Security Risk Assessment Checklist (Traditional Server)

This document is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR for Promoting Interoperability and MIPS Stage 3.

first insight

Table of Contents

Assessing Risks Regarding EHRs and Other Health IT Within Your Health Care Practice

Questions to Ask Yourself When Assessing Confidentiality Risks

Question/Threat	Response	Level of Risk/Comments	Date/Initial
What new electronic health information has been introduced into my practice because of EHRs? Where will that electronic health information reside?	• Patient electronic Protected Health Information (ePHI) will reside on the server and will be accessed over the network via a workstation. • All scanned documents and imported documents from the local drive should be kept at a secure location or removed after importing them in the application. Any document exported from the application should be kept at a secured location. • Data protection tools such as BitLocker Drive Encryption can be used.		
Who in my office (employees, other providers, etc.) will have access to EHRs, and the electronic health information contained within them?	• Your administrator should setup individual user names and passwords for each person that will access the EHR. • Newly added users can have permission sets assigned to ensure proper role-based access.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Security Risk Assessment Checklist (Traditional Server)

This document is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR for Promoting Interoperability and MIPS Stage 3.

first insight

Questions to Ask Yourself When Assessing Confidentiality Risks

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Should all employees with access to EHRs have the same level of access?	• Your administrator should set up each user with access to the parts of the EHR that pertains to their position. • Newly added users can have permission sets assigned to ensure proper role-based access.		
Will I permit my employees to have electronic health information on mobile computing/storage equipment? If so, do they know how and do they have the resources necessary, to keep electronic health information secure on these devices?	• It's critical that every eye care practice has an updated HIPAA employee handbook that documents internal policies and procedures. Your employees must sign a statement that confirms they read, understand, and agree to comply with privacy, security, and confidentiality policies. • Never leave mobile computing devices (laptops, tablets, mobile phones, Bluetooth devices, memory cards, flash drives, and external hard drives) unattended or in an exposed or unsecured area. Use encryption when storing ePHI on mobile computing devices. Password-protect every mobile device.		
How will I know if electronic health information has been accidentally or maliciously disclosed to an unauthorized person?	• Periodically check the EHR audit log for unauthorized or malicious activity. • You should also create a contingency plan and review/renew it regularly.		
When I upgrade my computer storage equipment (e.g., hard drives), will electronic health information be properly erased from the old storage equipment before I dispose of it?	• Consult your IT Administrator.		
Are my backup facilities secured (computers, tapes, offices, etc.) used to backup EHRs and other health IT)?	• Consult your IT Administrator.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Security Risk Assessment Checklist (Traditional Server)

This document is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR for Promoting Interoperability and MIPS Stage 3.

Questions to Ask Yourself When Assessing Confidentiality Risks

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Will I be sharing EHRs, or electronic health information contained in EHRs with other health care entities through a Health Information Organization (HIO)? If so, what security policies do I need to be aware of?	• Consult your IT or Practice Administrator.		
If my EHR system is capable of providing my patients with a way to access their health record/information via the Internet (e.g., through a portal), am I familiar with the security requirements that will protect my patients' electronic health information before I implement that feature?	• First Insight's patient health records portal, EyeClinic.net (integrates with MaximEyes EHR), offers patients access to their ePHI. • Patient portal data will only be accessible by the patient with a valid username and password that will be created by that patient.		
Will I communicate with my patients electronically (e.g., through a portal or email)? Are those communications secured?	• First Insight's patient health records portal, EyeClinic.net, allows staff and providers to communicate with the patient. • Patients must sign-in to EyeClinic.net using their secure login and passwords to view their ePHI.		
If I offer my patients a method of communicating with me electronically, how will I know that I am communicating with the right patient?	• First Insight's patient health records portal, EyeClinic.net, only allows communications to be sent while the staff or providers are viewing the patient's ePHI.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Questions to Ask Yourself When Assessing Integrity Risks

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Who in my office will be permitted to create or modify an EHR, or electronic health information contained in the EHR?	• The User Administrator can enable or remove privileges for creating, editing, or deleting ePHI. In MaximEyes EHR, each user will have individual login/password to access the EHR.		
How will I know if an EHR, or the electronic health information in the EHR, has been altered or deleted?	• Within MaximEyes EHR, the Audit Trail tracks changes to ePHI and has a search function to display a list of audits preformed on any patient’s ePHI. • The Audit Trail is encrypted and the administrator has the ability to restrict user access to the Audit Trail.		
If I participate in a HIO, how will I know if the health information I exchange is altered in an unauthorized manner?	• Consult your IT or Practice Administrator.		
If my EHR system is capable of providing my patients with a way to access their health record/information via the internet (e.g., through a portal) and I implement that feature, will my patients be permitted to modify any of the health information within their record? If so, what information?	• First Insight’s patient health records portal, EyeClinic.net, allows patients to modify their Medical History and patient demographic information. • Any Medical History information altered by the patient will be flagged for the provider or authorized staff to review.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Questions to Ask Yourself When Assessing Availability Risks

Question/Threat	Response	Level of Risk/Comments	Date/Initial
How will I ensure that electronic health information, regardless of where it resides, is readily available to me and my employees for authorized purposes, including after normal office hours?	• With MaximEyes, when software updates or maintenance are scheduled, your office will be notified in advance if the database will be offline.		
Do I have a backup strategy for my EHRs in the event of an emergency, or to ensure I have access to patient information if the power goes out or my computer crashes?	• Consult your IT Administrator.		
If my EHR system is capable of providing my patients with a way to access their health record/information via the Internet (e.g., through a portal) and I implement that feature, will I allow 24/7 access?	• First Insight's patient health records portal, EyeClinic.net, allows patients to access the portal 24/7. • Notifications will be posted alerting users of any temporary disruption of service.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Identifying Safeguards for EHRs and Other Health IT Within Your Health Care Practice

Questions to Ask Yourself When Identifying Administrative Safeguards

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Have I updated my internal information security processes to include the use of EHRs, connectivity to HIOs, offering portal access to patients, and the handling and management of electronic health information in general?	• Create a contingency plan and review/renew the plan regularly.		
Have I trained my employees on the use of EHRs? Other electronic health information related technologies that I plan to implement? Do they understand the importance of keeping electronic health information protected?	• First Insight provides training resources for MaximEyes via one-on-one trainer time (onsite and online), documents and guides, Computer Based Training (CBT) videos, searchable FAQs on the For Customers website, and webinars (live and recorded).		
Have I identified how I will periodically assess my use of health IT to ensure my safeguards are effective?	• Consult your IT Administrator.		
As employees enter and leave my practice, have I defined processes to ensure electronic health information access controls are updated accordingly?	• The user's login should be removed from your EHR.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Security Risk Assessment Checklist (Traditional Server)

This document is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR for Promoting Interoperability and MIPS Stage 3.

Questions to Ask Yourself When Identifying Administrative Safeguards

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Have I developed a security incident response plan so that my employees know how to respond to a potential security incident involving electronic health information (e.g., unauthorized access to an EHR, corrupted electronic health information)?	• Review the Audit Trail in the event of a security incident. • In MaximEyes, the Audit Trail tracks changes to ePHI and has a search function to display list of audits preformed on ePHI. The Audit Trail is encrypted and the administrator has the ability to restrict user access to the audit trail. • Workstations may contain exported ePHI from the application.		
Have I developed processes that outline how electronic health information will be backed-up or stored outside of my practice when it is no longer needed (e.g., when a patient moves and no longer receives care at the practice)?	• Consult your IT Administrator.		
Have I developed contingency plans so that my employees know what to do if access to EHRs and other electronic health information is not available for an extended period of time?	• It's critical that every eye care practice has an updated HIPAA employee handbook that documents internal policies and procedures. • Your employees must sign a statement that confirms they read, understand, and agree to comply with privacy, security, and confidentiality policies.		
Do I have a process to periodically test my health IT backup capabilities, so that I am prepared to execute them?	• Consult your IT Administrator.		
If equipment is stolen or lost, have I defined processes to respond to the theft or loss?	• The patient ePHI will be stored only on the server and should only be accessible via the local network. Workstations will not contain any patient ePHI.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Questions to Ask Yourself When Identifying Physical Safeguards

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Do I have basic office security in place, such as locked doors and windows, and an alarm system? Are they being used properly during working and non-working hours?	• Consult your IT and Practice Administrator. • It's critical that every eye care practice has an updated HIPAA employee handbook that documents internal policies and procedures. For more information about HIPAA privacy and ePHI security, refer to First Insight's HIPAA Compliance Guide for Eye Care Professionals.		
Are my desktop computing systems in areas that can be secured during non-working hours?	• Consult your IT and Practice Administrator. • It's critical that every eye care practice has an updated HIPAA employee handbook that documents internal policies and procedures. For more information about HIPAA privacy and ePHI security, refer to First Insight's HIPAA Compliance Guide for Eye Care Professionals.		
Are my desktop computers out of the reach of patients and other personnel not employed by my practice during normal working hours?	• Consult your IT and Practice Administrator. • It's critical that every eye care practice has an updated HIPAA employee handbook that documents internal policies and procedures. For more information about HIPAA privacy and ePHI security, refer to First Insight's HIPAA Compliance Guide for Eye Care Professionals.		
Is mobile equipment (e.g., laptops), used within and outside my office, secured to prevent theft or loss?	• Consult your IT and Practice Administrator. • It's critical that every eye care practice has an updated HIPAA employee handbook that documents internal policies and procedures. For more information about HIPAA privacy and ePHI security, refer to First Insight's HIPAA Compliance Guide for Eye Care Professionals.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Security Risk Assessment Checklist (Traditional Server)

This document is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR for Promoting Interoperability and MIPS Stage 3.

first insight

Questions to Ask Yourself When Identifying Technical Safeguards

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Have I configured my computing environment where electronic health information resides using best-practice security settings (e.g., enabling a firewall, virus detection, and encryption where appropriate)? Am I maintaining that environment to stay up to date with the latest computer security updates?	• Consult your IT Administrator.		
Are there other types of software on my electronic health information computing equipment that are not needed to sustain my health IT environment (e.g., a music file sharing program), which could put my health IT environment at risk?	• Consult your IT Administrator.		
Is my EHR certified to address industry recognized/best-practice security requirements?	• MaximEyes EHR is an ONC 2015 Complete Certified EHR and meets the General certification criteria (§170.314) for Complete EHRs or EHR Modules.		
Are my health IT applications installed properly, and are the vendor recommended security controls enabled (e.g., computer inactivity timeouts)?	• By default, in MaximEyes, the Audit Trail and automated logout features are already enabled.		
Is my health IT computing environment up to date with the most recent security updates and patches?	• First Insight provides regular updates to MaximEyes EHR. First Insight also recommends that your practice use the services of a professional/certified IT person to maintain a secure network environment.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.

Security Risk Assessment Checklist (Traditional Server)

This document is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR for Promoting Interoperability and MIPS Stage 3.

first insight

Questions to Ask Yourself When Identifying Technical Safeguards

Question/Threat	Response	Level of Risk/Comments	Date/Initial
Have I configured my EHR application to require my employees to be authenticated (e.g., username/password) before gaining access to the EHR? And have I set their access privileges to electronic health information correctly?	• First Insight provides an administrator login and password to a designated administrator. • The administrator can then set up each user with appropriate access to MaximEyes EHR and patient ePHI information.		
If I have or plan to establish a patient portal, do I have the proper security controls in place to authenticate the patient (e.g., username/password) before granting access to the portal and the patient's electronic health information? Does the portal's security reflect industry best-practices?	• Yes. First Insight's patient health records portal, EyeClinic.net, has user logins and passwords that are required for access to patient ePHI.		
If I have or plan to set up a wireless network, do I have the proper security controls defined and enabled (e.g., known access points, data encryption)?	• Consult your IT Administrator.		
Have I enabled the appropriate audit controls within my health IT environment to be alerted of a potential security incident, or to examine security incidents that have occurred?	• Review the Audit Trail in the event of a security incident. • In MaximEyes, the Audit Trail tracks changes to ePHI and has a search function to display a list of audits preformed on ePHI. The audit log is encrypted and the administrator has the ability to restrict user access to the audit trail.		

Source/Reference: The questions listed in this Security Risk Assessment Checklist are from the HealthIT.gov Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. This resource is a reference and starting point only to help optometry and ophthalmology practices assess their health information technology (health IT) and to conduct a HIPAA security risk assessment as it relates to an EHR. This document does NOT guarantee that the office will meet promoting interoperability, meaningful use, or MIPS criteria for a security audit.