SAMPLE Remediation Plan

Corrective Action Plan		Risk Recommendation	Risk Management Activity	Actual Remediation	Planned Completion Date	Additional Resources
The domains and content in this column reflects areas that create a risk and breach exposure to the organization.		These are recommendations on how to address the security risks in your organization based on the responses provided in the questionnaire. The column to the right will provide your organization the opportunity to either agree with the recommended course of action, or accept the risk as is.	Choose how your organization will respond to the recommendation (correct risk by following the recommendation or accept risk and do nothing).	If you have chosen to accept risk, please document rationale. If you have chosen to correct risk, please document the actual remediation steps planned and/or taken if different from the recommendations.	Your organization can use this column for setting completion dates and keeping track of remediation progress.	This column provides additional resources, examples and tools that may be beneficial when implementing remediation activities.
1	**Information Security Policies**					
1.1	Does the organization have Information Security Policies defined and documented?	Develop policies for information security as high level documents outlining what needs to be done, but do not dive into any details for how to do it, as a procedure would. Along with providing requirements for what needs to be done, they also serve as a document against which sanctions can be implemented.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practice's operations.	9/30/2013	InfoSec policy manual for identifying Information Security policy definitions and documentation http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331
1.2	Are all HIPAA required policies and procedures defined from a HIPAA compliance perspective?	Develop policies and procedures that meet HIPAA requirements which should be written in order to comply with the specific wording written in the HIPAA rules.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practice's operations.	9/30/2013	U.S. Department of Health and Human Services -HIPAA regulations: http://www.hhs.gov/ocr/privacy/index.html
1.2.A	Do policies/ procedures cover the following areas:					
	Risk Management	Develop a Risk Management (RM) policy which should address objectives, roles and responsibilities, what is considered an acceptable level of risk, and formal processes of identifying risk. Add policy specifying that no paper documents are to be removed from facility.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Risk Management policy and procedure with HIPAA standards: http://www.westhertshospitals.nhs.uk/documents/trust_policies/current/info_risk_management_policy.pdf
	Sanctions	Create or update sanction policies that focus on workforce member who fail to follow privacy or security policies and procedures for the organization.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Sanctions policy and procedure: http://www.chpw.org/assets/file/Sanction-Policy.pdf
	Termination	Create policies that identify termination procedures for voluntary and in-voluntary termination. Identify and provide details for step-by-step analysis of business process termination from supervisors to Human Resources regarding employment termination procedures and account suspension.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Termination policy and procedure: http://www.creighton.edu/fileadmin/user/doit/docs/policies/hipaa/Termination.pdf
	Mobile Media and Device Security	Create an Acceptable Use Policy that end users must sign off that contains clear requirements and expectations for the use of mobile media and devices, including corporate-owned and personally-owned devices that are allowed access to enterprise resources.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Insight: http://www.physicianspractice.com/blog/content/article/1462168/1867882 Policy Template: http://www.sans.org/security-resources/policies/Remote_Access.pdf
	Information System Access	Develop a Information System Access policy that identifies all employees currently requiring information system access for authorized users. Specific documentation should be collaborated for user validation for specified applications and level of access rights for PHI, sensitive data, and information systems from unauthorized access.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Information System Access policy and procedure: http://www.awphd.org/presentations/HIPAAproject/reference/ISaccess.pdf
	Security Training and Awareness	Develop a policy or update the existing Security Training and Awareness policy which requires all employees to periodically review a documented program for security training and awareness (supporting confidentiality, integrity, and availability) of organizational information. The security training and awareness policy should communicate the minimum requirements for all staff members regarding information security awareness and training.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Security Training and Awareness policy and procedure: http://www.nyu.edu/content/dam/nyu/compliance/documents/HIPAA6.SecAware-Train.v8.041505Rev.020211.pdf
	Anti-Malware	Develop a policy and procedure process for anti-malware that deploys a centralized anti-virus and management's software for protection against malicious software. The policy should describe procedural guidelines to detecting, removing, and preventing malware through the anti-virus or management system.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Anti-Malware policy and procedure: http://it.ouhsc.edu/policies/documents/infosecurity/Anti-Virus%20Policy.pdf
	Passwords	Develop a policy or update the existing password policy for password management regarding different levels of passwords (user and system). The policy should detail the standard for creating passwords, the protection of those passwords, and the frequency of change. The duration of password changes should be stated with quarterly basis for system-level and semi-annually for user-level passwords.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Passwords policy and procedure: http://www.sans.org/security-resources/policies/Password_Policy.pdf

SAMPLE Remediation Plan

	Security Incidents	Create or update policies and procedures of security incidents should be identified and presented. Developing security policy and Security Incident Report Forms can help develop an Incident Response Unit focusing primarily on exploitation of organizational information. This policy should establish responsibility and accountability for all steps in the process of addressing computer security incidents which should be clearly identified, contained, investigated, and remedied.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Security Incidents policy and procedure: http://policy.iastate.edu/policy/it/incident/
	Data Backup and Storage	Create policies that identify data backup and storage procedures, content, encryption types, backup types, and storage locations. This policy should outline data backup best practices and define what data needs to be backed up.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Data Backup and Storage policy and procedure: http://dept.wofford.edu/it/Data%20Backup%20Policy.pdf
	Disaster Recovery	Create or update policies and procedures of Disaster Recovery within the organization. Identifying the planning team is critical in developing disaster recovery policies within different sectors of the organization: information security, information technology, human resources, upper management, and operations.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Disaster Recovery policy and procedure: http://www.templatezone.com/pdfs/Disaster-Recovery-policy.pdf
	Third Parties and Business Associates	Communicate third parties and business associates information with policies and procedures for business associate agreement, provisions, breaches, obligations and activities. The BA policy states what requirements are needed to establish a relationship with a third party in compliance with the provisions of HIPAA. Identify third parties with whom BA contracts should be established.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Third Parties and Business Associates policy and procedures: http://www.himss.org/content/files/Code%20165%20HIMSS%20Sample%20BA%20Policy.pdf
	Workstation Acceptable Use	Establish or update policy and procedure documents for workstation acceptable use within the organization. The policy should cover General Use and Ownership Information, Security and Proprietary Information, Unacceptable Use, Communication activities, and Enforcement of all definitions of policies and procedures within Workstation Acceptable Use.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Workstation Acceptable Use policy and procedures: http://www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf
	Disposal	Create or update Disposal policies for computers and removable devices (computer systems, electronic devices, and electronic media). Identify procedures with media sanitization methods: disposal, wiping, destroying, reformatting, and ghosting of all confidential information.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Disposal policy and procedures: http://www.savannahstate.edu/faculty-staff/computer-services/docs/Policies/10-9%20Media%20Disposal%20Policy.pdf
	Media Re-use	Policies involving Media Re-use should detail reuse of hardware devices for reallocation of parts or entire device systems. This policy should define requirements for re-using or re-purposing media that contained prior data which can be complied within the Disposal policy.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Media Re-Use policy with HIPAA standards: http://www.creighton.edu/fileadmin/user/doit/docs/policies/hipaa/Media_disposal_and_reuse.pdf
	Unique User IDs	Access Control should be communicated within Unique User IDs policies and procedures. The procedure of this policy should be effectively communicated with System Administrators and Information Security Officers.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Unique User IDs policy with HIPAA standards: http://www.creighton.edu/fileadmin/user/doit/docs/policies/hipaa/Unique_ID.pdf
	Person/ Entity Authentication	Create or update Person/ Entity Authentication for all workforce members seeking access to network, system, applications with PHI information through required authentically procedures. Policy should detail misrepresentation violations and no delegation of authorized access authentication information. State repercussion if policy is violated. Outline business process of authentication procedures within the organization.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Example of Person / Entity Authentication policy with HIPAA standards: http://www.creighton.edu/fileadmin/user/doit/docs/policies/hipaa/Authentication.pdf
	PHI Security (ePHI)	Develop or update the policy on PHI security, which should outline minimum standards for ensuring the confidentiality, integrity, and availability of electronic protected health information (ePHI) received, maintained or transmitted by the organization.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Website link for PHI Security policy: http://www.upenn.edu/computing/security/policy/ePHI_Policy.html
	PHI Transmission Protection (email)	Develop or update the policy requiring the secure transmission of confidential or sensitive information (e.g., PHI). All transmissions exchanged with a third party or which occur over open, public networks (e.g., the Internet) shall be secured including email, FTP, and HTTP. Any transmissions sent shall be encrypted using modern standards with a minimum strength of 128-bit.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	Website link for PHI Security policy: http://www.upenn.edu/computing/security/policy/ePHI_Policy.html
1.3	Does senior management sign off on the approval of information security policies and standards for the organization?	Develop or update policies and standards which should be approved by senior management to ensure that they are enforceable and are applicable across the entire organization.	Correct Risk	Contracted with third party to develop policies. We will augment policies with any procedures specific to Medical Practrice's operations.	9/30/2013	This Policy Development Guide outline Senior Management sign-off approvals for information security policies and standard: http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331