damaging as the partner has been called in as a mutually trusted third party arbiter; hence producing expedient and low impact resolution to conflicts.


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## *GIAC Enterprises*

GIAC Enterprises is a small family practice clinic consisting for three doctors, six nurses and one assistant who schedules appointments, manages the computers, maintains records and maintains supplies. They are currently located in a single office park, but have plans of expanding to a second location with three years.

GIAC Enterprises has formally implemented compliance mechanisms for the HIPAA Privacy Rule, but have not reviewed their compliance with the HIPAA Security Rule, which unquestionably applies to them. Their infrastructure consists of a claim transaction system, medical records database, scheduling application and accounting software. There are three nurses' workstations for records access, a Nokia IP40 firewall with permanent Internet connection, wireless tablet PCs used by the doctors, a system dedicated for the office assistant and two servers (one running Unix and the other a Windows 2000 Server).

GIAC Enterprises is seeking a GAP Analysis and remediation plan for the HIPAA Security Rule.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

# Part 2: Proposal and Pitch

## *Proposal*

### Cover Letter/Executive Summary

# Circron Consulting Corporation

September 14, 2004

GIAC Enterprises
ATTN: Mrs. Jane Receptionist
65432 Medical Row
Houston, TX 77654

Dear Mrs. Receptionist:

This document is in follow-up to our discussion about your HIPAA Compliance needs. As you may recall, Mr. Lawyer has been a client of Circron for six years and gave you our contact information when he provided assistance with meeting these federal regulations. We believe we are uniquely positioned to provide the best service for this project.

Circron has focused a lot of effort on providing assistance to small and medium practices, such as GIAC Enterprises, with their HIPAA compliance needs. We know that your primary business is in providing care to your patients. We can help you meet the HIPAA requirements in as economical and expedient manner as possible so that you can focus on your core business. Towards this goal, we have managed to employ one of the co-authors of HIPAA Security Implementation Step by Step Guide published by SANS Press, in addition to another employee who is a former nurse. We have also obtained individual HIPAA certifications from two separate organizations to help ensure that our staff is knowledgeable and capable of understanding your needs.

We hope that this proposal will meet your expectations. If you need adjustments made to the project scope or to understand anything being presented, please feel free to contact me via email or phone at any time. Thank you for your consideration.

Sincerely,

<signed by hand>

Joselyn Sales Admin
Project Coordinator
713-555-5555
jsadmin@circronconsulting.com

***Circron Consulting***
*Keeping your business running around the clock*



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## Proposal/Scope of Work

| **Circron Consulting**<br>**Scope of Work** | **GIAC Enterprises HIPAA Gap Analysis and Remediation Plan**<br>Prepared for GIAC Enterprises |
|---|---|

## Contacts

| | | | |
|---|---|---|---|
| **Company Name** | GIAC Enterprises | | |
| **Customer Contact** | Jane Receptionist | 281-555-1234 | jreceptionist@giacenterprises.com |
| **Circron Account Manager** | Joselyn Admin | 713-555-5555 | jsadmin@circronconsulting.com |
| **Circron Project Lead** | Brian Granier | 713-555-5566 | bgranier@circronconsulting.com |

## Summary

| | | | |
|---|---|---|---|
| **SOW Creation Date** | 8/2/04 | **Project Name** | GE – HIPAA Gap & Rem. Plan |
| **Estimated Billable Hours** | 76 | **Start Date** | TBD |
| **Offer ID** | GE 19022 | **Project Type** | Audit |

## Scope Definition

| | |
|---|---|
| **Scope Definition** | Circron Consulting will perform a HIPAA Gap Analysis based specifically against the Final Security Rule and create a remediation plan for GIAC Enterprises. |
| **Scope Inclusions** | Circron Consulting will perform the following duties during the course of this project:<br>• Interview staff to identify current compliance stance and related business goals<br>• Review existing policies and procedures with respect to HIPAA Security Rule Compliance<br>• Access and audit technical infrastructure details as it applies to HIPAA Security Rule compliance<br>• Analyze compliance gaps and determine possible remediation methods<br>• Provide a report that clearly identifies the findings and providing a written remediation plan for GIAC Enterprises<br>• Present the report to GIAC Enterprises upon completion |
| **Scope Exclusions** | Circron Consulting is not expecting to perform the following tasks within the scope of this project:<br>• Implement remediation plan<br>• Provide policies or procedures to meet compliance needs<br>• Perform Gap Analysis and remediation plan for HIPAA Privacy Rule or HIPAA Data Transaction and Code Set Standards<br>• Any tasks not specifically defined in this scope of work |



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## Expectations

| | |
|---|---|
| **Customer Expectations** | GIAC Enterprises is expected to provide the following resources:<br>• Make available staff for necessary interviews as specified in the scope of work<br>• Provide administrative access to technical infrastructure as is required to complete the technical audit<br>• Provide any and all policies and procedures related to this project<br>• Supply all hardware, software and licenses required to complete this project |
| **Circron Expectations** | Circron Consulting will perform the following activities:<br>• Prepare interviews with efficiency in mind to minimize the time needed of GIAC Enterprises staff<br>• Take precautions to avoid interfering with GIAC Enterprises normal work flow<br>• Provide knowledge transfer during the engagement |

## Project Team

| | |
|---|---|
| **Joselyn Sales Admin** | Joselyn joins Circron from project management and sales roles with leading oil industry firms in the Houston area. With 20 years of experience and an MBA from Rice University, she has made contacts with some of the most influential business professionals in the Houston area. In this project, her role is to ensure the timely execution of tasks and general project management responsibilities. |
| **Brian Granier** | Brian is the founder of Circron Consulting. As co-author to SANS HIPAA Step-by-Step Guide, he provides a knowledgeable skill-set towards HIPAA compliance objectives. He has achieved several high-level security certifications and is consistently published in industry magazines. He is responsible for creating the practical assignment for the GIAC GHSC certification program and was the first to achieve this certificate. Brian's role for this project is to take primary responsibility for gathering the information and producing the deliverable for this project. |
| **Nova Ustabe Nurse** | Nova previously worked at Large Houston Hospital as a Registered Nurse (RN). She has been with Circron Consulting for approximately three years, providing a unique perspective on how to meet the technical needs within the medical industry. She is currently Microsoft certified and in additional to her RN license, maintains a CHP (Certified HIPAA Professional) certification from HIPAA Academy. Nova's primary responsibility with this project is to provide assistance to Brian in the collection of information and to help establish the remediation plan with inside knowledge of small clinic operation in mind. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## Overview of Project Plan

| Task # | Description | Est. hours |
|---|---|---|
| | **PHASE I: Collection of Information** | |
| 1 | Perform interviews of staff | 12 |
| 2 | Gather and review existing policies and procedures | 10 |
| 3 | Perform audit of technical infrastructure | 12 |
| | **PHASE II: Gap Analysis Creation** | |
| 4 | Analyze gathered information | 16 |
| 5 | Create Gap Analysis Report | 8 |
| 6 | Deliver Gap Analysis in a live presentation | 4 |
| | **PHASE III: Remediation Plan** | |
| 7 | Discuss options to close the gaps identified in the Gap Analysis report | 8 |
| 8 | Assist client with making decisions on specific technologies to close gaps | 4 |
| 9 | Document remediation plan and provide written report | 2 |

| Estimated Duration | 4 Weeks | Estimated Hours | 76 Hours |
|---|---|---|---|

## Cost

| Item Description | Est. Hours | Unit Cost | Extended Cost |
|---|---|---|---|
| **Estimated Billable Hours** | 76 | $180 | $13680 |
| | | | |
| **TOTAL** | | | **$13680** |

## Terms and Conditions

- Quote is valid for 30 days from delivery
- All work is expected to be performed during normal workdays and hors (M-F 8am-5pm). Hours spent outside this time frame is billed at time and a half
- Upon acceptance, GIAC Enterprises will be expected to pay 30% of the estimated quote before any work begins. An additional 15% will be due upon completion of Phase I. An additional 15% will be due upon completion of Phase II. The remainder of the final amount due will be payable immediately upon completion of Phase III.
- This Scope of Work will be billed on a time and materials basis. While every effort has been made to estimate actual required work effort, it may take more time to complete this project. Circron will discuss with the client immediately if there is concern that the estimated hours will be exceeded to reach a mutual understanding on how to proceed.

_____ PO Number:_____ Date:_____
GIAC Enterprises Signature

_____ Date:_____
Circron Consulting Signature


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## *Pitch*

At first, it might seem strange that the proposal is addressed to the receptionist role position. However, this person is the decision maker for this proposal and is the primary contact as well. She also serves functionally as the office manager and fulfills technical duties for GIAC Enterprises. From conversations with the customer and with Mr. Lawyer, it is clear that the customer is very motivated to move quickly and that they understand the pending April deadlines for compliance for the Security Rule. We also know that the client has budgeted approximately $15,000 for the project. Joselyn Sales Admin has established a very strong relationship with the client and is taking a lead on closing the deal. Circron has the edge on winning this bid due to recommendations from Mr. Lawyer who is a personal friend of the primary doctor at the clinic.

To help sell this deal, Joselyn will be highlighting the industry publications and certifications that the team has obtained. Specifically, she will be pushing the SANS HIPAA Step by Step Guide that was co-authored by the lead consultant. When meeting with Jane Receptionist to deliver the proposal, she will bring a copy of that book and give it to the potential customer. This will help provide a tangible reminder of the project and of the lead consultant's skill-set. Normally, this type of gift is given after an engagement is signed or at the end of the project, but since there is a high expectation of winning the bid and we are trying to manage first impressions, the decision was made to take the risk of providing it up front.

Since the client will be looking for a remediation plan at the very end, Circron will be looking for ways to meet the compliance needs for GIAC Enterprise by providing ongoing service to offload IT services from Jane Receptionist by more knowledgeable professionals who can ensure ongoing compliance. In order to help win this ongoing business, Circron is going to ensure over-deliverance and will make every effort to come in under the estimated hours for the project.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

# Part 3: Project Performance

## *Project Plan*

### Overview

The high-level project plan has been provided in the scope of work. All of the information provided in this section is considered internal information for Circron Consulting as it involves proprietary methodology information. Please note that the hours projected on the project plan are estimates only. Circron employees will be strongly encouraged to try to complete the work in less time than allotted without sacrificing quality. This can assist with making time for any unexpected problems during the engagement that require more time than expected and will also assist in keeping the project on target and aid in the overall objective of having a good first impression in order to win future business.

Immovable scheduled targets have been identified for Friday during each week of the engagement. This date is selected as the small clinic is closed on Friday's and the client has agreed to make this day generally available for conducting meetings and interviews with GIAC Enterprises staff. This constraint has made the first Friday of the project the date for staff interviews. The second Friday is reserved for any additional information gathering that is necessary as part of Phase I. The third Friday is reserved for the delivery of the Gap Analysis report and for working with client to explain what options are available to close the gaps and identifying the solutions that GIAC Enterprises wants to select. The fourth Friday is scheduled for the close of the project and is the date scheduled for delivery of the final Remediation plan. All of the other tasks related to this project will be scheduled around these fixed milestones. Other days during the week will permit Circron Consulting unrestricted access to GIAC Enterprise employees between 8 and 9 am. Other time needed during the day will be on a limited basis. As a result, Circron has identified that it would be ideal to begin the project on the first Friday.

### Objectives

In order to help keep the project on target, the following objectives have been created for internal use:

Phase I:

- Obtain all information possible to be able to perform a thorough analysis of GIAC Enterprises current compliance stance with regard to the HIPAA Security Rule.
- Keep the client informed of what information is being collected and why in order to foster knowledge transfer and to ensure that the client continues to perceive that we are staying on task.


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Do not be negative about weaknesses found. Only collect the data without judgment.
- Be thorough.

Phase II:

- Ensure that all identified gaps are measured against HIPAA regulations and not necessarily against personal preference or different best practice models.
- Provide actual legislation text and review all public comments on each requirement before finalizing analysis for each Implementation Specification.
- Create the Gap Analysis report in a clearly organized, understandable and professional manner.
- Deliver on time!

Phase III:

- Be able to identify and discuss the pros and cons of at least three possible solutions for each problem being solved.
- Be prepared to give a professional opinion on which option Circron consulting will recommend.
- Look for opportunities where Circron can obtain ongoing business that won't cost the client more than they'd be paying for alternate solutions. Be ethical with this objective!
- Deliver on time!

The people who are identified with responsibilities in the following project plan are as follows:

Peter Lead Doctor (PLD): The owner and primary practitioner at GIAC Enterprises
Jane Receptionist (JR): Office Manager/Technical Lead and primary contact for GIAC Enterprises
Joselyn Sales Admin (JSA): As described in Scope of Work
Brian Granier (BG): As described in Scope of Work
Nova Ustabe Nurse (NUN): As described in Scope of Work

These acronyms will be used to refer to these individuals in the project plan sections listed below.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## Phase I

This phase is predominantly interested in the collection of information. As identified in the scope of work, this is done by interviewing the staff, gathering existing policies/procedures, and performing an audit of the technical infrastructure.

For the interview process, the team member selected to interview each of the two employees who will be involved in this assessment was done with an understanding of the personalities involved. Joselyn Sales Admin has identified that Jane Receptionist is a Type D personality and will work best with direct questions. Brian Granier is chosen to interview her, because of the two, he is better equipped to handle this personality type from past experience. Peter Lead Doctor, however, has been identified as a Type I personality. This is not surprising given the high percentage of this personality type in the medical industry. Nova Ustabe Nurse was selected to be his interviewer because she has developed exceptional skills at handling this personality type, likely as a result of her background as a nurse.

For the gathering of documentation, generically speaking, Nova Ustabe Nurse will be responsible for these task items. She is best equipped to navigate the clinic and to keep a low profile, again because of her experience as a nurse. This should help keep the client satisfied that there is minimal impact to their normal business practices. Part of the unwritten task that will be performed is for her to keep her eyes and ears open during this process to be able to identify areas where written policy/procedure are adhered to and where they differ from reality. While she is predominantly gathering data related to the administrative safeguards, she will also be paying attention to details associated with physical safeguards.

During the audit phase, Brian Granier's primary responsibility will be to assess the technical safeguards. The specific details of how to do this are not documented as they can change depending upon the environment. General processes have been identified as part of Circron's boiler plate HIPAA audit methodology, but each situation is unique and he is well equipped to determine what and how to evaluate the situation. He will also be keeping his eyes and ears open for difference between documented policy/procedures and reality and paying attention to each of the physical security related issues as well.

A more detailed breakout of the tasks to be performed during this portion of the project is provided on the following page:


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004,

As part of GIAC practical repository.

Author retains full rights.

| | Task Name | Duration | Start | Finish | Resource Names |
|---|---|---|---|---|---|
| 1 | **PHASE I: Collection of Information** | **7.13 days** | **Wed 9/1/04** | **Fri 9/10/04** | |
| 2 | Obtain sign-off and collect 30% | 0 days | Wed 9/1/04 | Wed 9/1/04 | JR,JSA |
| 3 | Kick-off Meeting | 1 hr | Fri 9/3/04 | Fri 9/3/04 | PLD,JR,JSA,NUN,BG - Lead |
| 4 | **Perform interviews of staff** | **1 day** | **Fri 9/3/04** | **Fri 9/3/04** | |
| 5 | Interview Peter Lead Doctor | 1 hr | Fri 9/3/04 | Fri 9/3/04 | NUN - Lead,BG |
| 6 | Interview Jane Receptionist | 2 hrs | Fri 9/3/04 | Fri 9/3/04 | BG - Lead,NUN |
| 7 | **Gather and review existing policies and procedures** | **0.13 days** | **Fri 9/3/04** | **Fri 9/3/04** | |
| 8 | **Obtain copy of HIPAA Privacy Rule documentation** | **0.05 days** | **Fri 9/3/04** | **Fri 9/3/04** | |
| 9 | Obtain Gap Analysis | 0.3 hrs | Fri 9/3/04 | Fri 9/3/04 | NUN,JR |
| 10 | Obtain Remediation Plan | 0.3 hrs | Fri 9/3/04 | Fri 9/3/04 | NUN,JR |
| 11 | Obtain related policies and procedures created as a result | 0.4 hrs | Fri 9/3/04 | Fri 9/3/04 | NUN,JR |
| 12 | **Obtain all other policies and procedures** | **0.13 days** | **Fri 9/3/04** | **Fri 9/3/04** | |
| 13 | Compare to list of Standards and Implemetation Specifications | 1 hr | Fri 9/3/04 | Fri 9/3/04 | BG,NUN - Lead |
| 14 | Followup requesting documents identified as missing | 1 hr | Fri 9/3/04 | Fri 9/3/04 | NUN |
| 15 | **Perform audit of technical infrastructure** | **2.25 days** | **Fri 9/3/04** | **Tue 9/7/04** | |
| 16 | Obtain or create network diagram | 2 hrs | Fri 9/3/04 | Fri 9/3/04 | BG |
| 17 | Obtain necesarry username and passwords | 0 days | Fri 9/3/04 | Fri 9/3/04 | BG |
| 18 | Review each Implementation Specification and check against environment | 10 hrs | Mon 9/6/04 | Tue 9/7/04 | BG - Lead,NUN |
| 19 | **Pre-assessment** | **0.38 days** | **Tue 9/7/04** | **Tue 9/7/04** | |
| 20 | Prior to analysis, assess apparently missing policies procedures | 1 hr | Tue 9/7/04 | Tue 9/7/04 | BG - Lead,NUN |
| 21 | Identify areas that appear have an unstated policy/procedure | 1 hr | Tue 9/7/04 | Tue 9/7/04 | BG |
| 22 | Identify areas where more information is needed | 3 hrs | Tue 9/7/04 | Tue 9/7/04 | BG |
| 23 | **Follow-up Interview** | **0.13 days** | **Fri 9/10/04** | **Fri 9/10/04** | |
| 24 | **Interview Jane Receptionist** | **0.13 days** | **Fri 9/10/04** | **Fri 9/10/04** | |
| 25 | Discuss missing policies and procedures | 0.5 hrs | Fri 9/10/04 | Fri 9/10/04 | BG,JR |
| 26 | Discuss unstated, but enforced policies | 0.5 hrs | Fri 9/10/04 | Fri 9/10/04 | BG,JR |
| 27 | Cover remaining unanswered questions | 1 hr | Fri 9/10/04 | Fri 9/10/04 | BG,JR |
| 28 | Obtain 15% | 0 days | Fri 9/10/04 | Fri 9/10/04 | JSA,JR |

## Phase II

This phase will mostly be performed off-site, if the client permits it. Since Circron has performed a large number of audits, there are a number of templates and processes that have been developed as part of Circron's intellectual property that makes this process very efficient.

Brian Granier is tasked with the creation of the Gap Analysis report. Since this is a relatively small client, there is not really a reason to divide this between him and Nova. By having just one author, it will be much easier to maintain consistency of style and to ensure that all of the appropriate areas are covered.

Nova Ustabe Nurse will be primarily responsible for prepared for Phase III. Since the target is to be able to move directly from the Gap Analysis presentation into working with the client to create a remediation plan that they are comfortable with, significant preparation will need to be performed in a short period of time. Since Brian will be busy creating the Gap Analysis report, this responsibility is assigned to Nova.

Note, while Jane Receptionist is the primary source of contact for this work and is the one who made the decision to hire Circron Consulting, Joselyn Sales Admin has been able to determine that the decisions for the remediation plan creation are expected to be made by Peter Lead Doctor. With Jane Receptionist, the options would have been more pointed and the delivery would be very strong on the recommendation side. Since Peter Lead Doctor is the target, this will be intentionally softened. The pros and cons for each solution will be provided along with estimations on pricing when appropriate. Recommendations will not be given on which way to go until asked, as this seems to be how Peter Lead Doctor likes to work in these types of situations. Circron will be prepared to make their recommendations and will be prepared to answer any questions asked and to support the opinions given.

Joselyn Sales Admin time is not billable. However, she is involved in reviewing the Gap Analysis plan as an effort to ensure the best possible first impressions with GIAC Enterprises in order to help with getting future business. Her attendance at the Gap Analysis presentation is towards this goal as well and so that she can be available to answer sales oriented questions during the discussion of remediation, since there is an expectation that Circron will be able to meet a large portion of their needs in this area.

A more detailed breakout of the tasks to be performed during this portion of the project is provided on the following page:


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004,

As part of GIAC practical repository.

Author retains full rights.

| | Task Name | Duration | Start | Finish | Resource Names |
|---|---|---|---|---|---|
| 29 | **PHASE II: Gap Analysis Creation** | **5 days?** | **Mon 9/13/04** | **Fri 9/17/04** | |
| 30 | **Analyze gathered information** | **1.88 days** | **Mon 9/13/04** | **Tue 9/14/04** | |
| 31 | **Assess each implementation specification individually** | **1.88 days** | **Mon 9/13/04** | **Tue 9/14/04** | |
| 32 | Identify if policy/procedure exists on paper | 1 hr | Mon 9/13/04 | Mon 9/13/04 | BG,NUN |
| 33 | If not, identify if de facto policy/procedure exists | 2 hrs | Mon 9/13/04 | Mon 9/13/04 | BG,NUN |
| 34 | Identify if any steps have been taken towards compliance | 2 hrs | Mon 9/13/04 | Mon 9/13/04 | BG,NUN |
| 35 | Identify if a gap exists | 4 hrs | Mon 9/13/04 | Mon 9/13/04 | BG,NUN |
| 36 | Document each finding seperately | 7 hrs | Tue 9/14/04 | Tue 9/14/04 | BG,NUN |
| 37 | **Create Gap Analysis Report** | **1.25 days** | **Wed 9/15/04** | **Thu 9/16/04** | |
| 38 | Gather all documentation collected | 1 hr | Wed 9/15/04 | Wed 9/15/04 | BG |
| 39 | Create a spreadsheet giving a quickview of compliance stance | 1 hr | Wed 9/15/04 | Wed 9/15/04 | BG |
| 40 | Organize and format documentation from analysis phase | 2 hrs | Wed 9/15/04 | Wed 9/15/04 | BG |
| 41 | Fill in any missing sections in the report | 2 hrs | Wed 9/15/04 | Wed 9/15/04 | BG |
| 42 | Submit for editting to Nova Ustabe Nurse | 2 hrs | Thu 9/16/04 | Thu 9/16/04 | NUN |
| 43 | Submit for editting to Joselyn Sales Admin | 2 hrs | Thu 9/16/04 | Thu 9/16/04 | JSA |
| 44 | **Prepare for remediation plan discussion** | **1.25 days** | **Wed 9/15/04** | **Thu 9/16/04** | |
| 45 | Identify areas where an identified Gap exists | 1 hr | Wed 9/15/04 | Wed 9/15/04 | BG |
| 46 | When appropriate, identify 3 potential solutions | 2 hrs | Wed 9/15/04 | Wed 9/15/04 | NUN |
| 47 | Research the pros and cons for each solution | 5 hrs | Wed 9/15/04 | Wed 9/15/04 | NUN |
| 48 | Prepare notes on findings | 2 hrs | Thu 9/16/04 | Thu 9/16/04 | NUN |
| 49 | Distribute notes internally | 0 days | Thu 9/16/04 | Thu 9/16/04 | NUN |
| 50 | **Deliver Gap Analysis in a Live Presentation** | **2.25 days** | **Wed 9/15/04** | **Fri 9/17/04** | |
| 51 | Schedule meeting | 0 days | Wed 9/15/04 | Wed 9/15/04 | JSA,JR |
| 52 | Deliver presentation | 2 hrs | Fri 9/17/04 | Fri 9/17/04 | PLD,JR,JSA,BG - Lead,NUN |
| 53 | Obtain 15% | 1 day? | Fri 9/17/04 | Fri 9/17/04 | JSA,JR |

## Phase III

Phase III will be performed in a very short period of time. Since the delivery of the Gap Analysis will occur simultaneous with moving forward to identify the methods to close the gaps, the preparatory work for this performed during Phase II will be very important to the success of this Phase. To a very large extent, this portion of a Gap Analysis/Remediation Plan has become very routine. From previous engagements, Circron has spent a lot of time researching different solutions to meet clients HIPAA compliance needs and have rehearsed the discussions of the pros and cons of each solution on many occasions. To this extent, Circron's role is predominantly to identify possibilities and to assist the client towards making a decision to meet their budgetary and compliance concerns.

With respect to administrative safeguard compliance issues, Nova Ustabe Nurse will take the lead on these discussions. For physical and technical safeguard issues, Brian Granier will take the lead. For discussions on how Circron would price potential future engagements to help close the gap, Joselyn Sales Admin will take the lead.

The end date of Phase III is scheduled for a date earlier than the agreed upon due date. This is to help facilitate the under-promise/over-deliver principle. It also gives time to deal with unexpected issues that might take more time than was expected.

A more detailed breakout of the tasks to be performed during this portion of the project is provided on the following page:

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004,

| | Task Name | Duration | Start | Finish | Resource Names |
|---|---|---|---|---|---|
| 54 | **PHASE III: Remediation Plan** | **2 days** | **Fri 9/17/04** | **Tue 9/21/04** | |
| 55 | **Discuss options to close the gaps** | **0.25 days** | **Fri 9/17/04** | **Fri 9/17/04** | |
| 56 | Discuss each gap one at a time | 1 hr | Fri 9/17/04 | Fri 9/17/04 | PLD,JR,JSA,BG - Lead,NUN |
| 57 | Using notes, offer suggestions for implementation | 1 hr | Fri 9/17/04 | Fri 9/17/04 | PLD,JR,JSA,BG - Lead,NUN |
| 58 | Answer questions the client has about each solution | 2 hrs | Fri 9/17/04 | Fri 9/17/04 | PLD,JR,JSA,BG - Lead,NUN |
| 59 | **Assist client with making decisions to close gaps** | **0.13 days** | **Fri 9/17/04** | **Fri 9/17/04** | |
| 60 | Record clients decisions | 1 hr | Fri 9/17/04 | Fri 9/17/04 | BG,NUN - Lead |
| 61 | **Document remediation plan and provide written report** | **1 day** | **Mon 9/20/04** | **Tue 9/21/04** | |
| 62 | Create formal document identifying customers selected solution | 1 hr | Mon 9/20/04 | Mon 9/20/04 | NUN |
| 63 | Provide report to client | 0 days | Tue 9/21/04 | Tue 9/21/04 | JSA |
| 64 | Obtain 40% | 0 days | Tue 9/21/04 | Tue 9/21/04 | JSA,JR |

As part of GIAC practical repository.

Author retains full rights.



04, Author retains full rights.

## Budget Details – Estimate

This budget estimate is a tool used by Circron prior to beginning work on a project to ensure that the engagement will result in profit. Once the detailed project plan has been made, as provided above, this estimate is generated based upon the information provided in that document. Therefore, making the project plan as accurate as possible is crucial to ensuring that engagement remains profitable.

This budget estimate is not meant to be used as an accounting tool to record actual flows of cash. As a result, this estimation does not cover the overhead expenses associated with being in business, such as the partial salary paid to Joselyn Sales Admin, software and equipment purchased directly by Circron, bonus/incentive programs, marketing, etc…

| | |
|---|---|
| **Gross Income:** | |
| Estimated 76 hours @ $180/hour | $13,680 |
| **Expenses:** | |
| HIPAA Step by Step Guide – SANS Press | ($60) |
| Sales related expenses (travel/lunch) | ($100) |
| Per diem granted to consultants on site $25/ estimated @ 10 total days from plan * | ($250) |
| **Total:** | **($410)** |
| **Compensation:** | |
| Joselyn Sales Admin ~8% commission | ($1,095) |
| Brian Granier $100/hour estimated @ 54 hours ** | ($5,400) |
| Nova Ustabe Nurse $60/hour estimated @ 53 hours ** | ($3,180) |
| **Total:** | ($9,675) |
| | |
| **Net Profit:** | $3,595 |

* Note that since the client is local, the per diem expense is lower than it would be in other situations. Per Diems are awarded to billable consultants only for days on which they spend more than 4 hours at the customer site. Mileage and food expenses are all expected to be covered by this amount.

** For budgeting the compensation, it is intentional that the number of hours estimated for compensation to the employees does not necessarily match the number of hours quoted to the client. There have been cases where hours spent by a consultant are billable to the Circron, but may not necessarily be billable to the client. Additionally, by having this extra room for budget estimations, it can be possible to cover additional time spent without eating into the profits if the process goes just a little slower than it should. This can make it possible to still deliver at the original quoted price even if the engagement takes more hours than expected. When building the budget estimate, Circron will use the project plan created and assume the estimated hours for each task are accurate and that each team member on the task will be spending 100% of the estimated time for that step. This practice has worked well for Circron, but may not be advisable for others. It has usually resulted in a higher net profit than budgeted.


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## *Meeting/Interview Facilitation*

The organization of this section is based upon the flow for the interview and discusses specifically the initial interviews that will be conducted of Peter Lead Doctor and Jane Receptionist. Note that Peter Lead Doctor has been identified as a type I personality and Nova Jane Receptionist as a type D. These factors directly effect the prepared organization for each of these interviews. This section will cover the major aspects of the planned interview process and provide some sample questions that could be asked during each portion of the interview.

### Introduction

The introduction of the interview is going to set the tone for the rest of the conversation. The purpose of this phase is to introduce who the interviewee is and what the goal of the interview is to be.

**Peter Lead Doctor Introduction:** As a type I personality, it's usually best to open with some small talk and be personable. Let the client warm up to the conversation before diving into the business purpose for being there. Try to ask an open-ended question and avoid anything that could be politically or emotionally charged.

Question to ask: I understand you're a big Jeopardy fan. What do you think of Ken Jennings and his winning streak?

Question **not** to ask: I've been hearing a lot of stories lately about human cloning, what's your take on the subject?

Once enough small talk has occurred and Peter begins to open up, start into the purpose of the introduction. Consider using his desire for being recognized for doing something good to play on the typical type I motivational factors, but don't make things up either when doing it:

Question to ask: So I understand that you've been very helpful to Jane as she's taken on the responsibility of implementing HIPAA Privacy Rule requirements. She's mentioned how appreciative she is to have your support to make that a success. As you are aware, she's asked us to help continue the effort by looking at GIAC Enterprises through the eyes of the HIPAA Security Rule. You may have seen this high-level project plan (sliding the short project plan from the scope of work to him). Was there anything you'd like to understand about the project before we begin?

**Jane Receptionist Introduction:** As a type D personality, Jane is ready to get moving and is very task and accomplishment oriented. For this interview, cut the small talk and get to the point. Stay focused on the business at hand.


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Question to ask: Jane, it's a pleasure to meet you. I'm Brian. I will be taking the lead responsibility for providing the Gap Analysis and Remediation plan. I know you've been given the high-level overview of the steps we will be taken (noticing it in front of her). Do you have any questions?

Question **not** to ask: See the more longwinded question asked of Peter Lead Doctor.

## Identifying Keys to Success

The purpose of this phase of the interview is to identify what the client really wants to have. In this case, we know they want a Gap Analysis and Remediation plan, so we will be focused on how they want it delivered, if there are any specific areas that they wanted highlighted over another and generally how the client will identify the engagement as successful.

**Peter Lead Doctor IKS:**
Question to ask: We want to make sure that what we provide for you is the way you want it and that your employees can use. I understand that you selected XYZ Consulting firm when you reviewed your HIPAA Privacy compliance stance. How did that go? What did they do well and what could have been done better?

Be careful with this question. The goal is to find out what it will take for you to succeed. Not to discuss the negative aspects of XYZ Consulting who may or may not be a competitor. For example:

Question **not** to ask: I heard you did your HIPAA Privacy Rule Gap Analysis with XYZ Consulting. I've heard some bad things about them. What was your experience?

**Jane Receptionist IKS:**
Question to ask: I know you did a HIPAA Privacy Gap Analysis with XYZ Consulting. How did that go? What did they do well and what have been done better?

Question to ask: We want to make sure that the reports we provide are in a format that works for you and that you can be happy with. I have brought a couple of samples from previous engagements with permission from our clients and that have been altered so as not to reveal their identity. Would you mind looking them over and giving some feedback on the general format of the presentation and let me know any areas you want brought out?

Follow-up Question to ask: Great. Can we go over it now?

## Information Gathering

This portion of the interview is the primary purpose of the interview. In this case it is to begin the process of gathering data for the HIPAA Gap Analysis. In this


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

case, questions covering each of the three areas (administrative, physical and technical) will be asked. A focus will be on what is a documented policy or procedure vs. de facto policy or procedure. Also look for hot buttons the client might have in particular areas. In some cases there may be agendas or ulterior motives affecting their opinion. If these can be identified and incorporated into the project without defeating the purpose of the project or causing scope creep, it will help in the long run for the acceptance of the final work product.

**Peter Lead Doctor and Jane Receptionist IG:**
Question to ask: Have you implemented any type of virus filtering for your workstations?

Follow-up Question to ask: Can you disable it if is causing your system to run slow?

This follow-up question is key. It goes to two different issues. First is the administrative capability for users to disable anti-virus. The second is to identify if they've been educated about how important it is.

Question **not** to ask: I can't believe you chose abc anti-virus solution. They have the worst reputation in the industry. Have you had a lot of viruses get through?

Don't ask this question. It's judgmental. The goal is gather data, not to criticize the client for what is, that is saved for being presented in a **constructive** way in the Gap Analysis report if it is appropriate. By being judgmental, you are also reducing the likelihood of getting thorough and accurate information.

## Conclusion and Recap:

This section of the interview is to provide time for the client to unload anything else they might have or ask any questions. First, try to ask as open-ended a question as possible in order to get the client to talk. If you can get them talking and getting everything out that they have to say, there can be some useful information. Be careful of clients who have too much to say and try to keep things on track, but allow for **some** room to stray. Once this is done, recap the meeting. In some cases, it's better to do this later in an email. Sometimes it's better to do it at the meeting directly. This is a choice of personal style and is impacted by the type of client environment that is being dealt with.

**Peter Lead Doctor and Jane Receptionist CR:**
Question to ask: Great. Well those are the questions I have at this time. Are there any areas we didn't talk about that you would like to address or any additional information you have that might be helpful?

Question **not** to ask: Great. Well I think we're done here. Thanks for your time. Where's the door?


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

And for the recap:
Question to ask: Okay. There's a lot of information here that needs to be organized. Would it be okay if I put together an email documenting what we've discussed so that you can review it to identify any areas that I may have misunderstood?

## *Potential Pitfalls*

**Project behind schedule**
With almost every project, there's a risk of getting behind schedule. This is especially critical in this project since it's a relatively short time frame and the events scheduled for Friday's are fixed. While the documented project plan is not meant to be set in stone, it is intended to be used as a guideline. If the project is falling behind the scheduled events in the project plan, then quick action will need to be taken. Most likely, this action will be simply working longer days by doing work at home to catch up. It's not expected that bringing another consultant on the job would work, since the time frame is short and it would take time for the new person on the project to catch up.

**Deliverable doesn't meet clients' expectations**
Again, this is a risk with basically all projects. This potential pitfall is specifically addressed during the initial interviews with questions that probe at how the project will be gauged a success. To help avoid this disaster, it is important to pay attention to the style of the documents collected that were created by the client, especially the ones that will be determining the success of the project.

## *Value Add – Ongoing Business*

While this project is specifically targeted at the HIPAA Security Rule, we will also be reviewing the documents created by/for the client as it pertains to the HIPAA Privacy Rule. Since Circron is knowledgeable in these regulations as well and will be reading these documents anyways, it would not take much additional effort to identify potential short falls or to provide a validation that GIAC Enterprises HIPAA Privacy compliance is on track. Nothing formal is expected to be put together towards this end, but it can be used in conversation with GIAC Enterprises to give them additional information and feedback on their overall compliance stance.

Additionally, it is expected that GIAC Enterprises will be periodically audited as per the requirements of HIPAA. To help reduce the ongoing cost of being audited, the deliverable documents will be prepared with this in mind. Towards this end, copies of all documents produced by GIAC Enterprises and identified as part of the HIPAA Security Rule compliance stance will be gathered in one place and provided to GIAC Enterprises. This really is not anything different than would be done anyways. In this case the value-add is one of perception. By selling the


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

collection of information as a workbook as a tool for future auditors, there may be a perception of added value that already exists anyways.

With respect to additional work opportunities, there are many areas that Circron can provide follow on projects. Since the point of this project is to identify what actions need to be taken to comply with HIPAA regulations, Circron can position themselves as an obvious choice for the implementation of these tasks. Circron strives to identify and win long-term contracts to help ensure the ongoing success of the business. By understanding the technical environment and building the client relationship, GIAC Enterprises can likely fit well within this business objective.

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

# Part 4: Final Deliverables

## *Section A*

Note that this deliverable is made for a gap analysis that was never actually performed as this is a theoretical engagement. This has resulted in less than thorough coverage in this example deliverable. Typically, during a Gap Analysis of any kind, it is important to be as specific as possible about the environment. Details such as software applications and versions, system names and functions, policies and procedures reviewed, interviews conducted, etc… should all be included with the "current state assessment" information. The process of going through a Gap Analysis will reveal much more information than is available in this sample deliverable. However, the general flow and organization of the document demonstrates an appropriate flow for a HIPAA Security Rule Gap Analysis. Note that the scope of work calls for both a Gap Analysis report and a Remediation plan. While remediation options are given with this report, the Remediation plan for this engagement is intended to identify specific tasks and technologies to close the gaps instead of a general explanation of what the task goals need to be as shown in the Gap Analysis. In this sense the "Remediation plan" is really more of a task identification and project management process. The Remediation plan is not provided in this practical.

---

### Executive Summary

The following document provides a Gap Analysis performed by Circron Consulting for GIAC Enterprises with specific focus on the HIPAA Security Rule federal regulations.

GIAC Enterprises is well positioned to meet the regulatory compliance issues. Documentation provided related to the compliance process with the HIPAA Privacy Rule and the resulting changes made to the organization in a timely manner demonstrated healthy business processes that will facilitate the additional changes that are identified in this GAP Analysis.

In this document, a summarization of findings will be provided, followed by a more detailed explanation for each individual implementation specification. Finally, documents collected by Circron Consulting are provided in the appendices in order to be useful for future compliance auditing needs.

After GIAC Enterprises moves forward, it will be necessary to be proactive with closing the gaps discovered. Circron is prepared to continue to work with GIAC Enterprises to meet their compliance needs. It would be advisable to share this report with legal counsel. This can help to ensure that the findings provided by Circron are legally accurate and could potential protect this report from being a


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

legally discoverable document as it could be considered attorney/client privileged information.[1]

After the remediation process has been completed, it would be advisable to immediately proceed with a follow-up audit to ensure that the tasks as implemented closed the gaps as expected. Finally, all appropriate procedures, documents and tasks should be shared with legal counsel to ensure that they meet the regulatory compliance requirements. It is important to understand that the security related issues identified in this document and the Security Rule in general are addressed through an ongoing process and should not be expected to be completed once and then forgotten. Fortunately, through ongoing auditing requirements written into the Security Rule, this cyclical process will be built into GIAC Enterprises compliance strategy.

Circron Consulting would like to thank you for your business. We look forward to continue working with you on your compliance and general information technology and security needs.

## Summary of Results

The following table provides a high level review of the HIPAA Security Rule standards and general compliance stance. This table was modeled after the Gap Analysis table provided in the HIPAA Security Implementation: Step by Step Guide p 96. Specific details related to each implementation specification follow afterwards.

[1] This is currently a legally untested theory. Consult with legal counsel for details.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| Gap Analysis / Remediation Categories — WBS Element | | | Security Management Program (WBS 1.0) | Business Continuity & Disaster Recovery (WBS 2.0) | Policies and Procedures (WBS 3.0) | Human Resources Procedures (WBS 4.0) | Business Associated Agreements (WBS 5.0) | Training/Awareness (WS 6.0) | Technical Architecture (WBS 7.0) | Evaluation (WBS 8.0) | System/Network Management (WS 9.0) | User Management (WBS 10.0) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Rule/Section** | | **Gap** | | | | | | | | | | |
| **Administrative Safeguards** | | | | | | | | | | | | |
| 164.308(a)(1) | Security Management Process | ❖ | ✓ | | ✓ | ✓ | | | | | | |
| 164.308(a)(2) | Assigned Security Responsibility | ❍ | | | | ✓ | | | | | | |
| 164.308(a)(3) | Workforce Security | ❖ | ✓ | | ✓ | ✓ | | | | | | |
| 164.308(a)(4) | Information Access Management | ❖ | ✓ | | ✓ | | | | | | | ✓ |
| 164.308(a)(5) | Security Awareness and Training | ❖ | ✓ | | ✓ | | | ✓ | | | | ✓ |
| 164.308(a)(6) | Security Incident Procedures | ❍ | | | | | | | | | | |
| 164.308(a)(7) | Contingency Plan | ❖ | | ✓ | ✓ | | | ✓ | | | | |
| 164.308(a)(8) | Evaluation | ❖ | ✓ | | ✓ | | | | | ✓ | | |
| 164.309(b)(1) | Business Associates Contracts | ● | | | | | ✓ | | | | | |
| **Physical Safeguards** | | | | | | | | | | | | |
| 164.310(a) | Facility Access Control | ❖ | ✓ | ✓ | ✓ | | | ✓ | | | | |
| 164.310(b) | Workstation Use | ● | | | ✓ | | | | | | | ✓ |
| 164.310(c) | Workstation Security | ● | | | ✓ | | | | | | | ✓ |
| 164.310(d) | Device and Media Controls | ❍ | | | | | | | | | | |
| **Technical Safeguards** | | | | | | | | | | | | |
| 164.312(a) | Access Controls | ❖ | | | | | | | ✓ | | | ✓ |
| 164.312(b) | Audit Controls | ❍ | | | | | | | | | | |
| 164.312(c) | Integrity | ❖ | | | | | | | ✓ | | | |
| 164.312(d) | Person or Entity Authentication | ❖ | | | | | | | ✓ | | | |
| 164.312(e) | Transmission Security | ❍ | | | | | | | | | | |

● = Full Compliance, ❖ = Partial Compliance, ❍ = No Compliance, **N/A** = Not Applicable

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following table provides an explanation of the WBSAD categories used in the summarization table above. This table was taken from the HIPAA Security Implementation: Step by Step Guide p. 84-86:

| WBS Element | Remediation Option | WBS Activity Description (Brief) |
|---|---|---|
| 1 | **Security Management Program** | Formal and central management structure that creates, administers, and oversees security related policies and procedures to ensure the prevention, detection, containment, and correction of security breaches. |
| 2 | **Business Continuity Planning and Disaster Recovery** | Contingency planning to respond to a system emergency or disaster. Plans must be formally documented and periodically tested. |
| 3 | **Policies and Procedures** | An organizational framework that establishes needed levels of information security and privacy to achieve the desired confidentiality goals. |
| 4 | **Human Resource Policies and Procedures** | Personnel security and other security related aspects of dealing with employees. |
| 5 | **Business Associate Agreements** | Contract between two business partners for the electronic exchange or handling of data, protecting the integrity and confidentiality of the data exchanged or handled. |
| 6 | **Security Training and Awareness** | Education of the entity workforce regarding security and the reinforcement of that education through ongoing reminders to create security awareness as part of the daily responsibilities in the organization. |
| 7 | **System/Network Technical Architecture** | Standards based architecture that addresses security issues and mitigates risk while meeting entity business and functional needs and requirements. |
| 8 | **Evaluation** | Technical evaluation to establish the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. |
| 9 | **System / Network Management & Administration** | Standardized functions and services standardized applied uniformly throughout the organization, centrally managed, and support to capacity planning and management operations. |
| 10 | **User Management, Support and Outreach** | Management and support of the end-user environment, incorporating security requirements into the entities IT support structure, such as through user interactions with the helpdesk and online knowledge bases. |

## Administrative Safeguards: Details

The following sections provide the actual text from the Final Security Rule, available at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp

After each specific subsection is a table providing the information collected by Circron Consulting, Gap Analysis statement, and remediation options. The format for the presentation of this information comes from HIPAA Security Implementation: Step by Step Guide p 94.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

**164.308(a)(1)(i) Standard: Security management process**. Implement policies and procedures to prevent, detect, contain, and correct security violations.

**(A) Risk analysis (Required)**. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| A Risk Analysis was performed as a result of the HIPAA Privacy Rule Gap Analysis.<br><br>The Risk Analysis covered all of the details appropriate for both the Privacy and Security Rule. See Appendix A for the Risk Analysis Report. | Policies and Procedures have not been implemented to ensure that the risk analysis is performed on a periodic basis or otherwise kept updated. | Establish and implement a policy for regularly scheduled intervals to review, renew and maintain the Risk Analysis Report at least on a yearly basis. |

**(B) Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec. 164.306(a).

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Steps necessary to reduce risks were identified in the Risk Analysis that was performed and provided in Appendix A. Upon reviewing the items identified and evaluating the remediation steps taken by GIAC Enterprises, there has been significant progress in this area.<br><br>However, the report identified a few remediation steps that have not yet been implemented. | Items detailed in the remediation plan attached to Appendix A.<br><br>HR documents do not reflect an assignment of duty to ensure ongoing compliance with this implementation specification. | The remaining remediation steps identified in the attached Risk Analysis needs to be addressed. Along with the Risk Analysis requirement of both the Privacy and Security Rule, an ongoing risk management routine needs to be written in policy format.<br><br>Ensure an assignment of responsibility for compliance with this Implementation Specification in either the implemented policy or job descriptions. |

**(C) Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| | | |



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| Current HR documents reflect sanction policies for the HIPAA Privacy Rule.<br><br>The sanctions are reasonable.<br><br>The sanction policy section of the employee manual can be found at Appendix B. | HR documentation does not extend these sanctions to employees violating HIPAA Security Rules. | Modify HR policies to include the HIPAA Security Rule in addition to Privacy Rule in its sanction policy. |

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

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| System auditing parameters for all systems are in their default configuration. No policies or procedures exist to review logs and this task is currently not part of any job description at GIAC Enterprises. | This Implementation Specification has not been addressed in any manner.<br><br>Technical logging and auditing are inadequate to properly track events that should be reviewed. | GIAC Enterprises can choose to train an internal employee to comply with this Implementation Specification. Alternatively, this task can be outsourced to a third party contractor.<br><br>Systems need to be configured to log meaningful information to provide adequate information and to be able to identify potential problems that need to be investigated.<br><br>Policies and procedures need to be authored explaining how GIAC Enterprises plans to address this requirement. |

**(2) Standard: Assigned security responsibility.** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has identified Jane Receptionist as responsible for making all HIPAA related policies and procedures. She is also identified as the HIPAA Privacy Officer. | No one is identified as the HIPAA Security Officer.<br><br>When assigning responsibility for a task, it is generally better to assign the responsibility to a job role instead of a person by name. | Identify responsibility for HIPAA Privacy Officer and HIPAA Security Officer by job role in HR documentation. Rather than defining this by policy, it would be more appropriate to identify it in the job description for the role |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| The policy identifying Jane Receptionist as the HIPAA Privacy officer and as the person responsible for HIPAA Policies and Procedures in any form has been attached in Appendix C. | | currently filled by Jane Receptionist. |

**(3)(i) Standard: Workforce security**. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

**(A) Authorization and/or supervision (Addressable)**. Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has identified in all employee job descriptions the need to access ePHI and has implemented an acceptable use policy. The acceptable use policy limits usage to be only for business purposes. Current policies do not permit medical records leaving GIAC Enterprises without specific approval by the HIPAA Privacy Officer. Exceptions are logged. Current exceptions include information sent to a clearinghouse with whom GIAC Enterprises has a Business Associate Agreement. This agreement has been reviews by Mr. Lawyer and is reported to be compliant with the Security Rule requirements for a Chain of Trust Partner Agreement.<br><br>See Appendix D for this Business Partner Agreement. | GIAC Enterprises is believed to be fully compliant with this Implementation Specification.<br><br>No gaps identified. | |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

**(B) Workforce clearance procedure (Addressable)**. Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Background checks are performed on each employee before they are hired. Job descriptions all identify a clear need to access ePHI. | GIAC Enterprises does not have a written policy that identifies its standard practice of conducting background checks. | Document policy on conducting background checks and include this in HR documentation. |

**(C) Termination procedures (Addressable)**. Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Termination procedures exist that identify handing over building access cards and keys. The procedures do not cover termination of access to network resources where ePHI are stored. It has been identified that for the two systems where ePHI are stored, only two separate account databases exist.<br><br>Appendix E contains the termination procedure. | Termination procedures need to identify termination or disabling of accounts that have access to ePHI. | Include disabling of accounts on the Windows network and Unix system located at GIAC Enterprises as part of the termination procedure. |

**(4)(i) Standard: Information access management**. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

**(A) Isolating health care clearinghouse functions (Required)**. If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| This implementation specification does not apply to GIAC Enterprises | N/A | N/A |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| | | |

**(B) Access authorization (Addressable)**. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Currently, any external access to PHI in any form (including ePHI) must be approved by the Privacy.<br><br>This policy can be found in Appendix F. | The policy needs to be strengthened to include the specific terminology used in this implementation specification. | Incorporate Security Rule terminology in the Access Authorization Policy. |

**(C) Access establishment and modification (Addressable)**. Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| No policies or procedures were found that address this Implementation Specification. | No steps have been taken either in documentation or practice to comply with this Implementation Specification | Document a policy and procedure to "establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process" containing ePHI. |

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

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

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises currently includes periodic reminders about compliance issues to the HIPAA Privacy Rule. Most notably, new employees must sign off on attendance to training on Privacy Rule issues semi-annually and are followed up with a quiz to ensure their understanding of | While the HIPAA Privacy Rule is trained appropriately with ongoing training, security issues are not included. Incorporate security specific reminders. | Include security reminders with the privacy rule training on a semi-annual basis.<br><br>Obtain more regular security awareness training to the HIPAA Security Officer. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| the material. | | |

**(B) Protection from malicious software (Addressable)**. Procedures for guarding against, detecting, and reporting malicious software.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has currently implemented a Linksys Cable/DSL router between them and the Internet. They are using McAfee antivirus solution. Virus definitions are kept up to date. Users are able to disable antivirus. No detection procedures or reporting procedures exist. No documentation exists identifying GIAC Enterprises compliance stance. | There is a lack of policy and procedures identifying compliance with this Implementation Specification.<br><br>Users should not be able to disable antivirus software.<br><br>Protections provided by Linksys Cable/DSL router are too limited, even with built-in "firewall" protection turned on.<br><br>No IDS solution or system integrity software exists. | Implement more robust firewall solution.<br><br>Create appropriate policies and procedures.<br><br>Disable ability for users to disable anti-virus solution.<br><br>Implement IDS solution.<br><br>Implement system integrity solution to help identify potentially malicious software on the two servers on the network that contain ePHI. |

**(C) Log-in monitoring (Addressable)**. Procedures for monitoring log-in attempts and reporting discrepancies.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Failed and successful login attempts are not logged on the Windows systems. Failed and successful login events are enabled on the Unix system. No procedures exist for monitoring access logs. | Logging is not occurring for access on Windows systems.<br><br>Logs are not being reviews. | Create policies and procedures for logging and reviewing logs of system access. Implement logging on Windows system. Ensure that responsibility for compliance with this Implementation Specification is clearly assigned and that the responsible person is trained on how to look for and report discrepancies. |

**(D) Password management (Addressable)**. Procedures for creating, changing, and safeguarding passwords.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Password policies and procedures have been written. HR documentation includes | GIAC Enterprises appears to meet this Implementation Specification. | None Necessary |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| requirements for employees not to share their passwords. Workstations were checked to look for papers that had username/passwords and none existed. Passwords are changed every thirty days as enforced by operating system configuration. Employees were quizzed on their understanding of the policies outlined in the employee manual and all employees understood and are in compliance with the stated policies.<br><br>This policy is included in Appendix G | | |

**(6)(i) Standard: Security incident procedures**. Implement policies and procedures to address security incidents.

**Response and Reporting (Required)**. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Incident response procedure not found. | GIAC Enterprises is not in compliance with this Standard. | Document Incident Response Procedure. |

**(7)(i) Standard: Contingency plan**. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

**(A) Data backup plan (Required)**. Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises performs weekly full backups and daily incremental backups on all systems containing ePHI. | This procedure is not documented. | Documented the currently enacted procedure for performing backups. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

**(B) Disaster recovery plan (Required)**. Establish (and implement as needed) procedures to restore any loss of data.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Backups are not tested. Full backup tapes are taken home by Jane Receptionist every Friday. These tapes are stored in Jane's desk drawer at home. Jane lives twenty-five minutes away. Restoration procedures are not written. | Backups need to be tested.<br><br>Tapes are not properly secured when off-site.<br><br>Restoration procedures are not well understood or practiced. | Create and implement a policy and procedure to regular test restorations from backup media.<br><br>Obtain additional hard drives in order to test complete restoration on an annual basis. Document process to perform complete restoration.<br><br>Provide an environmentally controlled safe for Jane Receptionist or use an off-site tape storage service to keep off-site copies of backup tapes. |

**(C) Emergency mode operation plan (Required)**. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has an established business contingency plan in the event that they are suddenly required to relocate their business. This is an agreement between GIAC Enterprises and GIAC Health to share a facility. Both offices have adequate physical space to support growth. Contingency funds are available to purchase equipment necessary to rebuild their environment. Medical equipment is available to GIAC Enterprises as part of their agreement with GIAC Health.<br><br>Contingency Plan is available Appendix H | Technical issues that complicate this contingency plan are identified in other Implementation Specifications and do not need to be readdressed here.<br><br>No additional action necessary. | None necessary |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

**(D) Testing and revision procedures (Addressable)**. Implement procedures for periodic testing and revision of contingency plans.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| The contingency plan is reviewed between GIAC Enterprises and GIAC Health on a yearly basis as per their contingency contract. | No procedures exist for testing contingency plan. | Completely testing the contingency plan (independent of other Implementation Specifications in this realm) is deemed as overly costly. Since GIAC Enterprises is a small organization, it may be appropriate to document that no further steps to test the full contingency plan would be appropriate. This decision should be reviewed closely with legal counsel. Document this decision clearly. |

**(E) Applications and data criticality analysis (Addressable)**. Assess the relative criticality of specific applications and data in support of other contingency plan components.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| A thorough data criticality analysis was performed as part of the Risk Analysis performed in compliance with the HIPAA Security Rule. This is available in Appendix A. | The data criticality analysis from the Risk Assessment has not been extracted and documented as an order of restoration in contingency procedures. | Copy and modify data criticality analysis from Risk Assessment and include as a prioritization of restoration in the event of contingency plan activation. |

**(8) Standard: Evaluation**. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has documented a policy for a third party audit on an annual basis with regards to HIPAA Privacy Rules. However, they have not complied with this policy since it has been 18 months since | Documented policy for HIPAA Privacy Rule is not enforced.<br><br>Annual review is specifically worded to be targeted at the privacy rule; thus no such policy exists as it relates to | Expand existing policy to include HIPAA Security Rule.<br><br>Enforce documented policy. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| the last audit. | HIPAA Security Rule. | |

**(b)(1) Standard: Business associate contracts and other arrangements.** A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate will appropriately safeguard the information.

**(4) Written contract or other arrangement (Required)**. Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Sec. 164.314(a).

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has implemented appropriate business associate contracts with all appropriate parties as part of the HIPAA Privacy compliance initiative. These contracts were authored by Mr. Lawyer specifically to be in accordance with HIPAA Privacy and Security Rule regulations. | GIAC Enterprises is in compliance. | No actions required. |

## Physical Safeguards: Details

**164.310(a)(1) Standard: Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

**(i) Contingency operations (Addressable)**. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| No documented procedures exist. GIAC Enterprises is a small organization with a very limited number of employees. In practice, the office manager and doctors have keys to all | Procedures are implemented in practice, but are not documented. | Document policy/procedure identifying who has keys to all locks at GIAC Enterprises. Identify a procedure for getting in touch with these individuals. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| locks within the office. | | |

**(ii) Facility security plan (Addressable)**. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Locks are in place and correctly used on all points of entry. There is a card access system required to enter the treatment area. Patients are escorted in by nurses. The nurses' station has full view of all treatment rooms within the clinic from the nurses' station and during business hours, this area is almost always occupied by GIAC Enterprises staff. No access is available to ePHI in the treatment rooms except for information that are carried in by employees for purposes of delivering care. Policies and procedures dictate that employees carrying information in the presence of patients are responsible for ensuring that unsupervised access to ePHI is not permitted. Supervised access is only for the purposes of treatment and can only include records for which the patient has a right to view in accordance with the HIPAA Privacy Rule.<br><br>A Business Associate Agreement is in place with the janitorial staff. The related policies and procedures can be found in Appendix I.<br><br>The building provides a security guard during hours when the doors are unlocked to the public. Building policies indicate that equipment "larger than a bread box" are to be logged by security guards and an approval for removal must be signed by an authorized | Despite weaknesses, GIAC Enterprises has taken significant steps to comply with this requirement. Company policy should include a requirement of an employee always being in the nursing station.<br><br>Policies written by building management should be enforced.<br><br>No policies exist with regards to ensuring third parties who have a business need to work at GIAC Enterprises are appropriately controlled. | Create policy for fulltime occupancy of nursing station during business hours.<br><br>Work with building to enforce policies on removal of equipment.<br><br>Document policies and procedures addressing third party access. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| building tenant. Authorized building tenant is defined by someone who has signed the lease or whom someone has the lease has authorized. This policy was tested and found not to be enforced.<br><br>The building has video cameras that are recorded to tape. Tapes are overwritten on a weekly basis and are available to be retrieved through the building management company. Cameras cover all points of entry/exit to the building. | | |

**(iii) Access control and validation procedures (Addressable)**. Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Policies and procedures exist documenting that the Privacy Officer must authorize all access to PHI. Procedures exist controlling where patients are permitted to be unsupervised during a visit. No procedures exist for authorizing access by consultants or other service personnel. | Employee and patient access procedures are documented and properly implemented, but procedures need to be expanded to incorporate other people who may need access to the facility. | Document and implement procedures to control access to people other than patients and employees who need access to the facility. Ensure that the procedure includes validation of identity and that the purpose of the visit is clearly understood and expected. |

**(iv) Maintenance records (Addressable)**. Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| No maintenance records exist. | Maintenance records need to exist. | Establish and implement policies and procedures to document the type of access discussed in this implementation specification. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

**(b) Standard: Workstation use**. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| A very thorough acceptable use policy exists. The acceptable use policy also covers details associated with positioning of workstations to reduce the risk of unintentional exposure of (e)PHI. See Appendix J<br><br>These documents were created as a result of the HIPAA Privacy Rule. | The implemented policies and procedures are appropriate, enforceable, and implemented. No gaps have been identified. | None needed |

**(c) Standard: Workstation security**. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Details associated with this are discussed in the facility security plan above. | No gaps identified. | None needed |

**(d)(1) Standard: Device and media controls**. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

**(i) Disposal (Required)**. Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| No policies or procedures exist. GIAC Enterprises rarely disposes of equipment falling under this specification. | No steps have been taken to comply with this implementation specification.<br><br>Most important for GIAC Enterprises with regards to | Document and implement policies and procedures to comply with this implementation specification.<br><br>Consider using a third party |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| | this implementation specification is the disposition of tapes used for performing backups. Tape retention policies include the retirement of tapes, so appropriate steps must be taken to properly dispose of this tape media since it undoubtedly will contain ePHI. | contractor to ensure that hardware and media are properly disposed of. |

**(ii) Media re-use (Required)**. Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| All equipment at GIAC Enterprises is considered by the company to contain ePHI. As a result, re-use of equipment does not occur within the organization. | For GIAC Enterprises, compliance with this implementation specification is inherent in compliance with the disposal implementation specification above. | Complete remediation steps for the disposal implementation specification. |

**(iii) Accountability (Addressable)**. Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has no intent to move facilities or equipment. Backup tapes are taken home by Jane Receptionist as part of the contingency plan for offsite storage of backup tapes. | Documentation needs to exist to clearly identify what happens to both hardware and media containing ePHI. This will include mostly the backup tapes taken home by Jane Receptionist, but should also include other hardware incase a need to remove such devices from GIAC Enterprises arises in the future. | Document and implement policies and procedures document the movement of all hardware and electronic media from GIAC Enterprises. |

**(iv) Data backup and storage (Addressable)**. Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises has no | GIAC Enterprises is compliant | Document how GIAC |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| intent to move facilities or equipment. However, backups are performed according to policy. | with the intent of this specification. Documentation of this interpretation needs to exist. | Enterprises interprets and believes to comply with the intent of this implementation specification. |

## Technical Safeguards: Details

**164.312(a)(1) Standard: Access control**. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).

**(i) Unique user identification (Required)**. Assign a unique name and/or number for identifying and tracking user identity.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Two accounts exist for each employee at GIAC Enterprises that have access to ePHI. The first is a windows account that is an active directory username. This account is used for access to all ePHI stored on Windows based operating system. The same user account is independently created on the Unix system. This practice is not documented as a policy or procedure. | Compliance with this implementation specification needs to be identified. | Document the currently implemented policy for user account creation.<br><br>Review and consider implemented a method to use the Active Directory user accounts directly for access to the Unix operating system via Kerberos authentication. |

**(ii) Emergency access procedure (Required)**. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| No procedures were found. | This implementation specification has not been addressed at all. | Create the requirement procedure. Consider how administrative access can be obtained to ePHI in the event of an emergency. Consider storing the administrative password in a locked tamper evident container for the Unix and Windows operating system. Ensure that this password is updated if the administrative account |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| | | password changes. |

**(iii) Automatic logoff (Addressable)**. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises accesses all ePHI from their workstations. Screen savers are implemented to initiate in 10 minutes of inactivity and are password protected. | The implemented procedure addresses the intent of this specification. | Document the implemented procedure and identify it as the intended method to comply with this implemented specification. |

**(iv) Encryption and decryption (Addressable)**. Implement a mechanism to encrypt and decrypt electronic protected health information.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| The Unix system is accessed via SSH. A review of access to ePHI on the windows system was performed with a packet dump. ePHI is transmitted in clear text on the internal network. Data is not encrypted on backup tapes or while it resides on the disk. | Encryption in transit for ePHI on GIAC Enterprises network can easily be achieved amongst the Windows systems and should be implemented.<br><br>Encryption of data at rest has been deemed by GIAC Enterprises to be more than they believe required by this implementation specification. | Turn on encryption amongst Windows systems.<br><br>Document interpretation of need to encrypt data at rest for GIAC Enterprises and have it reviewed by legal counsel with respect to compliance with this implementation specification.<br><br>Document policy stating that all ePHI in transit is to be encrypted. Document procedures for how this policy is met. |

**(b) Standard: Audit controls**. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| The two applications used at GIAC Enterprises for ePHI storage and retrieval have software mechanisms for recording an audit trail. These are currently turned off. | Failed and successful login/logoff auditing was discussed in the administrative safeguards section.<br><br>Audit logs for the ePHI applications needs to be enabled. | Turn on auditing for applications that access ePHI to record who is viewing ePHI data.<br><br>Document a procedure on how to review these logs. |


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

| | | |
|---|---|---|
| | A procedure for examining these logs needs to be documented and implemented. | |

**(c)(1) Standard: Integrity**. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

**(2) Mechanism to authenticate electronic protected health information (Addressable)**. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Servers containing ePHI are using RAID 5. | GIAC Enterprises has identified that additional integrity controls are unnecessary for their environment. | Document GIAC Enterprises interpretation of the lack of need for them to take additional technical steps to comply with this implementation specification. Review these documents with legal counsel. |

**(d) Standard: Person or entity authentication**. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Controls exist as part of HIPAA Privacy rule compliance for verifying the identity of external entities requesting PHI that is held by GIAC Enterprises. This document is found appropriate for the Security Rule as well. See this in Appendix K.<br><br>Internally, all users access ePHI using their Windows or Unix accounts. | Documentation needs to exist to discuss username and password access to ePHI on GIAC Enterprises network. | Create user authentication methods for internal employees. |

**(e)(1) Standard: Transmission security**. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

**(i) Integrity controls (Addressable)**. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| GIAC Enterprises would like to implement a method to transfer ePHI to business partners (specifically their clearinghouse vendor) via a site to site VPN. | Policy needs to be established to ensure that the future IPSEC tunnel planned meets the integrity control requirement. | Document policy specifying what technical specifications are acceptable when transferring ePHI through a VPN tunnel to a business partner. |

**(ii) Encryption (Addressable)**. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

| Current State Assessment | Identified Gaps | Remediation Options |
|---|---|---|
| Along with Integrity of the site to site VPN discussed in the previous section is encryption needs. | Ensure that the policy for the site to site VPN includes encryption requirements. | Ensure compliance with this implementation specification in the integrity implementation specification requirement.<br><br>As stated earlier, document and implement the procedure encrypt traffic in transit with SSH to the Unix system and with IPSEC implementation on the Windows network |

## Appendices

Since this deliverable is for a theoretical engagement, the documents specified for inclusion in the appendices do not actually exist. Here is the list of documents identified for inclusion in the appendix section in the preceding text:

Appendix A: Risk Analysis performed during HIPAA Privacy Rule Gap Analysis

Appendix B: Company Sanction Policy

Appendix C: HIPAA Privacy Officer and general HIPAA documentation responsibility assignment policy

Appendix D: GIAC Enterprises Business Partner Agreement

Appendix E: Termination procedures

Appendix F: Access Authorization policy


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix G: Password Policy from Employee Manual

Appendix H: Business Contingency Plan

Appendix I: Policies and Procedures discussing responsibility for protecting (e)PHI from unauthorized disclosure. Business Associate agreement with Janitorial staff.

Appendix J: Acceptable Use Policy and Workstation Positioning Policy.

Appendix K: External access to PHI authorization and verification policy

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## References


1. Compton, Chris “Providing Network Traffic Analysis Services to a Government Contractor” URL: http://www.giac.org/practical/GCSC/Chris_Compton_PPT_GCSC.pdf (August 2004)

2. “Final HIPAA Security Rule” URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp (August 2004)

3. Happy, Robert, et al., SANS Press, HIPAA Security Implementation: Step by Step Guide v 1.0

4. Musgrave, Garry, “10 Common Project Pitfalls and How To Avoid Them” URL: http://www.conceptron.com/articles/pdf/ten_pitfalls.pdf (January 2001)

5. “Plan, DO, Check, Act – PDCA” URL: http://www.isixsigma.com/me/pdca/ (August 2004)


© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.