Example of the HIPAA Security Risk Assessment Report

from HIPAA Risk Analytics, LLC

Security Risk Assessment for Florida Urgent Care

Florida Urgent Care

123 Security Way
Tallahassee, Florida 32309

1/15/2020

Introduction

Conducting a Risk Assessment is mandated by the Health Information Portability and Accountability Act. Its objective is to "ensure that electronic health information created or maintained by certified EHR technology is thoroughly protected through the implementation of appropriate technical capabilities." HIPAA requires each health care provider's office to "conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a) (1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process." No exclusions are allowed.

The Security Risk Assessment template employed was developed by HIPAA Risk Analytics, LLC, in an online format. It is based on guidance from the Office of Civil Rights, the Centers for Medicare & Medicaid Services and the National Institute of Standards and Technology. This risk analysis report is created for Florida Urgent Care at 123 Security Way, Tallahassee, Florida 32309. The results of the security risk assessment survey are reported below along with recommendations for HIPAA compliance.

Health Insurance Portability and Accountability Act (HIPAA) Security Rule

The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the HIPAA Privacy Rule by addressing the technical and non-technical safeguards that "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI). The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction. 1

According to Section § 164.306 of HIPAA, the Security Standard, covered entities must:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- • Ensure compliance with these requirements by the workforce of the covered entity.

Section§ 164.308 of HIPAA addresses Administrative Safeguards relating to security management. A covered entity must implement policies and procedures to prevent, detect, contain, and correct security violations. HIPAA imposes four requirements on covered entities to ensure that they manage the security of electronic PHI: risk analysis, risk management, sanction policy and information system activity review. Both the Medicare Merit Incentive Payment System and the Medicaid Meaningful Use program require a risk analysis before a practice can attest and receive credit for the Promoting Interoperability measures.

The HIPAA Risk Assessment is based on the requirements of information security, which protect information systems against unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Risk is defined by the National Institute of Standards and Technology as the extent to which a physician's practice is threatened by potential events or by individuals trying to break into your computer system. Risk is estimated by weighing the negative impacts that would follow for your practice if the event occurs and the likelihood that the negative event will occur.

There are two related ideas in estimating risk: vulnerability and threat.

- Vulnerability refers to internal weaknesses in protecting ePHI. This means any flaw or weakness in your computer system's security that can be deliberately exploited could result in a security breach or a violation of your security policies.
- Threat refers to external events such as natural disasters or bad actors who could exploit a specific vulnerability in your computer system or destroy it completely.

Risk represents is the likelihood that a computer system will be vulnerable to both internal or external threats that could result in potential negative impacts on your practice.

The HIPAA Security Rule requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address those risks and vulnerabilities. The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to conduct "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity." Both risk analysis and risk management are standard information security processes and are critical to a covered entity's Security Rule compliance efforts.

The Centers for Medicare and Medicaid Services (CMS) recommend a set of steps to follow after a Risk Assessment. Because risk analysis and risk management are ongoing, they constitute dynamic processes that should be periodically reviewed and updated in response to changes in your environment. CMS recommends that provider practices:

- Develop and implement a risk management plan – the security risk assessment is the start of this plan.
- Implement security measures.
- Continuously evaluate and maintain security measures.

Conducting a risk analysis identifies the vulnerabilities – and securities - in your practice that can be used as input to your risk management process. Following the model proposed by CMS will help your practice reduce risks and vulnerabilities to reasonable and appropriate levels.

Security Risk Assessment

The security risk assessment identifies the extent to which your practice complies with the HIPAA requirements for security documentation. A high level of risk in any section indicates that your practice is missing a number of the documents required to manage the security of

your patient records. These sections are shown below in Table 1. The level of risk is calculated from the number of questions you answered positively or negatively.

Table 1. Level of Risk in Different HIPAA Sections for Florida Urgent Care

Section	**Risk**
Administrative Safeguards	High
Organizational Requirements	High
Physical Safeguards	High
Technical Safeguards	High
Documentation Requirements	High

In the following pages of this report you will find a list of the policy and procedure documentation you already have in your practice and those documents you need to create for each HIPAA section. These HIPAA sections are:

- Administrative Safeguards
    - The Administration Safeguards section covers issues that address topics such as risk management and policies and procedures. It covers topics on employee access, training, security management, sanctions and similar subjects. Within each topic the risk assessment asks questions that relate to your documentation of the policies and procedures required by HIPAA.
- Organizational Requirements
    - The Organizational Requirements section deals with relationships between your practice and vendors who are business associates. Each topic within this section addresses a specific requirement of HIPAA.
- Physical Safeguards
    - Physical Safeguards section deals with the security controls on your workstations and in your office. Topics include your facility security plan, access controls, workstation security, equipment disposal and similar topics as required by HIPAA.
- Technical Safeguards
    - The Technical Safeguards section covers the ways your practice manages the security of your technical infrastructure. Topics in this section include controls on access, authentication, emergency planning, encryption of data, transmission security and other similar topics.
- Documentation Requirements

- The Policies and Procedures Documentation section covers the HIPAA requirements for creating, maintaining and updating documentation in your practice.

Administrative Safeguards - High Risk

You have answered a number of questions in the Administrative Safeguards section positively as you worked through this security risk assessment. These indicate that you have a number of the documents required by HIPAA. It would be good to collect those documents in one location.

- In the past year you have conducted a risk assessment to discover risks or vulnerabilities that could negatively impact the protected health information you maintain or transmit.
- Your practice regularly conducts a risk assessment to uncover any risks or vulnerabilities to patient records that might arise with new technology, new services or when moving office locations.
- Your practice has developed security measures to reduce the vulnerabilities to patient records in your possession.
- Your practice has written procedures that specify the steps you will take to punish employees who do not obey your security requirements.
- Your practice has written procedures that outline the steps you will take to review the security of your computer network.
- Your practice has assigned an individual to be the security officer with responsibility for computer security.
- Your security officer takes the lead in developing security policies for your practice.

Security management process

The Security Management standard requires that you maintain written policies accompanied by specific procedures to deal with security violations at four different stages. They require that you train your employees to prevent security violations; that you enable procedures to detect a violation once it occurs; that you identify the steps you will take to contain a security violation after it occurs; and how you will correct that conditions that led to the security violation.

Your answers in the Security management process section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to write policies that deal with how to prevent security violations from happening and how to detect and contain them when they do occur. You will also need clear policies for correcting any security violations that do occur and limiting their damage.

- HIPAA requires your practice to write a set of procedures that specify the steps you should take to prevent security violations from happening and how to detect and contain them when they do occur. You will also need procedures for correcting any security violations that do occur and limiting their damage.

Risk analysis

The Risk Analysis standard requires you to conduct a thorough assessment of two significant factors – vulnerabilities in your practice that could lead to a security violation and risks outside of your practice that could threaten the security of electronic Protected Health Information that you collect and maintain.
Because you are completing this risk analysis your immediate risk is low. You should maintain a copy of this risk analysis, and any prior risk analysis that you have completed, as a clear demonstration of your compliance.

Your answers in the Risk analysis section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to keep all of the documentation from your risk assessment securely stored but available to all employees.

Risk management

This risk management standard requires your practice to lay out a set of policies that address a plan to reduce security vulnerabilities in your practice that could lead to a security breach and risks outside of your practice that could threaten the security of ePHI that you collect and maintain. Your practice should also have a written set of procedures that detail the measures will take to reduce both vulnerabilities and risk.

Your answers in the Risk management section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to write a policy that states the security measures you will take to reduce risks to patient records that you maintain or transmit. Risk is generally considered as threats to the security of patient records that you maintain. This policy would address the level of risk your practice will accept.

Sanction policy

The sanction standard requires that you have clear, written policies to discipline employees who do not comply with your security policies and procedures.

Your answers in the Sanction policy section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to write a policy that describes how you will punish employees who violate the security requirements of your practice. All of your employees should comply with the security conditions that you set or they should be penalized in some fashion. This policy addresses that response.

Information system activity review

Reviewing your computer network's activity is a requirement in the information system activity review standard. This means that you must establish specific procedures to review activity in your network. This would include regularly reviewing audit logs, logs of who has accessed the network and any other tracking reports.

Your answers in the Information system activity review section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to establish a regular schedule to review risks to your practice as shown in security incident reports and audit logs for your computers and network.

Assigned security responsibility

The standard for assigned security responsibility requires that you name an employee who is your security officer and is responsible for developing and implementing the security policies in your practice. This person is generally a manager or a doctor.

Your answers in the Assigned security responsibility section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to maintain documentation that identifies the name and contact information of your security officer.
- HIPAA requires your security officer to take the lead in implementing security procedures for your practice.
- HIPAA requires you to make the name and contact information of the security officer available all of your employees.

Workforce security

The standard for workforce security requires that you implement policies that establish the rules for appropriate access to electronic Protected Health Information and specify the procedures your practice will follow to allow only those employees with appropriate rights to access the electronic Protected Health Information you maintain.

Your answers in the Workforce security section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to write a policy for granting employees the rights appropriate for their roles to access patient records and to prevent someone who is not authorized from opening patient records.
- HIPAA requires your practice to write procedures for giving employees rights that are appropriate for their roles to access patient records and for preventing someone who is not authorized from opening a patient record.

Authorization and/or supervision

The standard for the authorization and supervision of your employees who have access rights to electronic Protected Health Information requires your practice to develop procedures for authorizing employee access and managing those employees who are given access to electronic Protected Health Information.

Your answers in the Authorization and/or supervision section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to write procedures about how you determine whether an employee can gain access to patient records.
- HIPAA requires your practice to write procedures to establish which managers have the authority to authorize an employee to access patient records.

Workforce clearance procedure

The workforce clearance standard requires that your practice establish procedures to ensure that access to electronic Protected Health Information is appropriate for all employees.

Your answers in the Workforce clearance procedure section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to write procedures that cover the clearance processes you use to screen an employee before granting access to patient records.

Termination procedures

The Termination procedures standard requires your practice to have a set of written policies and procedures in place for terminating access to electronic Protected Health Information when an employee no longer works for the practice, or if an employee's access rights are not appropriate.

Your answers in the Termination procedures section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to write procedures to terminate access privileges to patient records when an employee leaves employment.

- HIPAA requires your practice to have a written policy and procedure manual that complies with the Security Rule, either on paper or in electronic format.

Written Documentation

The action, activity and assessment standard requires your practice to keep written records of every action, activity or assessment required by the Security Rule.

Your answers in the Written Documentation section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to document all actions and assessments required by the HIPAA Security Rule, either on paper or in electronic format.

Document Retention

The time limit standard requires your practice to keep all documentation for six years from the date of its creation.

Your answers in the Document Retention section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to retain all of the documentation required by the HIPAA Security Rule for six (6) years from the date of its creation.

Availability

The availability standard requires your practice to make all written security documents available to employees responsible for implementing security procedures.

Your answers in the Availability section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to make written security policies and procedures available to employees responsible for documenting your actions and assessments.

Updates

The update standard requires your practice to periodically review all of your security documentation and update it routinely following any operational changes affecting your electronic Protected Health Information.

Your answers in the Updates section indicate that your practice is missing policies or procedures that are required by HIPAA. The following recommendations are intended as a guide for your writing.

- HIPAA requires your practice to periodically review and update the security documentation required by the Security Rule when operational or environmental changes affect the security of patient records.

Mitigation Plan

The next step for your practice is to develop a Mitigation Plan to work on developing the documentation listed above. A good way to start is to collect all of the documents that you do have in one place. Then, create a "to do" list for approaching the documents that you need. A good approach would be to assign responsibility for writing the documentation to the appropriate staff in your office, with specific target dates for completion. Once all of the required documentation is complete, they can become the basis for putting together your Privacy and Security Policy and Procedures Manual.

Example of the Asset Inventory Report

Appendix A

Florida Urgent Care Asset Inventory

Computer

Desktop PC

Name	Make and model	Serial number	CPU & RAM	Storage Size	CD ROM Drive	Date implemented
Jose Cuidado, MD PC	Dell Inspiron	1000001				5/1/2019
Yolanda Asistencia, RN PC	Dell Inspiron	1000002				5/1/2019
Exam Room 1 Laptop	Dell Latitude	1000003				5/1/2019
Exam Room 2 Laptop	Dell Latitude	1000005				5/1/2019

Tablet

Name	Make and model	Serial number	CPU & RAM	Storage Size	CD ROM Drive	Date implemented
Dr Cuidado iPad	iPad	1000004				5/1/2019

EHR

Electronic Health Record (EHR)

Name	Name of software	Version of software	Date installed	Certified Health IT Product List

Example of the Risk Survey Answers

Appendix B

Florida Urgent Care List of Responses in the Security Risk Assessment

Administrative Safeguards

Section	Question	Choice
Security management process	Does your practice have written policies that address how to prevent security violations from happening, how to detect and contain them when they do occur and finally how to correct them?	No
Security management process	Does your practice have written procedures that specify the steps you should take to prevent security violations from happening, how to detect and contain them when they do occur and finally how to correct them?	No
Risk analysis	In the past year, have you conducted a risk assessment to discover risks or vulnerabilities that could negatively impact the protected health information you maintain or transmit?	Yes
Risk analysis	Does your practice conduct a risk assessment to uncover any risks or vulnerabilities to patient records that might arise with new technology, new services or from moving office locations?	Yes
Risk analysis	Are your risk assessment documents stored together and available to all employees?	No
Risk management	Has your practice established the security measures you will take to reduce risks to patient records that you maintain or transmit?	No
Risk management	Have you developed security measures to reduce the vulnerabilities to patient records in your possession?	Yes
Sanction policy	Does your practice have a written policy that describes how you will punish employees who violate the security requirements of your practice?	No

Sanction policy	Does your practice have written procedures that lay out the steps you will take to punish employees who do not obey your security requirements?	Yes
Information system activity review	Does your practice have written procedures that establish a regular schedule to review risks to your practice as shown in security incident reports and audit logs for your computer network?	No
Information system activity review	Does your practice have written procedures that outline the steps you will take to review the security of your computer network?	Yes
Assigned security responsibility	Has your practice assigned an individual to be the security officer with responsibility for computer security?	Yes
Assigned security responsibility	Does your practice have documentation that identifies the name and contact information of the person who is your security officer?	No
Assigned security responsibility	Does your security officer take the lead in developing security policies for your practice?	Yes
Assigned security responsibility	Is your security officer responsible for implementing security procedures in your practice?	No
Assigned security responsibility	Do all employees know the name and contact information of the security officer for your practice?	No
Workforce security	Does your practice have a written policy for granting employees the rights appropriate for their roles to access patient records and to prevent someone with no authorization from opening a patient record?	No
Workforce security	Does your practice have written procedures for giving employees the rights that are appropriate for their roles to access patient and for preventing someone with no authorization from opening a patient record?	No
Authorization and/or supervision	Does your practice have written procedures for determining the appropriate level of access to patient records for an employee?	No
Authorization and/or supervision	Does your practice have written procedures to establish which managers have the authority to authorize an employee to access patient records?	No

Encryption	Does your practice use software to encrypt patient records when necessary?	No

Documentation Requirements

Section	Question	Choice
Documentation	Does your practice have a written policy and procedure manual that complies with the Security Rule?	No
Written Documentation	Does your practice document all actions and assessment required by the HIPAA Security Rule?	No
Document Retention	Does your practice retain the documentation required by the HIPAA Security Rule for at least six (6) years from the date of its creation?	No
Availability	Does your practice make its written security policies and procedures available to employees responsible for documenting your actions and assessments?	No
Updates	Does your practice periodically review and update its security documentation when operational or environmental changes affect the security of patient records?	No