Security Risk Analysis

ExamWRITER®

In this chapter:

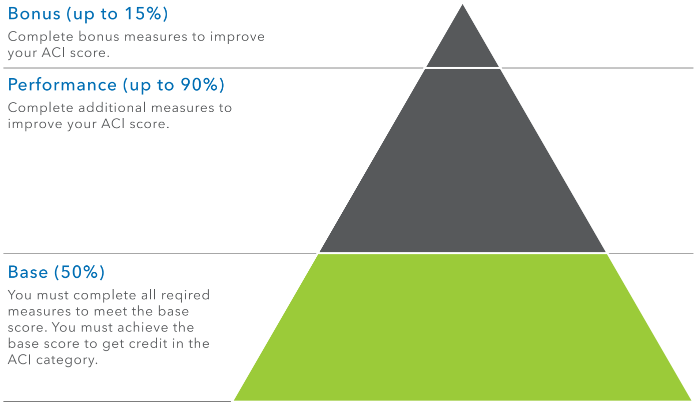
The objective of this measure is to protect electronic health information created or maintained by the certified EHR through the implementation of appropriate technical capabilities.

Measure

Conduct or review a security risk analysis in accordance with the requirements in 45 CFR §164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by a certified EHR in accordance with requirements in 45 CFR §164.312(a)(2)(iv) and 45 CFR §164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the MIPS-eligible clinician's risk management process.

Scoring

This measure is required for the ACI base score of 50%.



Bonus (up to 15%)
Complete bonus measures to improve your ACI score.

Performance (up to 90%)
Complete additional measures to improve your ACI score.

Base (50%)
You must complete all reqired measures to meet the base score. You must achieve the base score to get credit in the ACI category.

Requirements

To meet this measure, eligible clinicians must attest *yes* to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies.

OfficeMate/ ExamWRITER Instructions

OfficeMate/ExamWRITER received ONC-ATCB 2011/2012 certification as a Complete EHR by CCHIT and therefore contains the following features to protect your electronic health information. You may use some or all of these features as part of your comprehensive security plan.

Setting Up Security in OfficeMate/ExamWRITER

If desired, set up security in OfficeMate/ExamWRITER by following the instructions below. For more detailed instructions, see the *OfficeMate Administration User's Guide*.

1. In OfficeMate/ExamWRITER Administration, click **Setup** and select **Security**.
2. Click **Role Maintenance** and set up a new role or modify the name and description or copy an existing role. You can set up as many roles as desired.
3. Select a role on the left side of the window and define its details. The roles can be as broad or as limiting as you desire.
4. Click the **Users** tab and assign role to users. You can assign as many roles as desired to users. All users will initially be automatically assigned to a default administrator role, which allows them access to all products, modules, and tasks in all locations, until you modify their role assignments. To grant users read-only emergency access to ExamWRITER, select the **Allow Emergency Access** check box; users with emergency access must identify the emergency situation when logging into ExamWRITER and type their reason for using the emergency access login.
5. Click the **Preferences** tab and set up security preferences for your locations.
6. Click **Secure Reports** and restrict user access to reports.
7. Click **Print** to print the Security Roles Report that displays the roles that you set up.
8. Click **Close**.

Encrypting Data in OfficeMate/ExamWRITER

By default, OfficeMate/ExamWRITER encrypts patient and provider protected health information (PHI) in your database. If you need to disable or re-enable encryption, perform the following steps.

NOTE	Passwords are encrypted within the database regardless of whether the rest of the database is encrypted or not; this functionality requires no action on your part.

1. Back up your data!
2. In OfficeMate/ExamWRITER Administration, click **Setup** and select **Encrypt/ Decrypt Database**.
3. Click **Encrypt**.

Auditing in OfficeMate/ExamWRITER

To view the activities of OfficeMate/ExamWRITER users in your practice, track changes made to a particular patient's record, and view changes made to a specific exam, follow the instructions below:

1. In OfficeMate/ExamWRITER Administration, click **Setup** and select **Audit Log Management**.
2. Select the **Event Types** check boxes, as needed.
3. Click **Save/Exit**.
4. In OfficeMate Administration, click **Setup** and select **Audit Log Review**.
5. Record search criteria in the top of the window and click **Search** to find logs that meet your search criteria. Click **Print** to print the audit log search results or double-click on a log to view more details about it. To verify the integrity of an audit log entry that you have opened, click **Validate**.

Responsible Role

The following are suggested roles for completing this measure:

- Doctor
- Office Manager
- Technician
- Front Desk

NOTE Protecting patient information is the responsibility of everyone in the practice. One person in the practice should be appointed the privacy officer, and that person should oversee the security risk analysis each calendar year.

Audit Advice

Due to the scope of the measure, this audit advice is divided into sections.

- Security Risk Analysis, 3
- Encryption, 4

Security Risk Analysis

Document and date your security risk analysis each year.

You cannot fulfill this measure simply by turning a security feature on or off. Your practice must conduct, at least once per year, a comprehensive security risk analysis in accordance with the requirements under HIPAA (45 CFR §164.308(a)(1)) and correct identified security deficiencies.

OfficeMate/ExamWRITER includes some features, which you may choose to enable as *part* of your overall security plan, but you cannot stop there. Questions you would need to answer as part of a security audit include, but are not limited to:

- Does the practice have antivirus or antimalware software installed, enabled, and current on every computer and server? Are operating system security patches up-to-date and installed on every workstation and the server?
- Is the practice's network protected by a firewall? How often are the settings verified?
- Are mobile phones, tablets, laptops, desktops, and other devices used to access and transmit PHI password protected and encrypted?
- How is PHI removed from mobile phones, tablets, laptops, desktops, and other devices—including printers and fax machines—before disposition?
- Where is PHI collected, stored, maintained, and transmitted? What are the potential security threats and how likely are those threats?
- Does the practice have business associate contracts with all vendors that outline who is responsible and how PHI is protected?
- Is everyone in the practice trained in HIPAA? How is that education kept current?
- Does the practice have written, up-to-date policies and procedures in place regarding protecting PHI?
- How is the practice prepared to protect and restore PHI in case of natural or man-made disaster?
- How are off-site backups protected?

HIPAA rules strictly forbid us or you from distilling the security analysis down to a simple checklist. Security needs vary drastically from practice to practice. Refer to the *ONC Guide to Privacy and Security of Health Information* at http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf for further guidance.

Encryption

Although encryption is not strictly required by 45 CFR §164.312 (a)(2)(iv), encryption is enabled by default in OfficeMate/ExamWRITER v11.1 and later. You may decrypt your OfficeMate/ExamWRITER database, provided you meet the following criteria:

- During your security risk analysis, you determine that encryption is not a reasonable and appropriate safeguard of the confidentiality, integrity, and availability of PHI;
- You document your security risk determination; and
- You implement an equivalent alternative measure that is reasonable and appropriate.

If you maintain PHI in other systems, you must also check the encryption settings in those systems.