DRAFT REPORT

Of the

HIPAA / HITECH / Meaningful Use AUDIT

Of the

$COMPANY Facilities in $LOCATION

$DATE

Statement of Confidentiality

The information contained in this document is confidential and proprietary to $ASSESSOR and to the $CLIENT. It has been made available solely as the report of an audit. In no event shall all or any portion of this proposal be disclosed or disseminated outside of $CLIENT for any other purpose without the express written permission of $ASSESSOR.

Table of Contents

Table of Contents 2

I. EXECUTIVE SUMMARY 4

II. BACKGROUND AND GENERAL OBSERVATIONS 6

III. FINDINGS AND RECOMMENDATIONS........ 6

1. Many of $CLIENT’s Policies and Procedures are inadequate and contain no references to HIPAA, HITECH, or Meaningful Use 6

2. 8

3. .... **Error! Bookmark not defined.**

4. .... **Error! Bookmark not defined.**

5. .... **Error! Bookmark not defined.**

6. .... **Error! Bookmark not defined.**

7. .... **Error! Bookmark not defined.**

8. .... **Error! Bookmark not defined.**

9. .... **Error! Bookmark not defined.**

10. .... **Error! Bookmark not defined.**

11. .... **Error! Bookmark not defined.**

12. .... **Error! Bookmark not defined.**

13. .... **Error! Bookmark not defined.**

14. .... **Error! Bookmark not defined.**

15. .... **Error! Bookmark not defined.**

16. .... **Error! Bookmark not defined.**

17. .... **Error! Bookmark not defined.**

18. .... **Error! Bookmark not defined.**

19. .... **Error! Bookmark not defined.**

20. .... **Error! Bookmark not defined.**

21. ….. .... **Error! Bookmark not defined.**

22. .... **Error! Bookmark not defined.**

23. .... **Error! Bookmark not defined.**

24. .... **Error! Bookmark not defined.**

25. . ... **Error! Bookmark not defined.**

IV. Meaningful Use 9

V. OBSERVATIONS AND SUGGESTIONS 10

26. In the team's opinion, $CLIENT could benefit from such a help desk.............. 10

27. 10

28. 11

29. . . .. **Error! Bookmark not defined.**

30. . . .. **Error! Bookmark not defined.**

31. . ... **Error! Bookmark not defined.**

32. .... **Error! Bookmark not defined.**

33. . ... **Error! Bookmark not defined.**

Appendix A:... 12

Appendix B: HIPAA Security Checklist... 15

Appendix C: HIPAA Checklist for Providers 21

I. EXECUTIVE SUMMARY

In the constantly changing field of information technology, it is not uncommon to see organizations struggle to keep up with the pace of new rules and regulations. Economic and practical considerations preclude an active organization from instantly meeting these changing obligations. Having an audit performed shows dedication to one's medical customers, as well as to the shareholders that rely on such decisions to be made to keep them from losing money and business due to ineffective security processes and procedures.

The $CLIENT does not fully comply with HIPAA in at least 4 areas: 1) Policies and procedures, 2) Physical security, 3) User training and awareness, and 4) Implementation of security measures. The most critical flaw is the lack of defined, approved, and supported policies and procedures. While this report discusses these areas in detail, the team wishes to note that, in the HIPAA arena, $CLIENT is far from being the least-secure organization known to the team. $CLIENT has much to be proud of; not the least of which is the quality and dedication of its people.

The team firmly believes that the employees of $CLIENT are willing and able to implement whatever appropriate policies are promulgated by $CLIENT's Board, but, without the appropriate policies and procedures, the employees lack the tools and training necessary to meet the requirements of the law. While $CLIENT has many excellent people who are doing the right things for the right reasons, most interviewees believe that the system they work under handicaps their ability to excel at their jobs.
Specific findings include:

1 Many of $CLIENT's Policies and Procedures are inadequate and contain no references to HIPAA, HITECH, or Meaningful Use
2
3
4
5
6
7
8
9
10
11
12
13

14
15
16
17
18
19
20
21
22
23
24
30

II. BACKGROUND AND GENERAL OBSERVATIONS

This evaluation is based on interviews with various employees of $CLIENT that were conducted $DATE. The primary focus of the evaluation team was to determine $CLIENT's compliance with the Health Insurance Portability and Accountability Act (HIPAA,) which went fully into effect on April 21, 2005, and with the implementation of the *Health Information Technology for Economic and Clinical Health* (HITECH) Act.

In this report, a “Finding” is a topic or situation that the evaluation team believes must be addressed by $CLIENT Management. Similarly, a “recommendation” is a statement of what the team believes is necessary to correct the finding. In many cases, $CLIENT Management may choose not to implement the team's specific recommendation, to correct the problem some other way, or to accept the situation for the time being, perhaps because a fix is otherwise expected in the near future. In any case, prudent business practices would mandate that such decisions be documented in writing. In general, US Government (USG) and State of Alaska (SOA) auditors usually consider findings and recommendations as matters that should be addressed by Management, one way or the other.

In this report, an “Observation” is a situation or topic that the evaluation team noticed in the course of their evaluations and would like to bring to the attention of $CLIENT Management. A “suggestion” is just that – a suggested item that $CLIENT Management might want to consider. In general, USG and SOA auditors do not consider observations and suggestions as pertinent to whatever audits they are conducting.

In the case of both Findings and Observations, comments are exactly that – explanatory or hortatory remarks that elaborate on the topic. Auditors should not consider comments as part of findings, recommendations, observations, or suggestions.

III. FINDINGS AND RECOMMENDATIONS

FINDING:

1. **Many of $CLIENT's Policies and Procedures are inadequate and contain no references to HIPAA, HITECH, or Meaningful Use**

RECOMMENDATION:

1. Update IT Policies and Procedures ASAP, including references to HIPAA, HITECH, and Meaningful Use, where applicable. The following table should be considered as the Audit Team's recommendation in rough priority order (most-critical first,) not as a complete list.

Policy and Procedures	Example HIPAA Requirement
Disaster Recovery / Continuity of Operations (DR/COOP)	164.308(a)(7)(ii)(C)
Access Control and Accountability, including Auditing Trails, Regular Review of Audit Trails, Employee Termination and Reassignment, Passwords, and Destruction of PHI.	164.312(a)(2)(ii)
Assigned security responsibility	164.308(a)(2)
Security awareness and training	164.308(a)(5)(i)
Security incident procedures:	164.308(a)(6)(i)
Assess relative criticality of specific applications	164.308(a)(7)(ii)(E)
Access to ePHI during an Emergency	164.312(a)(2)(ii)
Appropriate encryption of ePHI	164.312(a)(2)(iv)
Business associate contracts and other arrangements	164.308(b)(1)
Security management process:	164.308(a)(1)(i)
Procedures for monitoring log-in attempts and reporting discrepancies	164.308(a)(5)(ii)(C)
Periodic testing and revision of contingency plans	164.308(a)(7)(ii)(D)
Facility access controls	164.310(a)(1)
Device and media controls:	164.310(d)(1)
Protect EPHI from improper alteration or destruction.	164.312(c)(1)
Periodic technical and nontechnical evaluation	164.308(a)(8)
Procedures for guarding against, detecting, and reporting malicious software?	164.308(a)(5)(ii)(B)

COMMENT:

1. From a US Government compliance point-of-view, IT Policies and Procedures are essentially the most important aspect of an organization’s security, and are, unfortunately, one of the most overlooked/neglected aspects. Without these, an organization has no solid ground to stand on when enforcing rules that are made to protect data, and maintain business continuity.

FINDING:

2. Physical security and security awareness at $LOCATION needs to be enhanced.

Sensitive Documents should not be left unattended on people’s desks. $CLIENT does a much better job of protecting lumber in building 615 than it does of protecting PHI in $LOCATION.

RECOMMENDATION:

2. Configure door locks properly on internal stairwell doors, remove and upgrade camera system at $LOCATION, and move key pad on the 5th floor behind the door instead of out front.

COMMENT:

2. Physical security is the discipline that underpins all protection of anything

FINDING:

3. Physical security and security awareness at $LOCATION needs to be enhanced.

Sensitive Documents should not be left unattended on people’s desks. $CLIENT does a much better job of protecting lumber in $LOCATION than it does of protecting PHI in $LOCATION.

RECOMMENDATION:

3. Configure door locks properly on internal stairwell doors, remove and upgrade camera system at $LOCATION, and move key pad on the 5th floor behind the door instead of out front.

COMMENT:

2. Physical security is the discipline that underpins all protection of anything

IV. Meaningful Use

In the Audit Team’s considered opinion, $CLIENT meets essentially all the criteria for Meaningful Use Level One and most of the criteria for Level Two.

V. OBSERVATIONS AND SUGGESTIONS

OBSERVATION:

4. Many organizations find significant economies of effort can be gained when the Help Desk is a general, organization-wide resource, rather than an IT support center resource only. In the team's opinion, $CLIENT could benefit from such a capability.

SUGGESTION:

4. Once the IT help desk's trouble-ticket system is replaced with a simpler, user-friendly, easy-to-use system, $CLIENT should consider reorganizing its help-desk into a triage resource that passes requests to the appropriate organization, rather than having technicians answer the help-desk phones and try to solve problems right there. A small, customer-service-oriented group (perhaps one to three people, depending on customer demands vs. time of day) would quickly take the call, determine the appropriate group to handle the problem, and route the ticket on for resolution.

COMMENT:

4. Many organizations have found this to be a very efficient way to get routine issues fixed quickly and easily. Issues from “My chair's broken.” to “A light bulb's out in my office.” to “My printer won't work.” can be efficiently solved this way. Primarily, it frees staff time to do their job, rather than staff taking the time to find out how to get their chair fixed. In general, the answer to any non-medical question of “How do I ...” is “Call the help desk.”

OBSERVATION:

5. Many employees consider the new employee orientation to be lacking, both in HIPAA and general security awareness issues.

SUGGESTION:

5. Improve new employee orientation by hiring an outside agency to train staff on HIPAA and security issues so that staff can train other employees during new employee orientation.

COMMENT:

5. Because this is one of the first things an employee will do after being hired, it is very important to provide good training that will cover the necessary material properly. New employees are generally in a mental state where they are more apt to learn things during the first few weeks/months of employment, making it that

much more important that the training not only breaches the topics, but also does so in an effective manner.

OBSERVATION:

6. **Process of issuing employee badges appears to have little, if any, impact on security. Badges are not checked when employees enter the building, and the process of issuing badges is far from perfect. The security card system is approximately 12 years old (running Windows 98).**

SUGGESTION:

6. Purchase and implement a new card system. Ensure that employees are adhering to the rules by either having a person check cards at the front door, or have a card reader installed where employees.

COMMENT:

6. Having a security system doesn't do any good if it isn't being used – it's like having a gym membership just to say you have one. Having the security card system won't thwart any attacks unless it is being used.

Appendix A

This document is the overview working guidance document used by the assessment team for HIPAA assessments.

1. Awareness and Accountability.

1.1. Designate staff / team responsible for overseeing review process.
1.2. Determine Sponsorship
1.3. Educate Hospital / Medical Clinic Management in their responsibilities and Ownership
1.4. Educate Board of Directors and Officers of the Corporation

2. Security Standards

2.1. Review the proposed standards
2.2. Determine your level of compliance by performing a gap analysis

3. Standards Development Organizations

3.1. Learn who the standards development organizations are:

3.1.1. ANSI – American National Standards Institute
3.1.2. ASTM – American Society for Testing and Materials
3.1.3. ISO – International Organization for Standardization

3.2. Become familiar with the content of the standards

4. Information Security Program

4.1. Look at what organizational structures are in place that can aid in the development and implementation of an Information Security Program

4.1.1. Management
4.1.2. Information Security Team
4.1.3. Compliance Committee
4.1.4. HIM Committee
4.1.5. Education Groups

5. Policies

5.1. Policies exist that relate to the security and confidentiality of health information

5.1.1. Access Control
5.1.2. Passwords
5.1.3. System and Network Access Control
5.1.4. Protecting Information in Offices, Patient/Work Areas

6. Users of Electronic Information

6.1. All users have a unique access code
6.2. Access be restricted to information needed to do one’s job

7. Physician Responsibilities

7.1. Medical Staff bylaws or rules and regulations include physician responsibilities regarding the protection of confidential health information
7.2. Consequences for inappropriate use and disclosure of the information

8. Employee Responsibilities

8.1. Responsibilities for protecting the confidentiality of health information is outlined and reviewed with all employees

8.1.1. e.g. development of employee handbook

8.2. Policies address consequences of inappropriate use or disclosure of health information

9. Education

9.1. Everyone with access to health information is trained about their responsibilities regarding confidentiality

9.1.1. Employees
9.1.2. Physicians
9.1.3. Business Partners

10. Vendor Contracts

10.1. Contracts dealing with outsourcing of health information include provisions regarding confidentiality and information security
10.2. Provisions for notification if unauthorized access occurs
10.3. Vendors are required to sign confidentiality agreements

11. Unlimited / Unrecorded Access

11.1. Ensure that Users such as System Managers, Network Managers, and Programmers do not have unlimited access to patient information

12. Monitoring of Access

12.1. Mechanisms to monitor access to information are in place and being utilized
12.2. Corrective action plans are established and enforced for violation of policy Risk Assessments
12.3. Risk Assessments are being performed to prioritize and continually improve the security of the systems

13. Next Steps

13.1. Analyze results to identify non-compliant areas
13.2. Identify Cost and Degree of Risk
13.3. Present to Management for Prioritization of Risks
13.4. Develop prioritized action plan for implementation
13.5. Implement the Plan
13.6. Perform an Internal Audit for Maintenance of the Plan

14. Maintain Current Knowledge

14.1. Keep up to date with Information Security Issues and Industry Responses

14.1.1. Publications

14.1.1.1. Briefing on Health Information Security at www.himinfo.com
14.1.1.2 NIST Security Publication 800-66 at www.nist.gov

14.1.2. Internet

14.1.2.1. http://www.ahima.org
14.1.2.2. http://www.astm.org
14.1.2.3. http://aspe.os.dhhs.gfov/adminsimp

Appendix B: HIPAA Security Checklist

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a, etc.
Administrative Safeguards		
164.308(a)(1)(i)	Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	
164.308(a)(1)(ii)(A)	Has a risk analysis been completed IAW NIST using Guidelines? (R)	
164.308(a)(1)(ii)(B)	Has the risk management process been completed using IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(C)	Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? (R)	
164.308(a)(2)	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.	
164.308(a)(3)(i)	Workforce security: Implement policies and procedures to ensure that all members of workforce have appropriate access to EPHI, 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 (EPHI).	
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine the access of an employee to EPHI is appropriate? (A)	
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to EPHI when an employee leaves your organization or as required by paragraph (a)(3)(ii)(B) of this section? (A)	

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a, etc.
164.308(a)(4)(i)	Information access management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.	
164.308(a)(4)(ii)(A)	If you are a clearinghouse that is part of a larger organization, have you implemented policies and procedures to protect EPHI from the larger organization? (A)	
164.308(a)(4)(ii)(B)	Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process? (A)	
164.308(a)(4)(ii)(C)	Have you implemented policies and procedures that are based upon your access authorization policies, established, document, review, and modify a user's right of access to a workstation, transaction, program, or process? (A)	
164.308(a)(5)(i)	Security awareness and training: Implement a security awareness and training program for all members of the workforce (including management).	
164.308(a)(5)(ii)(A)	Do you provide periodic information security reminders? (A)	
164.308(a)(5)(ii)(B)	Do you have policies and procedures for guarding against, detecting, and reporting malicious software? (A)	
164.308(a)(5)(ii)(C)	Do you have procedures for monitoring log-in attempts and reporting discrepancies? (A)	
164.308(a)(5)(ii)(D)	Do you have procedures for creating, changing, and safeguarding passwords? (A)	
164.308(a)(6)(i)	Security incident procedures: Implement policies and procedures to address security incidents.	
164.308(a)(6)(ii)	Do you have procedures to identify and respond to suspected or known security incidents; to mitigate them to the extent practicable, measure harmful effects of known security incidents; and document incidents and their outcomes? (R)	
164.308(a)(7)(i)	Contingency plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, or natural disaster) that damages systems that contain EPHI.	

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a, etc.
164.308(a)(7)(ii)(A)	Have you established and implemented procedures to create and maintain retrievable exact copies of EPHI? (R)	
164.308(a)(7)(ii)(B)	Have you established (and implemented as needed) procedures to restore any loss of EPHI data stored electronically? (R)	
164.308(a)(7)(ii)(C)	Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode? (R)	
164.308(a)(7)(ii)(D)	Have you implemented procedures for periodic testing and revision of contingency plans? (A)	
164.308(a)(7)(ii)(E)	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? (A)	
164.308(a)(8)	Have you established a plan for 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 EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart? (R)	
164.308(b)(1)	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 EPHI 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 appropriately safeguards the information.	
164.308(b)(4)	Have you established written contracts or other arrangements with your trading partners that document satisfactory assurances required by paragraph (b)(1) of this section that meets the applicable requirements of Sec. 164.314(a)? (R)	
Physical Safeguards		

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a, etc.
164.310(a)(1)	Facility access controls: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.	
164.310(a)(2)(i)	Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan? (A)	
164.310(a)(2)(ii)	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft? (A)	
164.310(a)(2)(iii)	Have you implemented procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision? (A)	
164.310(a)(2)(iv)	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks)? (A)	
164.310(b)	Have you implemented 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 EPHI? (R)	
164.310(c)	Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users? (R)	
164.310(d)(1)	Device and media controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.	
164.310(d)(2)(i)	Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored? (R)	
164.310(d)(2)(ii)	Have you implemented procedures for removal of EPHI from electronic media before the media are available for reuse? (R)	

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a, etc.
164.310(d)(2)(iii)	Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement? (A)	
164.310(d)(2)(iv)	Do you create a retrievable, exact copy of EPHI, when needed, before moving equipment? (A)	
Technical Safeguards		
164.312(a)(1)	Access controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	
164.312(a)(2)(i)	Have you assigned a unique name and/or number for identifying and tracking user identity? (R)	
164.312(a)(2)(ii)	Have you established (and implemented as needed) procedures for obtaining necessary EPHI during an emergency? (R)	
164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)	
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt EPHI? (A)	
164.312(b)	Have you implemented audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI? (R)	
164.312(c)(1)	Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner? (A)	
164.312(d)	Have you implemented person or entity authentication procedures to verify a person or entity seeking access EPHI is the one claimed? (R)	
164.312(e)(1)	Transmission security: Implement technical security measures to guard against unauthorized access to EPHI being transmitted over an electronic communications network.	

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status Complete, n/a, etc.
164.312(e)(2)(i)	Have you implemented security measures to ensure electronically transmitted EPHI is not improperly modified without detection until disposed of? (A)	
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate? (A)	

Appendix C: HIPAA Checklist for Providers

		Done
Build a Library of Key HIPAA Documents		
	Health Insurance Portability and Accountability Act of 1996, P.L. 104-191	□
	Standard Transaction and Code Set Rules and Regulations	□
	Privacy Rules and Regulations	□
	Security Rules and Regulations	□
	Implementation Guidelines	□
	Data Standard Maintenance Organizations	□
	Office of Civil Rights Guiding Documents	□
	HCFA/CMS Internet Policy	□
Build an awareness of HIPAA within your practice		
	Determine key staff to form a HIPAA Task Force	□
	Review key documents with Task Force	□
	Hold discussions to determine impact to your practice	□
	Identify key forms/templates/documentation to use in developing an overall Project	□
	Prepare and train personnel – deliver awareness sessions	□
	Develop ongoing plan to continue awareness and education	□
Build a HIPAA Inventory		
	Excel spreadsheets are an excellent tool for tracking inventories. Columns on the spreadsheet identify (1) description of the inventory item, (2) Classification – a priority code by criticality. Determine inventory format and perform inventory on items that follow	□
	All systems and applications; both internal and external	□
	All networks (LANs, WANs) and components	□
	Communications protocols for networks and third party connections	□
	All related systems, hardware, software and applications, including email (Including printers, copiers and fax machines)	□
	All personnel and access to offices and information	□
	Physical environment components (buildings, offices, security systems)	□
	Administrative processes and procedures	□
	Current privacy policies and procedures	□
	Current security policies and procedures, list existing safeguards	□

		Done
	Contracts in place and/or negotiation for Vendors, Partners, and Relationships	□
	Billing services, other third party agreements	□
	Business continuity plans	□
	Disaster recovery plans	□
	Electronic transactions and describe formats	□
	Types of communications	□
	Paper transactions and processes	□
	Current privacy notices	□
	Current consents	□
	Current authorizations □	□
Determine the impact from HIPAA		
	For each item in your inventory you need to determine the impact from:	□
	Transactions, Codes, Identifiers, Privacy, Security	□
	List all that apply. Add another column to your spreadsheet to enter this information.	□
	For each item, determine priority ranking. Add another column to your spreadsheet to enter this information.	□
	For personnel listed describe access to confidential and/or Protected Health Information (PHI)	
Perform a Gap Analysis and assess the impact on the inventory for compliance with transactions and code sets, privacy, and security, and identifiers.		
	Once the inventory has been completed, the assessment process begins. You may want to consider combining the assessment with the inventory by simply adding another column to the spreadsheet. The new column can contain your level of assessment.	□
	To develop the assessment you will need to perform a gap analysis that identifies missing components or required changes or additions.	□
	Changes may simply be enhancing existing policies and procedures, adding provisions to apply appropriate safeguards to protect your data and your environment, working with vendors to process standard transactions, assessing resources and budget for changes, working with vendors for needed modifications in current applications and systems, reviewing data storage needs, determining risks, and creating new policies and procedures. You will need to review your EDI, Privacy and Security options.	□

		Done
EDI evaluations must be performed and gaps must be addressed		
	How do you handle and process electronic transactions?	□
	Are these transactions in the standard formats?	□
	How do you address expanded data element requirements?	□
	What must be done to convert to the standards?	□
	How can your clearinghouse assist you?	□
	What are your vendors doing to address HIPAA standards?	□
	What options do you have in paper processing?	□
	Have you looked at all the standard transactions available to you electronically?	□
	How are you using code sets? (Local codes are being eliminated)	□
	What are your coding guidelines and best practices?	□
Evaluate Privacy Needs		
	Have you appointed a Privacy Manager or Official?	□
	What PHI is processed and handled within your operations?	□
	How are PHI disclosures processed?	□
	Do you send PHI in email or email attachments?	□
	Are patient files secure?	□
	Is PHI left exposed via copy or fax machines?	□
	How do you handle minimum necessary requirements?	□
	Who has access to patient files and data?	□
	Who has access to PHI on computer screens?	□
	How do you handle requests from patients regarding privacy?	□
	If you have a website, does it state your privacy practices?	□
	Do you need business associate agreements?	□
	Have you evaluated your existing consents and authorizations use?	□
	Policies and Procedures	□
	Employee Training	□
Evaluate Security Needs		
	Do you access the Internet?	□
	Do you have firewalls in place?	□
	Do you use encryption? If so, how do you use it and why?	□
	Do you have virus protection?	□
	Do you have access controls in place?	□
	Do you use passwords and entity authentication?	□
	Do have screen or session timeouts on your computers?	□

		Done
	Do you perform system and data back-ups?	□
	What are the security levels applied to electronic transactions?	□
	Do you have incident tracking for security violations or intrusions?	□
Develop an Action Plan		
	As you complete your gap analyses and assessments, you will have a good idea of actions that need to be taken. Remember that much of what you do is to be based on the scope and size of your practice.	□
	Many solutions are available that are low tech and may be applied very quickly. The rules and regulations for privacy and security mention reasonable and scalable throughout. Each practice will need to assess best business practices and apply changes as appropriate.	□
	You may now want to add another column to your inventory that applies a new priority ranking.	□
	Determine what areas must be addressed immediately, those for the short term, and those that are long range or part of future planning as your practice grows.	□
	Now sort the items by category by your priority code applied and apply timelines and deadlines for completion. Many items will need to be assigned and performed parallel to each other. Some will be subject to completion of prior tasks assigned. Determine the project manager, project management tools to be applied, roles and responsibilities of your task force and team.	□
	And finally, implement your plan.	□
Monitor the Plan – Process in Place		
	To stay on track you will need to consistently monitor and audit the progress of your action plan. Priorities may change and/or shift, but the plan must be completed. Determine the escalation and follow-up steps to changes and audits performed. Fully document and track all progress of your plan. Reassess your plan at regular intervals to determine effectiveness and match to needs identified.	□
Train on and enforce HIPAA policies and procedures		
	Reinforce existing policies and procedures	□
	Introduce and train employees on new ones	□
	Develop a plan to provide updates on a regular basis	□
	Document and maintain files on training provided	□

		Done
Perform on-going audits to ensure compliance		
	This is essential and critical to your practice. Maintain documentation as is appropriate.	□
Stay abreast of new rules and regulations and apply appropriate measures. Modify plans accordingly.		
		□
		□