**HIPAA SECURITY REGULATIONS**

**POLICY AND COMPLIANCE DOCUMENTS**

**For**

**(Lab name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**(Street Address) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**(City, State, ZIP) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Adopted \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **(Date)**

Introduction / Explanation

**The Vision Council Optical Lab Division Development Manual**

For Compliance with HIPAA Security Regulations

I. Disclaimer – *This Development Manual does not constitute, and is not a substitute for, legal advice.* *This Development Manual has been prepared by The Vision Council Optical Lab Division to guide and assist labs in understanding and complying with the HIPAA Security Regulations. This is a Development Manual only, and not a completed HIPAA Security Policy. The lab which uses this Development Manual must tailor the outline to the specifics of the lab’s operations. By marking appropriate sections, and inserting appropriate explanations, the lab will complete their own HIPAA Security Policy.*

II. **WHO** – Do The HIPAA Security Regulations Apply To Your Lab?

A. The HIPAA Security Regulations apply to the same “Covered Entities” which are subject to the HIPAA Privacy Regulations (i.e., “Covered Entities” are only those optical labs which make electronic payment claims to a vision plan or Medicare or Medicaid; and Business Associates of Covered Entities). As an optical lab, you are likely a Covered Entity subject to the HIPAA Security Regulations.

B. **If your lab does not make electronic payments claims to vision plans or Medicare or Medicaid, you are NOT a Covered Entity. However, you may be a Business Associate of another Covered Entity if you perform a Business Associate function or activity involving the use or disclosure of Protected Health Information on behalf of a Covered Entity. Business Associate functions do not include the receipt of RXs and fabrication of eyeglasses, but are instead ancillary services (consulting, claims processing, etc.) that involve access to PHI. Business Associates are subject to the HIPAA Security Regulations. If you are not a Covered Entity or a Business Associate of a Covered Entity, you are NOT subject to the HIPAA Security Regulations, and you DO NOT need to read any further, and you DO NOT need to complete this manual.**

III. **WHEN** – For a lab that is covered by the HIPAA Security Regulations, the original compliance date was April 20, 2005. As HHS releases updates to HIPAA Regulations, covered labs are required to comply within a reasonable amount time. Are you covered? See “II. **WHO**” above.

IV. **WHAT** – HIPAA Security Regulations – Here are the basic facts.

A. These Regulations detail the Administrative, Physical, and Technical safeguards which an optical lab will be required to implement in order to safeguard electronic protected health information (or ePHI).

B. “Electronic Protected Health Information” or “ePHI” includes individually identifiable health information that is transmitted by or maintained in electronic media (excluding employment records held by the lab in its role as an employer). Rx information which has a name, address, social security number, or other information from which one might identify the patient, is ePHI if it is in electronic form.

C. The HIPAA Security Regulations impose three sets of requirements: Administrative Safeguards (at Section 164.308); Physical Safeguards (at Section 164.310); and Technical Safeguards (at Section 164.312).

1. Under each of these three categories there are “Standards” (Std), and then under most Standards there are “Implementation Specifications” (ImpSpec).

 2. An Implementation Specification is either described as:

 a.) “REQUIRED” – in which event it MUST be complied with; or

 b.) “ADDRESSABLE”– in which event a covered lab has three options:

 (i) Comply with the Addressable Implementation Specification.

(ii) Document in writing why it is not reasonable and appropriate for the lab to comply with the Implementation Specification , and implement one or more alternative security measures to accomplish the same purpose; or

(iii) Document in writing why it is not reasonable and appropriate for the lab to comply with the Implementation Specification or implement an alternative equivalent measure, and take no other action with respect to that Addressable Implementation Specification.

A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

V. **THIS IS IT** – Purpose and Organization of This Development Manual

A. This Manual guides The Vision Council Optical Lab Division Member lab through the HIPAA Security Regulation’s Standards and Implementation Specifications. By reading and completing the checkboxes ([ ]) in the Manual, The Vision Council Optical Lab Division Member lab will document compliance with HIPAA Security Regulations. Where there are three boxes – the Addressable items – you only choose one alternative - **check 1 only**. There are 46 checkboxes completed when you are done.

B. This Manual is intended to **both explain** the HIPAA Security Regulations **and, when completed** by the lab, **to constitute documentation of the lab’s compliance** with such regulations.

C. This Manual sets forth **IN BLUE COLOR** the **actual text** of the HIPAA Security regulations (noted as “**HIPAA sez:**”) for the Administrative, Physical, and Technical Standards and Implementation Specifications at Section 164.308, 310, and 312. (The entire text of these regulations can be found at the back of the Manual.)

D. This Manual sets forth **IN GREEN COLOR an explanation** from The Vision Council Optical Lab Division(noted as “**The Vision Council sez**:”) as to what the Standard or Implementation Specification requires of the lab.

E. This Manual sets forth **IN BLACK COLOR a checkbox ([ ]) that the lab can use to confirm compliance with the Standard or Implementation Specification, and a space for the lab to insert any needed explanation about how it complies**.

1. In the case of a REQUIRED Standard or Implementation Specification, there is only one checkbox for the lab to check (i.e., “Yes, our lab complies.”)  **And the lab then explains, in writing, how.**  *Note: Don’t write a book! State the basic, simple facts. The “****The Vision Council sez****” text includes ideas.*

2. In the case of ADDRESSABLE Implementation Specifications, as explained above (IV-C-2-b), the lab has three checkbox options **(check 1 only)**:

(i) a checkbox saying, “Yes, our lab complies with the Implementation Specification” and explaining, in writing, how, or

(ii) a checkbox documenting why it is not reasonable and appropriate for the lab to comply with the Implementation Specification, and identifying an equivalent alternative measure adopted by the lab, or

(iii) a checkbox documenting why it is not reasonable or appropriate for the lab to comply with the Implementation Specification or adopt an alternative equivalent measure.

A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based. *Note: Don’t write a book! State the basic, simple facts. The “The Vision Council sez” text includes ideas.*

VI. **WHAT YOU NEED TO DO**

**By checking the appropriate boxes and inserting the explanations IN THE BLACK COLOR, the Lab documents its compliance with the HIPAA Security Regulations.** Be sure to **check 1 box only** for the Addressable items. There are 46 checkboxes completed when you are done. The regulations require this manual to be maintained and updated as long as the law is in effect. The documentation of any changes to the manual should be kept for six years from the date of the change.

***So, print pages 10-41 to use as a worksheet, and get started! You’ll be done soon!***

**Translation Table**

for Terms in the Manual

Covered Entity = labs which make electronic payment claims to a vision plan or Medicare or Medicaid

ePHI = electronic protected health information

Standards = Std = requirement of the HIPAA Security Regulations

Implementation Specifications = ImpSpec = requirement of the HIPAA Security Regulations

Required = standard or implementation specification that must be complied with; The Vision Council Optical Lab Division suggests how

Addressable = implementation specification that offers three choices for compliance; The Vision Council Optical Lab Division suggests alternatives

HIPAA sez: = this is the text from the HIPAA Security Regulations

The Vision Council sez: = this is The Vision Council Optical Lab Division’s explanation of the regulation and how the typical lab would comply

[ ] = the checkbox; items to be completed by The Vision Council Optical Lab Division Member lab to complete the manual and document compliance with the security regulations; you are done when you have 46 checkboxes completed

**List of HIPAA Security Regulation Requirements**

**A. ADMINISTRATIVE SAFEGUARDS - Section 164.308**

1) SECURITY MANAGEMENT PROCESS

 i) Risk analysis (Required - ImpSpec)

 ii) Risk management (Required - ImpSpec)

 iii) Sanction policy (Required - ImpSpec)

 iv) Information system activity review (Required - ImpSpec)

2) ASSIGNED SECURITY RESPONSIBILITY (Required - Std)

3) WORKFORCE SECURITY

 i) Authorization and/or supervision (Addressable - ImpSpec)

 ii) Workforce clearance procedure (Addressable - ImpSpec)

 iii) Termination procedures (Addressable - ImpSpec)

4) INFORMATION ACCESS MANAGEMENT

 i) Access authorization (Addressable - ImpSpec)

 ii) Access establishment and modification (Addressable - ImpSpec)

5) SECURITY AWARENESS AND TRAINING

 i) Security reminders (Addressable - ImpSpec)

 ii) Protection from malicious software (Addressable - ImpSpec)

 iii) Log-in monitoring (Addressable - ImpSpec)

 iv) Password management (Addressable - ImpSpec)

6) SECURITY INCIDENT PROCEDURES

 i) Response and Reporting (Required - ImpSpec)

7) CONTINGENCY PLAN

 i) Data backup plan (Required - ImpSpec)

 ii) Disaster recovery plan (Required - ImpSpec)

 iii) Emergency mode operation plan (Required - ImpSpec)

 iv) Testing and revision procedures (Addressable - ImpSpec)

 v) Applications and data criticality analysis (Addressable - ImpSpec)

8) EVALUATION (Required - Std)

9) BUSINESS ASSOCIATE AGREEMENTS

**B. PHYSICAL SAFEGUARDS - Section 164.310**

1) FACILITY ACCESS CONTROLS

 i) Contingency operations (Addressable - ImpSpec)

 ii) Facility security plan (Addressable - ImpSpec)

 iii) Access control and validation procedures (Addressable - ImpSpec)

 iv) Maintenance records (Addressable - ImpSpec)

2) WORKSTATION USE (Required - Std)

3) WORKSTATION SECURITY (Required - Std)

4) DEVICE AND MEDIA CONTROLS

 i) Disposal (Required - ImpSpec)

 ii) Media re-use (Required - ImpSpec)

 iii) Accountability (Addressable - ImpSpec)

 iv) Data backup and storage (Addressable - ImpSpec)

**C. TECHNICAL SAFEGUARDS - Section 164.312**

1) ACCESS CONTROL

 i) Unique user identification (Required - ImpSpec)

 ii) Emergency access procedure (Required - ImpSpec)

 iii) Automatic logoff (Addressable - ImpSpec)

 iv) Encryption and decryption (Addressable - ImpSpec)

2) AUDIT CONTROLS (Required - Std)

3) INTEGRITY

 i) Mechanism to authenticate electronic PHI (Addressable - ImpSpec)

4) PERSON OR ENTITY AUTHENTICATION (Required - Std)

5) TRANSMISSION SECURITY

 i) Integrity controls (Addressable - ImpSpec)

 ii) Encryption (Addressable - ImpSpec)

**ORGANIZATIONAL REQUIREMENTS - Section 164.314**

1) Business associate contracts or other arrangements.

**POLICIES, PROCEDURES AND DOCUMENTATION REQUIREMENTS - Section 164.316**

1) DOCUMENTATION

 i) Time limit (Required - ImpSpec)

 ii) Availability (Required - ImpSpec)

 iii) Updates (Required - ImpSpec)

**DEFINITIONS - Section 164.304**

**SECURITY STANDARDS: GENERAL RULES - Section 164.306**

**A. ADMINISTRATIVE SAFEGUARDS - Section 164.308**

**1) SECURITY MANAGEMENT PROCESS**

 **HIPAA sez:** Implement policies and procedures to prevent, detect, contain, and correct security violations.

 **i) Risk analysis** **(Required - ImpSpec)**

**HIPAA sez:** 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, or business associate, if applicable.

[ ] Yes. Our management team identified and analyzed the ways that electronic protected health information in our lab can be compromised.

**The Vision Council *sez****: Have your management team review the ways that electronic protected health information (ePHI) in your lab can be accessed by both authorized and unauthorized personnel and the extent to which the integrity of ePHI can be compromised. This would typically include an assessment of the means by which unauthorized internal users can gain access to ePHI and the extent to which unauthorized external users can similarly gain access. It would include an assessment of the storage, retrieval and transmission of information and identify vulnerability or weaknesses in security procedures or safeguards. To further ensure compliance with the Security Rule have your management team review the manner in which ePHI can be remote accessed or stored off-site.*

 **ii) Risk management** **(Required - ImpSpec)**

**HIPAA sez:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R. § 164.306(a).

[ ] Yes. We completed an implementation of the measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

**The Vision Council *sez****: In the process of completing this manual, you will confirm, identify and implement security measures to comply with the requirements. This may include installing firewalls and antivirus software, enabling security settings on hardware and software and encrypting data for storage and transmission. These security measures must be undertaken with regard to systems used (1) only on-site, (2) off-site through portable devices (whether lab owned or employee owned), and (3) systems (including employee owned home computers) used to remotely access ePHI. If ePHI can be accessed through portable media devices (including laptop computers) and/or through remote connections, it is necessary that your lab’s compliance plan address the various risks associated with remotely accessing ePHI. If lab employees use flash drives to access or store ePHI, the lab should require that USB flash drives must include data encryption capabilities and all data stored on flash drives must be encrypted. Additionally, your lab may want to require that all lab employees using a home computer to access EPHI install specific firewall/virus protector software, as well as require that such software be kept up to date.*

*Portable media storage devices include, but are not limited to, laptops, PDAs, Smart Phones, USB Flash Drives, and Memory Cards, floppy disks, CDs, DVDs, email, and Smart cards. Such devices should only be used by lab employees if the device contains appropriate encryption capabilities. Additionally, security measures should address situations involving stolen or lost laptops or other portable media devices, as well as the security risks associated with using home-based personal computers or public workstations (e.g., hotel business centers) to access ePHI information.*

 **iii) Sanction policy** **(Required - ImpSpec)**

**HIPAA sez:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. or business associate, if applicable.

[ ] Yes. Our lab complies with this implementation specification.

**The Vision Council *sez****: Establish personnel policies that address failures to comply with security policies and procedures. This would typically include verbal warnings, written warnings and termination with possible criminal prosecution for violations, depending on the severity of the violation. These policies would typically be explicitly included in the lab’s list of policies. If your lab permits employees to access ePHI off-site through remote access of the lab’s systems, or if ePHI is taken off-site via portable devices, it is necessary that your sanction policy address unauthorized off-site access to ePHI, as well as situations where the security of ePHI is compromised as a result of off-site remote access, the theft of portable devices containing ePHI. Each instance of workforce disciplinary action regarding the security of ePHI should be documented in a written or electronic record by the Lab’s Security Officer.*

 **iv) Information system activity review** **(Required - ImpSpec)**

**HIPAA sez:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

[ ] Yes. Our lab has established a program to periodically review the records of information system activity, including audit logs, access reports, and security incident tracking reports.

**The Vision Council *sez****: Many operating systems (such as Microsoft Windows Server’s Active Directory) have audit features that track user access to files. Confirm that the lab’s audit tools track remote access as well as on-site access to files. The Lab’s Security Officer should review these records periodically. The Security Officer should review the records of system activity when a security incident or known or suspected security breach has occurred. This review should occur even if it is not time for a periodic review. If a security incident of breach has occurred, the Security Officer should then follow the procedures set forth in Lab’s security incident and breach policies.*

**2) ASSIGNED SECURITY RESPONSIBILITY (Required - Std)**

**HIPAA sez:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule for the covered entity, or business associate, if applicable.

[ ] The security official who is responsible for the development and implementation of the policies and procedures required by this subpart for this lab is . *[Insert the name.]*

**3) WORKFORCE SECURITY**

**HIPAA sez:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section (*“Information Access Management”*), and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

 **i) Authorization and/or supervision** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how the lab does this, such as by having a policy which includes procedures for assigning passwords to employees for authorizing access to systems that contain protected health information and by including in job descriptions whether a person in that job requires access to ePHI. If necessary, this policy should also address heightened authentication procedures for employee off-site remote access to ePHI.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **ii) Workforce clearance procedure** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how lab does this such as by having a table of passwords and assigned authorization levels that is reviewed and approved by management prior to any additions or changes being implemented. The policy should include procedures for only granting access of ePHI to those employees who require access. Implement a policy that addresses the potential theft or loss of log-on/password information. For example, the lab may want to consider the use of two-factor authentication (a password, and a security question).*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **iii) Termination procedures (Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (3)(ii) of this section.

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how lab does this, such as by having a policy that, upon termination of employment, or upon change in an employee’s authorization status, an employee’s user access authorization codes, access cards, ID badges, keys, etc. are canceled/recovered or changed to the appropriate new level of access. Permitting employee use of only lab owned portable devices (including removable media storage devices such as USB flash drives) will greatly improve the lab’s ability to ensure that terminated employees do not maintain access to ePHI post-termination. Such a policy will better ensure your lab that data stored on USB flash drives are encrypted, etc. Additionally, and if possible, an employee’s authorization codes and passwords should be “turned off” prior to the lab’s notifying the employee of his/her termination.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**4) INFORMATION ACCESS MANAGEMENT**

**HIPAA sez:** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of this part.

 **i) Access authorization** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

**The Vision Council *sez****: This addresses the need to have individual authorization prior to having access to ePHI information.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how the lab does this, such as by having workstation sign-on (passwords).*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **ii) Access establishment and modification (Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement policies and procedures that, based upon the covered entity's or business associate’s (if applicable) access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

**The Vision Council *sez****: Document a process that periodically reviews a user’s need to access ePHI. If changes to access rights are necessary, the process would also indicate a change in job description for that job.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how the lab does this, such as by implementing periodic review of user needs to access ePHI and has documented the process in (give the reference to the document).The policy should also identify procedures for modifying a person’s access to ePHI upon a change in the person's job function, or if specifically directed by their manager.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**5) SECURITY AWARENESS AND TRAINING**

**HIPAA sez:** Implement a security awareness and training program for all members of its workforce (including management).

 **i) Security reminders** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Periodic security updates.

**The Vision Council *sez****: Security training encompasses awareness of internal lab personnel procedures and processes, as well as awareness of new external threats (malicious software). Training should be provided to all employees that have access to ePHI. Security reminders/notifications and procedures to deal with them should be provided as new threats are identified.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how lab does this, such as by establishing security training programs for all employees with access to ePHI and, additionally, by providing Security Reminders/Notification to employees as threats are identified.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **ii) Protection from malicious software (Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Procedures for guarding against, detecting, and reporting malicious software.

**The Vision Council *sez****: Malicious software includes viruses, bugs, Trojans and spyware. Labs typically should install software patches, firewalls, anti-virus software, anti-spam software and anti-spyware software and get frequent updates of virus definitions.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how the lab does this, such as by installing a firewall and providing anti-virus and anti-spyware software on servers and workstations, obtaining frequent virus definition updates, receiving automated notification of patches for computer Operating Systems and applying the patches as they become available. Labs should train its workforce to identify, report, and protect against malicious software. The Lab should ensure that any system that has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **iii) Log-in monitoring (Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Procedures for monitoring log-in attempts and reporting discrepancies.

**The Vision Council *sez****: Labs should implement software to monitor and document log-in attempts on each system containing ePHI. Labs should the logs on a periodic basis.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how the lab does this, such as by implementing log-in monitoring and reporting.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **iv) Password management** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Procedures for creating, changing, and safeguarding passwords.

**The Vision Council *sez****: Passwords are typically managed by the system administrator. On a periodic basis, all passwords are changed. Only the system administrator has a list of all passwords and that list is kept in an encrypted file. Passwords should be at least 4 characters long and contain characters and numbers. In order to further protect against potential security incidents, the lab should consider using two-factor authentication.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how the lab does this, such as by implementing a password management procedure.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**6) SECURITY INCIDENT PROCEDURES**

 **HIPAA sez**: Implement policies and procedures to address security incidents.

 **i) Response and Reporting** **(Required - ImpSpec)**

**HIPAA sez:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity. or business associate, if applicable; and document security incidents and their outcomes.

[ ] Our lab is in compliance with the Response and Reporting requirement.

**The Vision Council *sez****: Risk assessment should have resulted in a list of potential physical or technological events (hacking, viruses, etc) that could result in a security breach. A written procedure must be in place that reports and handles such security breaches and a response team identified and trained to deal with them. This procedure should address security breaches that occur both on-site and off-site, as well as those involving removable media storage devices.*

**7) CONTINGENCY PLAN**

 **HIPAA sez:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

 **i) Data backup plan** **(Required - ImpSpec)**

**HIPAA sez:** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

[ ] Our back-ups are done every .*[state the frequency]*

**The Vision Council *sez****: In the event of data storage failure or disaster occurring, it is necessary to restore application programs and data. For these reasons, back-ups on a regular and frequent basis are required, and these back-ups should include information stored on removable media storage devices (including laptops), and well as ePHI information being accessed or edited by users remotely accessing such information. Since loss of data may require re-keying new information since the last back-up, it is recommended that back-ups should be done at least twice per day. The lab should then have a daily, weekly, monthly and yearly back-up. Labs should periodically validate that the back-up was successfully done by doing a restore test. Additionally, all backups should be stored in a secure off-site location that can be accessed at any time by authorized personnel. When an off-site or backup service is used, a Business Associate Agreement must be used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.*

 **ii) Disaster recovery plan** **(Required - ImpSpec)**

**HIPAA sez:** Establish (and implement as needed) procedures to restore any loss of data.

[ ] Our lab has a disaster recovery plan that is documented separately. The title of the document is [*provide title*] and is kept at [Describe *location where the document is kept*].

**The Vision Council *sez****: Each laboratory must develop a disaster recovery plan. The disaster recovery plan outlines how a lab would recover lost data due to an emergency or a disaster, such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing ePHI. Restoration would typically require restoring data from the data back-ups.*

 **iii) Emergency mode operation plan** **(Required - ImpSpec)**

**HIPAA sez:** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

[ ] Our lab has an emergency mode operations plan that is documented separately. The title of the document is [*provide title*] and is kept at [Describe *location where the document is kept*].

**The Vision Council *sez****: The Lab should establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode*

 **iv) Testing and revision procedures** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement procedures for periodic testing and revision of contingency plans.

**The Vision Council *sez****: Every data backup plan, disaster recovery plan and emergency operation plan requires periodic testing. This would typically involve a simulated restore to a test computer system of the computer Operating System, Application programs and all data. This should be described in the data backup, disaster recovery and emergency mode operations plans.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how lab does this, such as by periodically testing and revising contingency plans.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **v) Applications and data criticality analysis** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Assess the relative criticality of specific applications and data in support of other contingency plan components.

**The Vision Council *sez****: As part of disaster recovery and emergency operation plans, certain application programs and data restoration will be determined to be more important and therefore need to be brought back on-line before others. For example, an email system may not be as important as the lab computer system and billing systems. The disaster recovery and emergency mode operation plans would therefore identify the sequence and timing to restore these systems.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how lab does this, such as by assessing the criticality of applications and data and including in the disaster recovery and emergency operations plans the sequence, timing and hardware and software needs to re-establish functionality.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**8) EVALUATION (Required - Std)**

**HIPAA sez:** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate’s (if applicable) security policies and procedures meet the requirements of this subpart.

[ ] Our lab has developed a checklist and is performing the evaluation periodically.

**The Vision Council *sez****: Develop a checklist that is used to confirm that each part of the HIPAA Security requirements that are intended to be implemented are, in fact, implemented satisfactorily. The evaluation should be performed periodically.*

**9) BUSINESS ASSOCIATE AGREEMENTS**

**The Vision Council *sez****: See discussion of Business Associate Agreements under Section 164.314 (“Organizational Requirements”) below at page 33.*

**B. PHYSICAL SAFEGUARDS - Section 164.310**

**1) FACILITY ACCESS CONTROLS**

**HIPAA sez:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

 **i) Contingency operations** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

**The Vision Council *sez****: In the event of a disaster, recovery of data and re-establishment of operations is necessary. In some cases, the original lab facility can be used. In other cases, an alternate site must be used. In either case, facility access control is required.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe your process such as (a) only authorized people being issued keys and/or pass codes or (b) admission being granted by an employee who observes any person entering the building; and (c) in the event of a disaster, access to our lab would follow the same procedure described above. If an alternate site is necessary, the access control plan would mimic the plan used at our lab.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **ii) Facility security plan** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

**The Vision Council *sez****: Your facility that houses the equipment that has access to ePHI information should have policies and procedures in place that require authorized physical access to such facility, protects against equipment being tampered with, and has a facility security system that protects the ePHI information from theft. To the extent your facility allows the use of off-site equipment that has access to ePHI information, the policies and procedures should address protection and access to such equipment.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how your lab safeguards your facility and equipment from having unauthorized physical access, tampering and theft; such as: our facility has a written policy defining our procedures protecting against unauthorized access, tampering or theft of ePHI information.(reference written policy name and location). Our facility has a managed access security system that is control by a trained associated or a password control electronic access system (keyed or alarm code security alarm system) protecting against tampering and theft of ePHI information at all times.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **iii) Access control and validation procedures** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

**The Vision Council *sez****: Your laboratory should have procedures and physical controls in place that control person’s access to ePHI information. This should included access to the area that physically houses the computers and the programs that allows access to ePHI information*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe your lab procedures to control and validate a person’s access to your facilities; such as: our facility controls and validates workforce members’ access to facilities based on their role or function, and our facility has visitor controls that do not allow unauthorized personnel access to laboratory areas where ePHI information is visible or accessible. Our computer systems that access ePHI information have login authorization controls that do not allow unauthorized personnel access to ePHI information. All storage areas containing ePHI information are controlled by lock and key allowing access only to personnel with ePHI access authorization.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **iv) Maintenance records** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

**The Vision Council *sez****: Your lab should have documents, either electronic or printed, that track all modifications and or repairs to areas in your facility that store or process ePHI information. Such documentation should also include appropriate mention of laptops and other portable media storage devices being used by the lab’s employees.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe your policies and procedures for documenting repairs and modifications to your physical facilities that house ePHI information such as; our laboratory has a facilities repair manual (name manual and its location, computer or printed copy) that documents all repairs made to our laboratory facilities that house the electronic equipment processing ePHI information and or areas that store ePHI information.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**2) WORKSTATION USE (Required - Std)**

**HIPAA sez:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

[ ] Yes. Our lab complies with this standard by .

**The Vision Council *sez****: Determine the application programs that can be run and the data that can be accessed for each workstation that can access ePHI. Define the policies that specify the physical location of workstations that can access ePHI to minimize viewing of ePHI by unauthorized persons. Describe your lab’s policy and procedures for the use and configuration of your computer work stations, such as: all of our work stations require user log in and password validation prior to their use accessing ePHI information and the areas they are located in are secured by electronic security authorization. This policy should also provide procedures for remote access, internet use, and E-Mail.*

**3) WORKSTATION SECURITY (Required - Std)**

**HIPAA sez:** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

[ ] Yes. Our lab complies with this standard by .

**The Vision Council *sez****: For computer workstations that access ePHI, implement appropriate physical safeguards. These could include isolating workstations using dividers, doors and screen barriers to prevent unauthorized viewing. It may also include relocating workstations to non-public areas. Describe how you have physically safeguarded your computer workstations accessing ePHI information, such as:*  *our computer workstations have dividers, doors and or screen barriers to prevent unauthorized viewing of ePHI information, or the area where work stations accessing ePHI information are secured by electronically controlled access doors restricting unauthorized personnel.*

**4) DEVICE AND MEDIA CONTROLS**

 **HIPAA sez:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

 **i) Disposal** **(Required - ImpSpec)**

**HIPAA sez:** Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

[ ] Yes. Our lab complies with this implementation specification by .*.*

**The Vision Council *sez****: When disposing of media (tapes, CD, floppy disks, removable hard-drives, etc.) and or computers with hard drives containing ePHI information, simply reformatting the hard drives or media is insufficient to remove data. Acceptable procedures are to physically destroy the media or hard drives (incineration, breaking or cutting into multiple pieces) or running commercially available media erasing programs (this website - www.privacysoftwarereport.com - references many software tools that will erase hard drives). Prior to destruction or disposal, care must be taken to ensure the device or media does not contain ePHI. Describe your lab’s policy and procedures for the disposal of hardware, or electronic media which stores ePHI information, such as: our lab’s disposal of electronic media and computer hard drives containing ePHI is accomplished by running a media erasing program (name program or procedure) and/or physically destroying the media*

 **ii) Media re-use** **(Required - ImpSpec)**

**HIPAA sez:** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Before reusing media (tapes, CD’s, floppy disks, removable hard-drives, etc.) and/or computers with hard drives containing ePHI information, one must make sure that all ePHI information has been removed. Describe your lab’s procedures for the removal of ePHI information from electronic media before its reuse, such as: our laboratory procedures require reformatting of all computer data drives by using a security sensitive data removal program (name program; there are many available) before the data drives are reused. We document (name document, and location of this document) all equipment that goes through this process.*

 **iii) Accountability** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

**The Vision Council *sez****: A written or computer created document/log should be maintained documenting who, what, and where media containing ePHI information is moved.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe your lab’s record keeping procedures for the movement/relocation of computer equipment containing ePHI information such as; our laboratory maintains a log (name log, either electronic or hard copy) that tracks personnel responsible for the implementation, maintenance and reuse of all hardware that contains ePHI information.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **iv) Data backup and storage (Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment

**The Vision Council *sez****: If equipment containing ePHI is going to be moved or relocated, an exact copy of the ePHI information should be made on a retrievable storage device (like tapes, CD’s, floppy disks, removable hard-drives, etc). After the ePHI information has been backed up/copied you should validate that the backed up/copied media is accessible and is a true representation of the original ePHI information.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe your lab’s backup procedures for equipment storing ePHI information; such as: our computer systems backs up (hourly, daily, weekly) to a redundant data storage system allowing us to remove the primary storage system without loss of ePHI information. All ePHI authorized users have access to the backup data storage system.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**C. TECHNICAL SAFEGUARDS - Section 164.312**

**1) ACCESS CONTROL**

 **HIPAA sez:** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

 **i) Unique user identification** **(Required - ImpSpec)**

**HIPAA sez:** Assign a unique name and/or number for identifying and tracking user identity.

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Your lab software programs that have access to ePHI information are required to have unique login names and/or numbers so software users accessing ePHI information can be tracked or identified. Describe how your lab’s computer system has unique user identification, such as: our software requires unique logins and password for each software user accessing ePHI information. It has reports (name reports) that identify all users that are logged in to our system.*

 **ii) Emergency access procedure** **(Required - ImpSpec)**

**HIPAA sez:** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: This requires your lab software having ePHI accessibility to have built in redundancy (backup, duplication) so that in case of a hardware or software emergency users will have access to ePHI information. Describe your emergency procedures for obtaining ePHI information during an emergency, such as: Our computer systems that store ePHI information are backed up to redundant systems allowing users having ePHI access authorization, access to ePHI information from our backup system during an emergency with our primary system. All the security controls for ePHI information on our primary systems are used on our redundant system.*

 **iii) Automatic logoff** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

**The Vision Council *sez****: Your lab software system that accesses ePHI information should have users automatically logged off programs that have access to ePHI information after a predetermined time of inactivity. Automatic logoff should also occur for users remotely accessing ePHI information.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how your lab computer accessing ePHI information terminates electronic sessions; such as: our software system automatically logs users out of applications accessing ePHI information after 1 minute of inactivity.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **iv) Encryption and decryption** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement a mechanism to encrypt and decrypt electronic protected health information.

**The Vision Council *sez****: Your lab software and or hardware systems that electronically access and/or store ePHI information electronically should encrypt ePHI information when storing such information, as to make it not printable or readable when accessed by computer software applications, unless it has been decrypted by software and or hardware programs that are ePHI security compliant. All laptops and removable media storage devices should also encrypt ePHI information that is stored or accessed by such a device.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how your lab’s computer system encrypts and decrypts ePHI; such as: all stored ePHI information in our laboratory computer system is encrypted as to make it not readable or printable without being accessed by a computer program that complies with ePHI access security requirements. After laboratory use any paper with ePHI information is destroyed or stored in a ePHI secured environment.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**2) AUDIT CONTROLS (Required - Std)**

**HIPAA sez:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

[ ] Yes. Our lab complies with this requirement by .

**The Vision Council *sez****: Verify that your computer hardware or OS (Operating System) uses system features that track user activity accessing ePHI information. Describe how your lab’s computer systems that access or store ePHI information, record and or track their activity, and how logs are reviewed, such as: our Windows 2000 OS has a directory/file services feature that tracks and records ePHI information access activity. We review these system audit logs periodically. Any potential threats or incidents are reported to the Security Officer, who must investigate all reports of threats or incidents.*

**3) INTEGRITY (Required - Std)**

 **HIPAA sez:** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

 **i) Mechanism to authenticate electronic PHI** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

**The Vision Council *sez****: Develop procedures and documentation for your lab computer system that accesses ePHI information to verify a system user cannot alter or destroy ePHI information once it has been electronically stored.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how your lab verifies and authenticates ePHI information has not be altered or destroyed; such as: our lab has developed procedures, refer to your laboratory procedures document that retrieves ePHI stored information and compares it to the original document validating that it has not be altered. We also periodically test our laboratory computer software system, which accesses ePHI information, that it cannot randomly or inadvertently delete or change ePHI information once stored on our computer.*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****; or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**4) PERSON OR ENTITY AUTHENTICATION (Required - Std)**

**HIPAA sez:** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

[ ] Yes our lab complies with this specification by .

**The Vision Council *sez****: Verify that your lab’s computer system accessing ePHI information validates/verifies the person accessing ePHI information is who they claim to be. Describe how your lab verifies and authenticates that persons accessing ePHI information are who they claim to be; such as: our computer system requires user defined passwords for validating people are who they claim to be.*

**5) TRANSMISSION SECURITY**

**HIPAA sez:** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

 **i) Integrity controls** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

**The Vision Council *sez****: All ePHI information transmitted to your laboratory computer system should not allow modification of ePHI information without electronic documentation of who, what, when, and why the document was modified. Such electronic documentation shall stay with the original document until the original document has been disposed of.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how your lab maintains the integrity of ePHI information before it is disposed of, such as: our laboratory computer system does not grant system users accessing ePHI information the right to modify or delete an original ePHI document. Our systems administrative users, that have the right to modify ePHI information, have all of their transactions logged and documented by our laboratory computer system (refer to the computer log that tracks these transaction).*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

 **ii) Encryption** **(Addressable - ImpSpec) Check one box below**

**HIPAA sez:** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

**The Vision Council *sez****: Wherever ePHI information is stored, accessible or printable in your laboratory (or off-site through removable media storage devices), your laboratory systems should encrypt ePHI information when it is not necessary for processing Rx’s in your laboratory.*

[ ] Yes. Our lab complies with this implementation specification by .

**The Vision Council *sez****: Describe how your lab’s computer system encrypts ePHI information, such as: our laboratory computer system encrypts all ePHI information, as to make it not accessible or readable and does not print ePHI information on laboratory paper work (i.e. not printing full patient names on work tickets, or social security numbers on any documents being processed in your lab). Any paper work that has ePHI information revealed is destroyed after its use.]*

[ ] Our laboratory **does adopt** an equivalent alternative measure: .

[ ] Our laboratory **does not adopt** an equivalent alternative measure: .

**The Vision Council *sez****: Explain why it is not reasonable and appropriate to adopt the implementation specification. Then explain either:*

*- the equivalent alternative measure which the lab* ***does adopt****, or,*

*- the reasonable and appropriate basis why the lab* ***does not adopt*** *an equivalent alternative measure.*

*NOTE: A lab must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the lab’s risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a lab makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.*

**ORGANIZATIONAL REQUIREMENTS - Section 164.314**

**1) Business Associate Agreement**

[ ] In those instances where this lab is required to obtain a BAA, it shall do so using the form at Exhibit A hereto, and shall attach a copy of the signed BAA as Exhibit A-1 hereto. If this lab already has a BAA with another entity under the HIPAA Privacy Rule, the lab should replace such BAA with a signed copy of the BAA as set forth in Exhibit A hereto.

**The Vision Council *sez****:*

*A. When is a Business Associate Agreement required?*

 *If the lab provides electronic PHI to a Business Associate, it must enter into a Business Associate Agreement (“BAA”) to assure that the Business Associate adequately protects that electronic PHI. With respect to a Covered Entity, a “Business Associate” is a person or entity who performs a function or activity involving the use or disclosure of PHI on behalf of the Lab, such as claims processing or administration, data analysis, processing or administration, utilization review or quality assurance, which activity involves disclosure of ePHI. The Business Associate will sign a Business Associate Agreement stating that the Business Associate will comply with the Security Rule with respect to ePHI.*

 *For example, if a lab utilizes a supplier of lab processing software, and that supplier accesses the lab’s ePHI, either online or via backup tapes, for purposes of software support and process control troubleshooting, a BAA would be required.*

 *Some entities to which a lab will provide electronic PHI may not be**Business Associates and therefore will not need to sign a BAA with the lab.*

*B. A Business Associate Agreement* ***IS NOT*** *required when:*

*1. A lab gives electronic PHI upstream to an eye care professional or downstream to a coating lab or other entity for further lens treatment, since both situations involve provision of electronic PHI for treatment purposes, which is expressly exempted from the BAA requirements.*

*2. A lab gives electronic PHI to a vision plan as part of a payment claim.*

**POLICIES, PROCEDURES AND DOCUMENTATION REQUIREMENTS - Section 164.316**

**HIPAA sez:** Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of HIPAA Security Regulations.

[ ] Yes. Our lab complies with this requirement. This Manual and compliance with this manual constitutes this Lab’s implementation of policies and procedures to comply with the HIPAA Security Regulations.

**1) DOCUMENTATION**

**HIPAA sez:** Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and, if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

[ ] Yes. Our lab complies with this requirement. This document (which may be maintained in electronic and/or hard copy form), when properly completed and signed by the lab’s security official, constitutes the documentation of this lab’s policies and procedures for compliance with the HIPAA security regulations. All actions, activities or assessments required by the policies herein shall be documented in this document.

 **i) Time limit** (**Required - ImpSpec**)

**HIPAA sez:** Retain the documentation required by paragraph (1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

[ ] Yes. Our lab complies with this requirement. Each document within this overall document shall be retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later.

 **ii) Availability** (**Required - ImpSpec**)

**HIPAA sez:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

[ ] Yes. Our lab complies with this requirement. This Manual will be made available to those persons responsible for implementing the procedures herein.

 **iii) Updates** (**Required - ImpSpec**)

**HIPAA sez:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[ ] Yes. Our lab complies with this requirement. This document shall be reviewed at least annually and in addition in response to environmental or operational changes affecting the security of electronic PHI; and this document shall be updated as needed in response to such review. The dates of each annual or event-driven review shall be set forth below and initialed by this lab’s security official; and a written report summarizing any update resulting from such review shall be attached hereto at Exhibit B.

 Type of Review

(Annual or Event-Driven) Date Report on Review

|  |  |  |
| --- | --- | --- |
|  |  | See Exhibit B |
|  |  | See Exhibit B |
|  |  | See Exhibit B |
|  |  | See Exhibit B |
|  |  | See Exhibit B |
|  |  | See Exhibit B |

*(Attach Additional Pages When Necessary)*

**DEFINITIONS - Section 164.304**

As used in this subpart, the following terms have the following meanings:

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this the Security Rule, not as used in [the Privacy Rule].)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate’s workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

**SECURITY STANDARDS: GENERAL RULES - Section 164.306**

a) General requirements. Covered entities and business associates must do the following:

1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

4) Ensure compliance with this subpart by its workforce.

b) Flexibility of approach.

1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

i) The size, complexity, and capabilities of the covered entity or business associate.

ii) The covered entity's or business associate’s technical infrastructure, hardware, and software security capabilities.

iii) The costs of security measures.

iv) The probability and criticality of potential risks to electronic protected health information.

c) Standards. A covered entity or business associate must comply with the applicable standards as provided in this section and in Sections 164.308, 164.310, 164.312, 164.314, and 164.316 with respect to all electronic protected health information.

d) Implementation specifications. In this subpart:

1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.

2) When a standard adopted in Sections 164.308, 164.310, 164.312, 164.314, or 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

3) When a standard adopted in Sections 164.308, 164.310, 164.312, 164.314, or 164.316 includes addressable implementation specifications, a covered entity or business associate must--

i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

ii) As applicable to the entity--

A) Implement the implementation specification if reasonable and appropriate; or

B) If implementing the implementation specification is not reasonable and appropriate--

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

e) Maintenance. A covered entity or business associate must review and modify the security measures implemented under this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at Section 164.316.

**EXHIBIT A BUSINESS ASSOCIATE AGREEMENT**

**(For Compliance with HIPAA Privacy and Security Rules)**

This Business Associate Agreement (“B.A. Agreement”) is entered into by and between *[Optical Laboratory]* (“Covered Entity”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(“Business Associate”) as of this \_\_\_\_\_\_ day of \_\_\_\_\_\_\_, 20\_\_ (“Effective Date”) .

**RECITALS**

WHEREAS, *[Optical Laboratory]* is a “Covered Entity” as defined under the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) and its implementing regulations (collectively, “HIPAA”), as amended by the regulations promulgated pursuant to the Health Information Technology for Economic and Clinical Health (“HITECH”) Act (Division A, Title XIII and Division B, Title IV of Public L. 111–5) (which was part of the American Recovery and Reinvestment Act of 2009), and \_\_\_\_\_\_\_\_\_\_\_\_\_ is a “Business Associate” as defined under HIPAA; and

WHEREAS, in connection with the *[services]* agreement between Covered Entity and Business Associate for Business Associate to provide *[certain services]* for and on behalf of Covered Entity (the “Agreement”), Covered Entity may provide Business Associate with Protected Health Information (defined below); and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to this BAA, which is drafted to satisfy specific components of HIPAA and relevant implementing regulations, including the Privacy Rule (defined below), the Security Rule (defined below) and the Breach Notification Rule (defined below).

**I. DEFINITIONS**

(a) “Breach” shall have the meaning given to such term in 45 C.F.R. § 164.402 and applicable State data breach notification law.

(b) “Breach Notification Rule” shall mean the rule related to breach notification for Unsecured Protected Health Information at 45 C.F.R. Parts 160 and 164.

(c) “Designated Record Set” shall have the meaning given to such term under the Privacy Rule at 45 C.F.R. § 164.501.

(d) "Electronic Protected Health Information" or ("EPHI") shall have the same meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity..

(e) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. Parts 160 and Part 164, Subparts A and E.

(f) “Protected Health Information” or “PHI” shall have the meaning given to such term under the Privacy and Security Rules at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(g) “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. § 164 Subparts A and C.

(h) Other capitalized terms used, but not otherwise defined, in this B.A. Agreement shall have the same meaning as those terms in the Privacy, Security or Breach Notification Rules.

**II. PRIVACY RULE****OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE**

(a) Limitations of Disclosures. Business Associate agrees to not use or disclose PHI other than as permitted or required by this B.A. Agreement or, the Agreement, or as Required By Law. Business Associate shall not use or disclose PHI in a manner that would violate the Privacy Rule if done by Covered Entity, unless expressly permitted to do so pursuant to the Privacy Rule, the Agreement, and this B.A. Agreement.

(b) Appropriate Safeguards. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as permitted by this B.A. Agreement, the Agreement, or as Required By Law.

(c) Obligations on Behalf of Covered Entity. To the extent Business Associate carries out an obligation for which Covered Entity is responsible under the Privacy Rule, Business Associate must comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation.

(d) Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of HIPAA, the Agreement, or this B.A. Agreement.

(e) Reporting of Improper Use or Disclosure. Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this B.A. Agreement within five (5) days of which it becomes aware.

(f) Business Associate’s Subcontractors. Business Associate agrees to ensure that any Subcontractor, consistent with 45 C.F.R. § 164.502(e)(1)(ii), that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees in writing to the same restrictions and conditions that apply through this B.A. Agreement to Business Associate with respect to such PHI.

(g) Access to PHI. Business Associate shall provide access, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual or a third party designated by the Individual, in order to meet the requirements under the Privacy Rule at 45 C.F.R. § 164.524.

(h) Amendment of PHI. Business Associate shall make any PHI contained in a Designated Record Set available to Covered Entity (or an Individual as directed by Covered Entity) for purposes of amendment per 45 C.F.R. § 164.526. Business Associate shall make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to the Privacy Rule, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity. If an Individual requests an amendment of PHI directly from Business Associate or its Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of receiving such request. Any denial of amendment of PHI maintained by Business Associate or its Subcontractors shall be the responsibility of Covered Entity.

(i) Government Access to Records. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI, available to the Secretary, in a time and manner designated by the Secretary, for determining Covered Entity’s compliance with the Privacy Rule.

(j) Documentation and Accounting of Disclosures. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528. Business Associate agrees to provide to Covered Entity, in time and manner requested by Covered Entity, information collected in accordance with this paragraph, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

(k) Retention of PHI. Notwithstanding Section VI(c) below, Business Associate and its Subcontractors shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under Section II(j) for a period of six (6) years after termination of the Agreement.

(l) Minimum Necessary. Business Associate shall only request, use and disclose the Minimum Necessary amount of PHI necessary to accomplish the purpose of the request, use or disclosure.

**III. PERMITTED USES AND DISCLOSURES OF PHI BY BUSINESS ASSOCIATE**

(a) Permitted Uses and Disclosures of PHI. Except as provided in Paragraphs (b), (c), and (d) of Section III, Business Associate may only use or disclose PHI to perform functions, activities or services for, or on behalf of Covered Entity, as specified in the Agreement.

(b) Use for Management and Administration. Except as otherwise limited in this B.A. Agreement, Business Associate may, consistent with 45 C.F.R. 164.504(e)(4), use PHI if necessary (i) for the proper management and administration of Business Associate, or (ii) to carry out the legal responsibilities of Business Associate.

(c) Disclosure for Management and Administration. Except as otherwise limited in this B.A. Agreement, Business Associate may, consistent with 45 C.F.R. 164.504(e)(4), disclose PHI for the proper management and administration of Business Associate, provided (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed (“Person”) that it will be held confidentially and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the Person, and that the Person agrees to immediately notify Business Associate in writing of any instances of which it becomes aware in which the confidentiality of the information has been breached or is suspected to have been breached.

(d) Reporting Violations. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

**IV. SECURITY RULE OBLIGATIONS OF BUSINESS ASSOCIATE**

(a) Compliance with the Security Rule. Business Associate agrees to comply with the Security Rule with respect to Electronic Protected Health Information and have in place reasonable and appropriate Administrative, Physical, and Technical Safeguards to protect the Confidentiality, Integrity, and Availability of EPHI and to prevent the use or disclosure of EPHI other than as permitted by the Agreement, this B.A. Agreement, and as Required By Law.

(b) Subcontractors. Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits EPHI on behalf of Business Associate agrees in writing to comply with the Security Rule with respect to such EPHI.

(c) Security Incident/Breach Notification Reporting. Business Associate shall report any Security Incident promptly upon becoming aware of such incident. Separate from the requirements related to Security Incident reporting, Business Associate shall also make the reports set forth below in Section V, related to a Breach of Unsecured PHI.

**V. BREACH NOTIFICATION (FEDERAL AND STATE) RULE OBLIGATIONS OF BUSINESS ASSOCIATE**

(a) Notification Requirement. Immediately following Business Associate’s discovery of a Breach, or upon Business Associate’s reasonable belief that a Breach has occurred, Business Associate shall provide written notification of such Breach to Covered Entity.

(b) Discovery of Breach. For purposes of reporting a Breach to Covered Entity, the discovery of a Breach shall occur on the first day on which such Breach is known to Business Associate or, by exercising reasonable diligence, would have been known to or suspected by the Business Associate. Business Associate will be considered to have had knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known to any person (other than the person committing the Breach) who is an employee, officer or agent of the Business Associate.

(c)Content of Notification. Any notice referenced above in Section V(a) of this B.A. Agreement will include, to the extent known to the Business Associate, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach, as well as the information, to the extent known by Business Associate, that Covered Entity is required to include in its notification to the individual pursuant to the Breach Notification Rule or applicable State data breach notification laws. Business Associate will also provide (on a continuing basis as information is discovered) to Covered Entity other available information that Covered Entity is required to include in its notification to the individual pursuant to the Breach Notification Rule or applicable State data breach notification laws.

(d) Cooperation with Covered Entity. Business Associate shall:

(i) Cooperate and assist Covered Entity with any investigation into any Breach or alleged Breach, including those conducted by any Federal agency, State Attorney General, State agency (or their respective agents);

(ii) Comply with Covered Entity’s determinations regarding Covered Entity’s and Business Associate’s obligations to mitigate to the extent practicable any potential harm to the individuals impacted by the Breach; and

(iii)As directed by the Covered Entity, assist with the implementation of any decision by Covered Entity or any Federal agency, State agency, including any State Attorney General, or their respective agents, to notify and provide mitigation to individuals impacted or potentially impacted by a Breach.

**VI. TERM AND TERMINATION**

(a) Term. The term of this B.A. Agreement shall commence as of the Effective Date, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy the PHI, protections are extended to such information, in accordance with the provisions of this Section VI.

(b) Termination for Cause. Upon Covered Entity’s knowledge of a material breach of the terms of this B.A. Agreement, Covered Entity shall:

(i) Provide an opportunity for Business Associate to cure, and, if Business Associate does not cure the breach within thirty (30) days, Covered Entity may immediately terminate this BAA and the Agreement;

(ii) Immediately terminate this BAA and the Agreementif Covered Entity has determined that (a) Business Associate has breached a material term of this BAA, and (b) cure is not possible; or

(iii) Immediately terminate this BAA if the Agreement has been terminated.

(c) Effect of Termination.

(i) Except as provided for in paragraph (ii) of this Section VI(c), upon termination of this B.A. Agreement for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, and shall not retain copies thereof. This provision shall apply to PHI that is in the possession of Subcontractors of Business Associate.

(ii) In the event that Business Associate and Covered Entity determine, by mutual agreement, that returning or destroying the PHI is infeasible, Business Associate shall extend the protections of this B.A. Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

**VII. MISCELLANEOUS**

(a)Regulatory References. A reference in this B.A. Agreement to a section in the Privacy, Security, or Breach Notification Rule means the section as in effect or as amended, and for which compliance is required.

(b) Survival. The respective rights and obligations of Business Associate under Section 6(c) of this BAA shall survive the termination of the BAA.

(c) No Third Party Beneficiaries. Nothing express or implied in this B.A. Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

(d) Amendment. The parties agree to take such action as is necessary to amend this B.A. Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy, Security or Breach Notification Rules, as well as HIPAA and HITECH.

(e) Effect on Agreement. Except as specifically required to implement the purposes of this B.A. Agreement, or to the extent inconsistent with this B.A. Agreement, all other terms of the Agreement shall remain in force and effect.

(f) Interpretation. The provisions of this B.A. Agreement shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provision in this B.A. Agreement. Any ambiguity in this B.A. Agreement shall be resolved to permit Covered Entity to comply with the Privacy, Security, and Breach Notification Rules, as well as HIPAA and HITECH.

(g) Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this B.A. Agreement is satisfactory for Business Associate to comply with any obligations it may have under HIPAA, the Privacy Rule, or any other applicable law or regulation pertaining to the confidentiality, use or safeguarding of health information. Business Associate is solely responsible for all decisions it makes regarding the use, disclosure or safeguarding of PHI.

(h) Indemnification.

(i) Business Associate shall indemnify, defend and hold Covered Entity and its officers, directors, employees, agents, successors and assigns (“Covered Entity Indemnitees”) harmless, from and against any and all losses, claims, actions, demands, liabilities, damages, costs and expenses (including, but not limited to, costs of providing notifications and credit monitoring services to individuals pursuant to the Breach Notification Rule and State data breach notification laws, administrative costs associated with Covered Entity’s and Business Associate’s compliance with Breach Notification Rule and State data breach notification laws, judgments, settlements, court costs and reasonable attorneys’ fees actually incurred) (collectively, “Information Disclosure Costs”) arising from or related to: (1) any breach of this BAA by Business Associate, including but not limited to the use or disclosure by Business Associate of Individually Identifiable Information (including PHI) in violation of the terms of this B.A. Agreement or applicable law; and (2) whether in oral, paper or electronic media, any Breach caused, directly or indirectly, by Business Associate.

(i) Counterparts. This B.A. Agreement may be executed in multiple counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument. Facsimile or electronic (PDF) signatures shall be treated as original signatures. This B.A. Agreement shall be binding when one or more counterparts hereof, individually or taken together, shall bear the signatures of all of the parties reflected on this B.A. Agreement as the signatories thereto.

***[Optical Laboratory]*: *[Business Associate]*:**

By:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_