Whitepaper on

HIPAA Security Rule Compliance

September 2021

securex

CYBERSECURITY +
HIPAA COMPLIANCE

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

IMPORTANT COVID-19 UPDATE:

Due to the constantly changing environment during the COVID-19 Pandemic, details of services herein may be subject to modification, particularly those about onsite inspections and meetings, to address any regulatory & additional changes. HIPAA (45 CFR 164:308 & 314) requires an organization to periodically renew or update their HIPAA Security Risk Analysis, staff training, and other documentation annually/as needed for significant changes in your environment (such as those that may have occurred during the pandemic). For questions regarding how COVID-19 affects your business and its HIPAA Compliance, please feel free to reach out to us.

Confidentiality Notice and Disclaimer (The following Confidentiality Notice and Disclaimer is intended for the IT Support Vendor or Third-Party Service Provider of the recipient and any other recipients.)

Confidentiality Notice and Disclaimer: This document contains information that is proprietary to Securex LLC and is copyright and confidential. The information in this document is strictly for the use of the intended and rightful recipient, for the sole purpose of providing information to consumers about HIPAA compliance and other requirements. It is a violation of the laws of copyright and common law for any organization to use the information contained in this document in any way that conflicts with the rights, as well as the intended purpose of Securex LLC, in permitting the sharing of this information (e.g., it is forbidden to engage in the further sale of the information to one's clients). Use of the information in this document that is in violation of the rights of Securex LLC can result in legal action & prosecution under the applicable laws (e.g., plagiarism, copyright infringement, preventing/tortious business, etc., that can also violate laws that are enforced by religious courts and legal systems in the United States and is considered immoral and unethical). Should you wish to legally use our templates to service your client's, you can feel free to contact Securex LLC to participate in our partnership program so that you can benefit more without having to resort to plagiarism or other illegal operations. The use of the information in this document does not guarantee compliance, in whole or in part, with the GLBA Safeguards Rule or any other regulations and legal requirements. Securex LLC disclaims any-and-all potential liability on its part arising pursuant to the information and material provided in this document and pursuant to any use, misuse, or inability to use the contents of this document. Securex LLC does not guarantee, in whole or in part, compliance with any regulations or requirements that apply to the recipient, any-and-all clients, or any other legal entity. Securex LLC does not guarantee to discover any and all risks to any entity's security or compliance with applicable regulations and legal requirements or to mitigate any and all risks to any entity's security and compliance with applicable regulations and legal requirements. Securex LLC is not a law firm nor lawyers nor attorneys and is not providing attorney services or legal advice in any of the information or services that it provides. Further use of this document constitutes acceptance of this Confidentiality Notice and Disclaimer.

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

Table of Contents

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

A Word from our Chief Cybersecurity Compliance Consultant

I seek to make others' lives better. Life is filled with puzzles that I work to solve, and that detective work is my go-to approach to removing your pain. Ultimately, I want to help others rise up and be self-sufficient.

As the Chief Cybersecurity Compliance Consultant at Securex, I help remove pain relating to the compliance of HIPAA, GLBA, IRS Security Requirements, New York Shield, and NYDFS regulations from companies of all sizes. My inclination is to service my clients in 3 ways: Firstly, being that the industry and laws are really vague, I choose to meet and exceed the needs to help minimize your risk and avoid unnecessary and easily preventable pain. Secondly, I provide a solution that can be tailored to each scenario and threat by providing multiple tiers of service to accommodate everyone's needs. Lastly, everything I do is to help remove pain and worry, and as stressful as cybersecurity and compliance are, I will take good care of you.

Here for you,

Ariel Sandell | CISRCP | Cybersecurity Compliance Consultant

Certified Information Systems Risk and Compliance Professional

Certified Microsoft Technology Associate: Security Fundamentals

Servicing Compliance Needs for CPAs, Tax Preparers, Insurance Brokers, and More |

IRS Compliance, GLBA, NYSHIELD, NYDFS, HIPAA, and More

455 Oak Glen Road / Howell, New Jersey 07731

securex
CYBERSECURITY + COMPLIANCE

The Security Experts™

https://www.securexcyber.com/

Introduction - HIPAA

Companies that deal with electronic protected health information (ePHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance. HIPAA is audited and investigated by the United States Office of Civil Rights (OCR). However, most business leaders think HIPAA has only to do with privacy, confidentiality, and forms alone, primarily the focus of attorneys. At Securex, our focus and specialty are with the lesser-known but critically important **HIPAA Security Rule**. The first requirement of the HIPAA Security Rule is to conduct a thorough and accurate **HIPAA Risk Analysis.** The responsibility to perform a HIPAA Risk Assessment falls on the entity themselves. However, due to the complex process involved, the Government allows a business to enlist the services of a third party to ensure that the assessment meets the required standards.

At **Securex**, we have been trained and certified in HIPAA, Healthcare Cybersecurity, HIPAA Risk Assessment, and HIPAA Disaster Recovery. We have also had the privilege of receiving training and guidance from leaders in HIPAA Compliance & Security, who have shared with us their own knowledge, experience, and software tools, gained from years of helping others pass OCR audits & investigations with 100% success.

This document is meant to provide a general breakdown of the services offered by Securex for HIPAA security and compliance.

NOTE: *This whitepaper is for informational purposes only and is not a legal agreement, legal advice, or engagement letter. (Read further: "What does a Risk Assessment Require").*

It is also important to note that ePHI means electronic health information that ties to an individual and relates to healthcare covered by insurance or related to insurance coverage. For example, if a healthcare provider that accepted insurance (not cash/credit card only) created health information, that information is governed by HIPAA. If that information was then given to a third-party vendor (e.g., an insurance company, medical biller, their subcontractor, etc.) ALL of that information by ALL those organizations are covered by HIPAA.

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

What's Included in the Securex HIPAA Compliance Package?

1. HIPAA Risk Assessment

In a Risk Assessment handled by Securex, our assessments, questionnaires, investigations, and meetings do not just seek to fulfill the minimal HIPAA Security Rule requirements. Our Risk Assessment can also provide many security best practices & recommendations for issues that exceed HIPAA in both compliance and protecting the business.

HIPAA requires that organizations conduct an accurate and thorough yearly assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of *electronic protected health information* (ePHI). There are numerous requirements for HIPAA Risk Assessment. Securex performs this assessment so you can fully comply with HIPAA requirements. Securex will provide supporting documentation and a final report of the results.

What does HIPAA Risk Assessment Require?

Well, first, let's tell you what ***doesn't*** qualify as HIPAA Risk Analysis:

- *A HIPAA/Security Gap Assessment*
- *An IT security scan & workforce training*
- *Penetration Testing*
- *A HIPAA/Security questionnaire or checklist*
- *A Risk Assessment for insurance, PCI, GLBA, or any other non-HIPAA requirements.*

The OCR (the Government's Office of Civil Rights), which audits & enforces HIPAA, outlined several points, each with its numerous requirements (see "Additional Resources" at the end of this document). Every HIPAA Risk Assessment must cover these points, ***as a minimum:***

1. Scope analysis *(what is being assessed)*
2. Data collection *(gathering the information being evaluated)*
3. Vulnerabilities/threat identification *(to the security of health information)*
4. Assessment of current security measures *(administrative, physical and technical)*

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

5. Likelihood of threat occurrence *(using specific probability metrics)*
6. The potential impact of threat *(using specific impact metrics)*
7. Risk level *(using specific risk metrics)*
8. Periodic review/update as needed *(to continually monitor risk).*
9. Documentation (of the Risk Analysis)
10. Distribution (to the necessary workforce members)

Securex provides a HIPAA Risk Assessment designed to meet and exceed the OCR's standards used in a HIPAA audit.

Risk Assessment Process

The HIPAA Risk Assessment can be broken down into 4 phases.

Particular order, specifics, and time allotment for various phases may vary per organization.

The different phases of the Risk Assessment process are as follows:

1. **Gathering Organization Information**
    - Planning the *assessment (order of assessment phases, methods, and questionnaires used in the engagement)*
    - Onsite investigation (if needed) *of all local facilities.*
        i. ***NOTE: PRESENTLY, DUE TO THE COVID-19 PANDEMIC, THIS IS NOT REQUIRED NOR PROVIDED UNLESS OTHERWISE SPECIFIED.***
    - Interviews/Questions for critical *employees (Chief Information Officer, Chief of IT Department, questionnaires, etc.)*
        i. A questionnaire is sent to you and your IT. The questionnaires for you/your IT are either sent as one form or as a few smaller forms. The questionnaires may take one to several hours for you/your IT to fill out (depending on the complexity of your organization and how much information you have about your security and procedures. You/your IT try to answer what you can, and whatever questions you need help with, we are here for you via phone interviews, email, a phone call, etc.!) We may provide checkboxes where you can indicate that a specific safeguard is not implemented or if the answer is unknown. As part of our services, Securex provides an allotted amount of time to help you via phone and email to get the answers to the remaining questions. Some of the questions cover whether your third-party vendors have provided the required HIPAA agreements. You may need to reach out to your vendors to get this information. As needed, in some circumstances, Securex can

try to obtain this information from them as well. Securex may require proof that certain safeguards are in place (e.g., backups, antivirus, etc.) to be provided by your IT support via screenshots, reports, etc.).

- Assessment of documentation, policies & procedures currently in effect *(and additional relevant documentation)*

NOTE: ***Risk assessments are time-sensitive, so it's important that an organization promptly get back to us with the required questionnaires and information.***

2. Gathering and Verifying IT Information

- Taking a complete inventory of and documenting ALL the organization's systems.

  Inventory includes:

  i. Computers, etc., working with electronic health information or have a bearing on the security of ePHI.
  ii. Medical devices which store or access electronic health information*)*
  iii. Computer and system investigation on specific computers *(inspecting individual computers, servers, and cloud-based apps)*
  iv. Accounting of Computer Systems and Personnel *(all computers and medical devices, users, and employees with potential access to health information).*
  v. Follow up with necessary critical employees for any questions about results before or after creating reports.

NOTE: *Securex uses a non-invasive approach, and we don't scan/access your actual computers or collect your client's information. You would need IT to support (whether in-house or outsourced) to obtain the necessary details on all the devices and provide them to us. If you need to find a third party who can assist with this, let us know, and we can see how we can help you or refer you to an IT specialist who can assist with this. Suppose Securex needs assistance to access certain information from outside services (such as an outsourced IT). In that case, this assistance must be provided to us by the external services, in a HIPAA compliant manner, such as signing a HIPAA Business Associate Agreement with the (client) organization, as needed.*

NOTE: ***Risk assessments are time-sensitive, so it's vital that an organization promptly get back to us with the required questionnaires and information.***

3. **Analyzing the Information**

   - Analyzing the information obtained from the investigation (discerning vulnerabilities and risks).
   - Assessment of current security measures (administrative, physical and technical)
   - Vulnerabilities/threat identification (to the security of health information)
   - Assessment of current security measures (administrative, physical and technical)
   - Likelihood of threat occurrence (using specific probability metrics)
   - The potential impact of threat (using specific impact metrics)
   - Risk level (using specific risk metrics)

4. **Consolidating the information and creating the reports.**

2. HIPAA Risk Management

Next, HIPAA requires management of the risks uncovered in the Risk Assessment to comply with HIPAA. There are numerous HIPAA requirements in this process. The key ingredients of this process are an outline of the risks & gaps discovered, recommendations on how to address them, followed by a detailed plan of action. Securex guides an organization through the process, coordinating with the company's leadership and IT to present recommendations on mitigating the risks so they can meet and exceed HIPAA requirements. Securex generates reports/lists to help ensure your organization and your IT support understand everything.

NOTE: Some of the IT recommendations provided in the Risk Assessment are vendor-neutral; some mention a few options for specific procedures and software.

3. HIPAA Policies and Procedures

HIPAA requires detailed written policies and procedures for your security and compliance. There are numerous requirements for these policies and procedures under HIPAA. Securex provides your firm with clear policies and procedures to address the HIPAA requirements for Security, Privacy, and Breach Reporting. Some policies and procedures may need to have information entered by you later (e.g., the name of a specific antimalware software being used, if no particular solution has been decided on). Other policies and procedures may need to be further developed

later to meet your specific needs (e.g., emergency operations). Securex provides the necessary policies and procedures to be implemented, their source in HIPAA, and shows where you may need to input additional information if it cannot be entered right away. As you need, Securex can always help you modify and edit the policies and procedures later as a separate service.

4. HIPAA Documentation

The most important part of compliance is to prove to others (e.g., the Government) that you are compliant when needed! The HIPAA Privacy, Security, and Breach Reporting Rules require that you document the following of your policies and procedures (e.g., screenshots of some encrypted computers, schedules, and certifications for staff training, etc.) HIPAA outlines the various documentation requirements. Securex can provide you with written guidance on the documentation requirements for the HIPAA Security Rule and how you should proceed to document your compliance. We can provide information, forms, and Government guidance that you can use to help with that. Generally, HIPAA investigations/audits are conducted via 'desk audits' where the Government first requests basic information and documentation. We strive to help you have what you need to pass a Desk Audit successfully. If a HIPAA Desk Audit is passed to the satisfaction of the OCR, they do not require a more in-depth onsite audit. As needed, Securex can guide you in documentation requirements regarding the onsite audits as well. It should be noted that even if an organization doesn't entirely pass an audit, the fact that they made a serious effort can make the difference between a request for corrective action vs. a serious onsite audit or fine!

NOTE: HIPAA documentation regarding the Privacy and Breach reporting rules may require keeping extensive records of patient forms, breach information, etc. Such information is usually already retained by many medical practices. Such information may be requested in the event of an audit on the HIPAA Privacy and Breach Reporting Compliance. Securex only provides the general information on Privacy and Breach Reporting matters covered in the policies and procedures from a security standpoint. Securex can provide Government information regarding these documentation requirements. The most common and severe HIPAA audits/investigations (resulting in thousands to millions of dollars in fines) are regarding the lesser-known HIPAA Security Rule. As Securex's primary focus is on the HIPAA Security Rule, you are encouraged to consult with a HIPAA lawyer regarding the more legal, privacy, client notification, and 'patient rights to access information' parts of HIPAA.

The HIPAA security rule also requires an end of the year/periodical assessment of compliance. Securex can provide you a template to use when you are ready to assess your compliance at a later time.

5. HIPAA Business Associate Agreement

Third-party vendors may also be storing the company's healthcare information. If so, they too must be HIPAA compliant and secure. HIPAA requires vendors to provide specific documentation

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

for an organization to be allowed to use their services. This agreement is called a HIPAA Business Associate/Subcontractor Agreement (BAA). Securex can provide you with a template that you can provide your vendors and use for those to whom you provide services.

6. HIPAA Certificate

The Government doesn't recognize a third party attesting to one's HIPAA compliance. HIPAA compliance is the sole responsibility and burned of each individual organization. However, we can provide a certificate that you can show your clients and associates that we have provided you with a security assessment, policies, and procedures to comply with HIPAA, as well as a seal that you can use to display on your website etc.

How Long Does the Process Take?

The length of time from the beginning of the process to the end can vary due to the size & scope of an organization. The length of time can range from 30 hours (or more) for a small/medium organization to 50+ hours for a large organization, hospital, or healthcare system.

To help you, we estimate the number of hours for the project, and apply our hourly rate (approximately $250 per hour) and provide a set price. Every client's situation is unique. We let you know if unforeseen circumstances arise that would significantly increase the number of hours and the cost before proceeding and reengage. Once the main HIPAA Compliance Package is delivered, you may want additional 'tailormade security & compliance consultations. The length of these consultations can vary significantly based on the client. To help reduce the cost, we apply the above scoping & pricing method or use an hourly billing system. We let you know ahead of time how we can help you.

Additional factors that may impact the length of the project may include contributors such as the number of facilities requiring an assessment, internal & external IP networks, Active Directory (which makes the process faster), traveling & onsite investigation (if necessary), and more.

We provide a free security consultation to assess your HIPAA needs.

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

Additional Services not Included in the HIPAA Compliance Package

7. HIPAA Training:

HIPAA requires periodic (yearly) training of employees who **work with health information** in the relevant areas of HIPAA, including those that govern cybersecurity. Securex provides the cybersecurity training appropriate to HIPAA and helps document the training, as required by HIPAA. Training covers HIPAA and relevant cybersecurity and best practices used to maintain HIPAA compliance.

Training is provided online, for "at your own pace" training, with exams and certification seals for each employee (or the Chief Compliance Officer) and can be provided as needed. Our online training is accredited for Continued Education for doctors and nurses. (Eligibility varies per state and specific healthcare occupation). Training is priced per employee being trained. Securex offers promo codes for 20% discounts per employee and discounts for bulk training of 100+ employees. Training starts at $59.00 per employee for unlimited training for the year. For our training catalog, click here.

8. HIPAA Evaluation

The HIPAA security rule also requires an end of the year/periodical assessment of compliance. Securex can assist you in performing this evaluation.

9. HIPAA Consultations

Tailormade Software Solutions

Securex provides general recommendations for types of software in its reports, policies, and procedures. You can also consult on whether specific technology's security is HIPAA compliant. If you'd like, we can also collaborate with other legal experts you use to answer specific organization, technology, and vendor-related questions regarding HIPAA.

Third-Party Vendor HIPAA Compliance Assessments

Third-party vendors may also be storing the company's healthcare information. If so, they too must be HIPAA compliant and secure. HIPAA requires vendors to provide specific documentation for an organization to be allowed to use their services. Securex helps assess all third-party vendors and includes information about their security and compliance to ensure all collaborating organizations are compliant and safe.

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com

Updating Documentation

HIPAA compliance is an ongoing process. Its documentation, such as the Risk Management, policies and procedures, and other documentation, needs to be reviewed and updated periodically as you implement the security and compliance, fixes, undergo changes that impact your security, etc. Securex can help you keep your documents up to date.

Third-party vendors may also be storing the company's healthcare information. If so, they too must be HIPAA compliant and secure. HIPAA requires vendors to provide specific documentation for an organization to be allowed to use their services. Securex helps assess all third-party vendors and provides information about their security and compliance to ensure all collaborating organizations are compliant and safe.

Additional Resources

For additional information on the required HIPAA Risk Assessment standards used by the OCR and others, as well as additional resources about HIPAA, feel free to check out the following link or reach out to us (the following does not provide an exhaustive list of OCR & Government recommendations & requirements for a Risk Assessment):

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

https://www.hhs.gov/hipaa/for-professionals/security/index.html

455 Oak Glen Road
Howell, New Jersey 07731

Phone / 732.285.4702
info@securexcyber.com
securexcyber.com