SAMPLE Risk Analysis Report for [Name of Clinical Application]

Overview

This report summarizes the residual risks inherent in organizational practices based upon the assessment and analysis conducted in _____ (date) and documented within a risk profile.

Report date:	[date of report]
Information/Data Owner:	[name of information owner – executive] [their job title] [information owner's department]
Primary author of report:	[author of report] [their job title] [their department]

System description

Business functions:	Electronic Medical Record (EMR)
Sensitivity of information:	Confidential, ePHI
Criticality of information:	Critical

[name of application] is the electronic medical record (EMR). **[name of clinical application]** runs on _____ *(types of servers and operating system)*. The servers are housed _____ *(locally in the server room, at a remote data center, or at the vendor site)*. Data is stored on ___ *(a SAN and backed up to another SAN)*. Daily incremental backups are created and full backups are created weekly and stored ____ *(off-site?)*. Backups are *(or are not)* encrypted. The risk profile, upon which this report was based, primarily addresses the threats to the application and the data.

Description of Risk Analysis Approach

The risk analysis process was based upon common practices and guidelines from National Institute of Standards and Technology (NIST). An interview was conducted to determine the existing security controls and vulnerabilities. Then a risk profile was created which defines the most probable threats capable of exploiting the vulnerabilities inherent in the system after considering existing security safeguards and controls. Risks were assigned a numerical value corresponding to the rating of the likelihood and the resulting impact if the threat was realized. Threats rated with a numerical score and those with the highest risk scores represent the greatest risks. The table illustrates how risks were rated. Likelihood and Impact are each rated as either: "H" (high = 3); "M" = (medium = 2); "L" = (low = 1). Threats rated with a numerical score of a two or less were considered well within the organizational threshold of risk tolerance and were not considered for remediation.

Likelihood	Impact	Risk Score	Color Rating
H	H	9	Red
H	M	6	
M	H	6	
M	M	4	Yellow
H	L	3	
L	H	3	
M	L	2	Green
L	M	2	
L	L	1	

Analysis team members:

(list team members' names here; if necessary include titles and contact information)

Findings (Yellow = 4 or 3) *(listed in order of priority)*

The following findings rated risk scores of **4** and should be given some consideration for remediation:

1. IT assigns users their password and it does not change; minimum password length is set at three characters and complexity rules are not enforced
2. No auto logoff after a predetermined period of inactivity
3. Notification from HR when an employee leaves is not consistent; HR may not always provide notification when an employee changes jobs, is on medical disability, or is placed on disciplinary suspension
4. Managers are not periodically provided a listing of their employees and their access privileges to review and verify that their access is appropriate
5. Inactive user accounts (Ex: More than 30 days since last use) are not disabled
6. Users can have concurrent logons under the same user ID
7. Audit logs are not regularly reviewed and are primarily used for problem solving
8. No warning banner displayed at logon prompt notifying users that their activities are being monitored and audited
9. Users are not required to receive training in order to receive their password

The following selected finding rated a risk score of **3** which is generally an acceptable level of risk, but these selected vulnerabilities should also be given some considered for remediation either because of their potential impact or because they are easy to resolve:

10. Server Room lacks many of the basic physical and environmental security controls

    Note: *While the probability of the threat being realized is low, the impact would be unacceptable*

Recommendations

The following recommendations *(listed in order of priority)* should be considered to help reduce risks:

Suggested Controls	**Estimated Resources** (Capital, Expense, and Hours)	**Possible End User Impact(s)**	**Owner's Decision** √ = Yes X = No
1. Set users' passwords to a minimum length of six or more characters and if possible, enforce complexity and initial and periodic expiration	30 hrs to implement password rule changes and notify users	Users may complain about changing their passwords	
2. Consider establishing an auto logoff after 10 minutes of inactivity or activating computer workstation screen savers (in patient care areas) to trigger within five minutes to prevent incidental disclosure of PHI	5 hrs to investigate auto logoff capabilities 5 hrs to obtain buy-in 2 hrs to implement	Users may complain about being frequently logged off from the application	
3. Establish a process so that HR quickly notifies IT when an employee terminates, changes jobs, is on medical leave, or is placed on disciplinary suspension	3 hrs to review termination notification process	None	
4. Work with managers on periodically reviewing user access privileges and roles to determine if access is appropriate	10 hrs every 6 months to review user access rights	None – except for users who have had excessive privileges	
5. Create a process to automatically disable user accounts that have been inactive for 60 or more days since last log on	5 hrs annually to review manually; __hrs to automate	None	
6. Eliminate concurrent logon capability	2 hrs to assess the feasibility; 1 hr to implement	It could prevent users from sharing their passwords	
7. Formalize audit log review process and responsibilities	3 hrs to formalize log review process; 4 hrs/week to review	Users may be less likely to snoop if they are audited	
8. Create a warning banner that notifies users of auditing and monitoring	2 hrs to create and implement	It may slow down the logon process	
9. Consider requiring users to attend training prior to granting access to the application; training should include privacy and security requirements	5 hrs to determine the feasibility 15 hrs to implement	Users would have to take time off from their job to attend the training	
10. Implement new physical and environmental controls outlined in the risk profile **– OR –**	$35K to update Server Room with controls	None	
Move production servers to a Tier III or IV commercial data center [Transfer the risk]	$2K per month hosting fee	None	

Key for Information/System Owner's Decision:

√ = Yes (The suggested control will be implemented to reduce risks or in some rare cases, transfer the risk)

X = No (The owner has decided to accept the risk)

Information/System Owner Comments

(The Information/Data Owner can note any exceptions to the risk profile, findings, or recommendations.)

_____

_____

_____

_____

_____

Statement of Understanding

I, the Information/System Owner, understand that the vulnerabilities identified in this report could cause a negative impact to business operations if the threat was realized. For each recommendation in this report, I have determined whether risks will be mitigated by implementing the recommended controls, transferred or insured against, or accepted. I understand that choosing to accept the risks could adversely affect business operations and/or result in noncompliance with regulatory requirements.

I have been informed of the risks for operation of the system in its current configuration.

_____

Information/Data Owner or Designee Date