#

Security Self-Assessment

**Table of Contents**

[Introduction 2](#_Toc410899289)

[Objectives 2](#_Toc410899290)

[Approach 2](#_Toc410899291)

[Answering the Self-Assessment Questions 2](#_Toc410899292)

[Security Self-Assessment Questions 3](#_Toc410899293)

[Policy and Procedure Management 3](#_Toc410899294)

[Physical Security 4](#_Toc410899295)

[Password Management 6](#_Toc410899296)

[User Role Management 6](#_Toc410899297)

[Information Technology 7](#_Toc410899298)

[Wireless Network 9](#_Toc410899299)

[Monitoring and Enforcement 10](#_Toc410899300)

[Third Party Agreements 11](#_Toc410899301)

[Security Modifications and Improvements 12](#_Toc410899302)

[Action Plan 12](#_Toc410899303)

[Questionnaire Interviewees 12](#_Toc410899304)

The information in this assessment is provided for education and guidance only and is not intended to replace expert advice. Physicians are responsible for making informed decisions to meet their medical-legal obligations.

# Introduction

Security self-assessments are conducted by clinics to determine if there are gaps in a clinic’s security policies, practices and procedures.

## Objectives

The purpose of the security self-assessment is to:

* Enable a clinic to analyze its security policies, procedures and practices.
* Identify security risks that are present in a clinic and determine if the existence of clinic controls are in place to mitigate those risks.
* Develop and implement security improvements and controls where necessary to reduce clinic security risks.

## Approach

The security self-assessment is used as an evaluation tool to help clinics review security policies and practices annually and identify areas for improvement.

The questions can be answered in two ways:

1. Answer the assessment questions based on an understanding of how processes within the clinic operate without providing or confirming the existence of documentation of the process, but by describing the procedure in effect at the clinic.

For example, one question asks the following: “Does the clinic have established policies and procedures that mandate the safeguarding of personal information by all clinic staff?” The clinic may respond to this question by indicating that the procedure in place requires support staff to shut off their computers at the end of each workday. No documentation needs to be provided to confirm this practice within the clinic.

1. Answer the assessment questions based on an understanding of how processes within the clinic operate and provide documentation of the process within the clinic.

For example, one question asks the following: “Does the clinic have established policies and procedures that mandate the safeguarding of personal information by all clinic staff?” The clinic may respond to this question by referencing the existence of a checklist that is completed each night by the clinic manager verifying that all computers have been shut off at the end of a workday.

The first approach helps clinics gain a general idea of the security policies and practices implemented within the clinic. This helps the clinic identify areas for improvement and areas that require more stringent security measures.

The second approach provides the clinic with confirmation that security policies and procedures in the checklist are implemented within the clinic and are being followed consistently.

## Answering the Self-Assessment Questions

The Privacy Self-Assessment Questions in the following table can be answered by clicking in the available fields. Entered content can be saved using the File > Save As command which enables you to save your current answers and reopen your assessment to complete it at a later time.

# Security Self-Assessment Questions

The following questions are categorized by the type of security the questions address.

1. In the “How is it confirmed that the policy or procedure is operating in the clinic?” column, identify what evidence is available to confirm that the policy and or procedure is currently operating in the clinic.
2. In the “Reference the name of the policy or procedure that answers the question” column, identify the name of the clinic policy or procedure that addresses or answers the question.

| **Questions** | **1. How is it confirmed thatthe policy or procedure is operating in the clinic?** | **2. Reference the name of the policy or procedure that answers the question** | **Notes and comments** |
| --- | --- | --- | --- |
| Policy and Procedure Management |
| 1. Are security policies and procedures implemented within the clinic?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are security policies and procedures reviewed and updated regularly in the clinic?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are appropriate background checks performed on potential clinic employees during the hiring process?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Who is responsible for performing background checks on potential clinic employees during the hiring process?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Have all clinic staff members reviewed clinic security policies and procedures, including revisions as added?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are clinic staff regularly trained or provided with refreshers on security policies and procedures?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Have the clinic’s third-party vendors been provided with a copy of the clinic’s security policies and procedures?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are access control items used and recorded with an employee confidentiality and security checklist (e.g., key FOBs, door keys, pass codes, swipe cards)?

What items are tracked, and is the list updated as needed? | **Y [ ]** **N [ ]**  |  |  |  |
| Physical Security |
| 1. Does the clinic have an alarm system?
* Is it armed every day?
* Do only required staff members have access?
* Do users have individual pass codes for the alarm (non-shared)?
* Are the alarm codes changed, and how frequently?
* Is the alarm access log monitored, and by whom?
 | **Y [ ]** **N [ ]** **Y [ ]** **N [ ]** **Y [ ]** **N [ ]** **Y [ ]** **N [ ]** **Y [ ]** **N [ ]** **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are laptops properly secured when in use during office hours?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are laptops properly secured or stored when not in use and after office hours?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are computer and laptop screens secured from public view and access within the clinic?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are workstations secured during office hours and after office hours?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are patient records in paper format secured away from public view and access within the clinic?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are clinic fax machines located in a secure area away from public view and access?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Do fax machines use pre-set numbers (speed dial)?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are staff members required to confirm recipient’s receipt of fax?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Is paper-based information (including patient charts) securely destroyed at the end of its lifecycle? If so, how is the paper-based information destroyed? How is this process documented?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Does the clinic have fire extinguishers, smoke detectors, deadbolt locks, and other general security provisions in place within the clinic?
 | **Y [ ]** **N [ ]**  |  |  |  |
| Password Management |
| 1. Are clinic staff members required to change their password to access clinic computers or laptops every 90 days?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are clinic staff members required to change their password to access the clinic electronic medical record (EMR) every 90 days?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are password standards currently enforced in the EMR and clinic computers? Do these standards include the following?
* Required minimum length?
* Uppercase and lowercase letters?
* Numbers?
* Special characters?
* Number of days for password expiry?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are alarm system codes changed on a regular basis?
 | **Y [ ]** **N [ ]**  |  |  |  |
| User Role Management |
| 1. Is an approval process in place for clinic staff to obtain a user ID and password to access the EMR? What approvals must be attained?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Is an approval process in place for clinic staff to obtain a user ID and password to access clinic computers? What approvals must be attained?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Is a clinic staff member responsible for assigning clinic staff to the appropriate user group in the EMR? Who is the clinic staff member?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are there approvals in place to re-assign clinic staff members to a different user group in the EMR? What approvals must be attained?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are clinic staff members assigned unique user IDs, and are staff members prohibited from sharing their user IDs?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are clinic staff members assigned appropriate user access rights, and not administrative rights to the EMR and computer network? Does this include the physicians and clinic manager?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Who has access to the administrative accounts for the EMR and the computers?
 |  |  |  |
| 1. Are only required staff members given access to specific EMR functionality, such as clinic billing?
 | **Y [ ]** **N [ ]**  |  |  |  |
| Information Technology |
| 1. When a computer or laptop has been idle for five minutes, does a password-protected screensaver automatically display and lock the computer or laptop?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are staff members advised to lock their workstations if they leave them unattended (using “ctrl-alt-del” key combination)?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. When a user is logged into the EMR and has been idle for more than 30 minutes, is the user automatically logged off the EMR?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Who has administrator access to configure and modify EMR settings?
 |  |  |  |
| 1. Are hard drives in computers and laptops encrypted?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Do laptops have the same security measures as workstations computers, (e.g., power-on passwords, encryption, renamed administrator account, personal firewall)?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are users prohibited from using mobile data devices (e.g., iPods, flash memory sticks, external hard drives) on computers and laptops that access the EMR?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. How does the clinic back up their EMR data, including personnel files, email and other clinic information?
* Is the backup encrypted?
* Where is the backup device kept?
 |  |  |  |
| 1. Is the clinic using anti-virus or anti-spyware software?
* Is the software updated automatically?
* When are scan logs reviewed, by whom, and how frequently?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. How is the clinic maintaining properly secured Internet access?
* Is it using a router with firewall protection?
* Has the default router password been changed?
* Are driver updates applied to the router?
* Are non-required access ports on the router disabled?

**(Note:** If you are unsure about these, contact the service provider that installed your router.**)** |  |  |  |
| 1. Are software updates done automatically, particularly Windows security updates?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are computers set to automatically clear browser history, cache, cookies, etc.?
 | **Y [ ]** **N [ ]**  |  |  |  |
| Wireless Network |
| 1. Is the clinic’s wireless network encrypted using a Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2) standard?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Is the wireless router out of public view and access?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Does the router have a unique SSID (Service Set Identifier)?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Has MAC (Media Access Control) address filtering been implemented?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are wireless network scans performed to check for potential connectivity issues such as other businesses on the same wireless network channel?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. If a clinic laptop is used outside of the clinic, are remote connections achieved via a secure wireless connection, a free wireless “hotspot” or a cellular connection (using a mobile “Rocket Stick” or similar)?
 |  |  |  |
| Monitoring and Enforcement |
| 1. Are audit logs reviewed in the EMR regularly? Who conducts these reviews?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are the clinic’s computer network audit logs reviewed regularly and by whom?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are the clinic’s router audit logs reviewed regularly and by whom (to detect potential network access attempts from the Internet)?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Who is monitoring access and use of Netcare by clinic staff members?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Is staff Internet usage restricted and monitored? Who is responsible for this?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Who is responsible for enforcing and monitoring clinic staff compliance with clinic security policies and procedures?
 | **Y [ ]** **N [ ]**  |  |  |  |
| Third Party Agreements |
| 1. Are vendors required to adhere to a code of conduct and report all security incidences or breaches to the clinic as part of their contractual terms?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are vendors required to sign Vendor Confidentiality Non-Disclosure Agreements as part of contractual terms?
 | **Y [ ]** **N [ ]**  |  |  |  |
| 1. Are vendors required to sign Information Manager Agreements and Information Sharing Agreements as part of contractual terms?
 | **Y [ ]** **N [ ]**  |  |  |  |

# Security Modifications and Improvements

When the Security Self-Assessment questions are complete, it’s important to review your answers and determine if any security processes or procedures are being overlooked in your clinic.

Identify the processes and or procedures that need to be implemented and develop an action plan that addresses when and how they can be made operational. This action plan should be based on priority.

Some considerations in developing these modifications and improvements include but are not limited to:

* Any urgent or high-risk areas of concern which need to be addressed immediately
* Processes and procedures that can be improved within the clinic to strengthen security controls
* Regularly scheduled reviews of clinic security policies and procedures
* Any upcoming clinic changes that will affect clinic security policies and procedures that need to be addressed

## Action Plan

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Action** | **Date and Time** | **Responsible Party** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Questionnaire Interviewees

|  |  |  |
| --- | --- | --- |
| **Interviewees** | **Date and Time** | **Location and Role** |
|  |  |  |
|  |  |  |
|  |  |  |