SECTION 1. POLICY: OVERVIEW

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

A. HIPAA AND PRIVACY CONTINUING EDUCATION

Our organization is committed to protecting the privacy of individual health information in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations promulgated thereunder. Our Compliance Officers and Compliance Site Leads will remain knowledgeable and stay up to date on HIPAA regulatory requirements (HIPAA background, Privacy and Security Rules, and Enforcement/Penalties).

BACKGROUND OF HIPAA

The Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191, 42. U.S.C. §§ 1320d-1320d-8), better known as "HIPAA," was one of the most sweeping pieces of federal legislation to impact the health care industry. Its initial intent was to reduce the rising costs of health care by providing portability of health care coverage for consumers and creating efficiencies in health care administration through standardization in electronic transactions. During debate over this legislation, Congress recognized that the advances in technology that were proposed could erode the privacy of health information. Therefore, as part of the Act, Congress mandated the development of federal privacy protections for Individually Identifiable Health Information.

THE PRIVACY AND SECURITY RULES

The HIPAA Privacy and Security Rules (45 CFR. Parts 160, 162 and 164) set forth standards to protect the privacy and security of Protected Health Information (PHI) in all forms—verbal, written and electronic. Business Associates must develop, implement and maintain privacy and security policies and procedures that meet the numerous standards under the Privacy and Security Rules, with a primary focus on prohibiting unauthorized or inappropriate use and disclosure of PHI. Entities must also educate employees with respect to its HIPAA privacy and security policies.

ENFORCEMENT/PENALTIES

The Federal Trade Commission and state attorneys general are taking an active role in protecting the privacy rights of consumers. Enforcement actions by the Federal Trade Commission or a state attorney general can include injunctive relief (e.g., requiring the challenged conduct to stop) and/or civil fines.

The Office for Civil Rights in the Department of Health and Human Services is the regulatory agency responsible for enforcing civil penalties under HIPAA. The Department of Justice is the agency that enforces criminal penalties under HIPAA. Furthermore, the HITECH Act gives state attorneys general the authority to file suit in federal court against any entity accused of violating HIPAA in a manner that the attorney general has reason to believe adversely affects any resident of that attorney general's state.

The civil monetary penalties for noncompliance with HIPAA are significant. The HITECH Act increased the amount of civil penalties that can be applied to violators of HIPAA. The civil monetary penalties now range from $100 to $50,000 per HIPAA violation. The maximum penalty that can be applied for all identical violations in any one year is $1,500,000.

B. PRIVACY PROGRAM OVERSIGHT — ROLES & RESPONSIBILITIES

Our organization has designated a Compliance Officer (CO) who shall be responsible for overseeing the implementation of, and compliance with, our privacy policies and procedures that provide guidance for the protection and safeguarding of Protected Health Information (PHI) and Personally Identifiable Information (PII). This will include oversight of privacy-related policies and procedures; receiving and responding to requests, complaints and reports of alleged violations (security breaches); and providing guidance and information about privacy-related matters.

The Compliance Officer will be responsible for implementing and coordinating the compliance program within the organization, which includes a HIPAA Privacy Program, elements required by CMS—Centers for Medicare & Medicaid Services (when applicable), Telephone Consumer Protection Act (TCPA), California Consumer Privacy Act (CCPA) and other regulatory elements as applicable. The Partner may designate additional compliance team members as Site Leads if additional assistance is needed. Collectively, the Partner Compliance Officer and Site Leads make up the organization's Compliance Team.

The Compliance Team shall develop administrative policies and procedures and maintain them as necessary in accordance with HIPAA privacy regulations, TCPA, CCPA and CMS regulations. The Compliance Team shall revise the policies and procedures from time to time and as may be required by changes in federal and/or state law.

SECTION 1. PROCEDURES: OVERVIEW

A. HIPAA AND PRIVACY CONTINUING EDUCATION

The Compliance Officers and Site Leads are expected to remain current on their understanding of HIPAA regulations and enforcement actions through a variety of virtual or self-study options including but not limited to webinars or conferences.

- Subscribing to alerts and industry newsletters regarding updates to HIPAA or privacy and security topics (e.g., Bloomberg Privacy and Security Newsletter)

B. DEFINITIONS — GLOSSARY OF TERMS

The following terms, when capitalized, have the following meanings:

1. **Platform.** Integrity Marketing Group is a shared services platform for multiple insurance marketing organizations. All references to "Integrity" or the "Platform" hereafter include all organizations under the common ownership of Integrity. A listing of Integrity organizations can be provided upon request.
2. **Partner.** Integrity Marketing Group is a platform of Partners operating as independent insurance marketing organizations leveraging Integrity's shared services that include a compliance program with elements that cover insurance marketing organization regulatory responsibilities.
3. **Accounting for Disclosures.** Information that describes a Covered Entity's or Business Associate's disclosures of PHI, other than disclosures of hard-copy or electronic-copy (other than electronic health records as described below) PHI for Treatment, Payment and Health Care Operations; disclosures made with patient authorization; and certain other limited disclosures, provided that disclosures of PHI through electronic health records for purposes of Treatment, Payment and Health Care Operations must be listed on an accounting of disclosures. For those categories of disclosures that need to be in the accounting, the accounting must include disclosures that have occurred during the six years prior to the date of the request for an accounting (or a shorter time period at the request of the Individual), with two important exceptions: (1) an accounting of disclosures for Treatment, Payment and Health Care Operations made through an electronic health record need only include disclosures that occurred within the three years prior to the date of the request for an accounting, and (2) disclosures made before the compliance date for a Covered Entity are not part of the accounting requirement.
4. **Authorization (HIPAA Authorization).** A specific type of written permission given by the Individual to use and/or disclose Protected Health Information about the Individual. The requirements of a valid authorization are defined in the HIPAA regulations and Integrity's policies/procedures.
5. **Breach.** The unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of such information, except where an unauthorized person to whom the information is disclosed would not reasonably have been able to retain such information. Breach means the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under Subpart E of HIPAA, which compromises the security or privacy of the Protected Health Information. The definition of Breach excludes

the use or disclosure of Protected Health Information that does not include the identifiers listed in 45 CFR § 164.514(e)(2), date of birth and ZIP code and does not compromise the security or privacy of Protected Health Information. The identifiers listed in 45 CFR § 164.514(e)(2) are as follows:

- Names
- Postal address information, other than town or city, state and ZIP code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographic images and any comparable images

Breach Assessment Factors

The following four risk factors help determine the probability that Protected Health Information has been compromised:

i. The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification

ii. The unauthorized person who used the Protected Health Information or to whom the disclosure was made

iii. Whether the Protected Health Information was actually acquired or viewed

iv. The extent to which the risk to the Protected Health Information has been mitigated

Notice to the U.S. Department of Health and Human Services

If Integrity determines that it is a Breach of unsecured Protected Health Information based on the Breach Assessment Factors and it affects more than 500 individuals, Integrity or applicable Carrier or Carriers shall notify the U.S. Department of Health and Human Services within sixty (60) days of discovery.

If less than 500 individuals are affected by a Breach of unsecured Protected Health Information, Integrity shall maintain a log of breaches and notify the Department of Health and Human Services within sixty (60) days after the end of each calendar year.

5. **Business Associate.** Generally, an entity or person who performs a function or service on behalf of a Covered Entity, and in performing the function or service, creates, receives or maintains PHI from or on behalf of a Covered Entity.
6. **Confidential Information.** Confidential Information is information related to Integrity or its clients that is proprietary or otherwise nonpublic information. Confidential Information includes, but is not limited to, any of the following information in any form: proprietary information of Integrity or of an Integrity client; PHI; PII; minutes for board of directors and other committee meetings; business records; marketing and business development goals, strategies and plans; correspondence; fees; compensation and benefits information; intellectual property; trade secrets; human resources data; business processes; and financial information. Also, SSNs, DOBs, policy #s, HICN #s, agent #s, license #s, etc.
7. **Covered Entity.** A health plan, a health care clearinghouse or a health care provider who transmits health information in electronic form in connection with financial or administrative activities related to health care.
8. **De-identified Data.** Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is de-identified. Health information is considered de-identified (1) if stripped of all the 18 direct identifiers defined under HIPAA, or (2) if an expert in statistical and scientific method determines that there is a very small risk that the information could be used alone or in combination with other information to identify an individual. The HIPAA standards do not apply to De-identified Data.
9. **Designated Record Set.** A group of records maintained by or for a Covered Entity that includes (1) medical and billing records about individuals maintained by or for a covered health care provider; (2) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; and (3) used, in whole or in part, by or for the Covered Entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity.
10. **Disclosure.** The release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.
11. **Health Insurance Portability and Accountability Act of 1996 (HIPAA).** A federal law (Public Law 104-191), which, in part, governs the standards for the electronic exchange,

privacy and security of health information. The definition of "HIPAA", as used herein, includes the regulations promulgated thereunder (45 CFR Parts 160 and 164).

12. **Individual.** The person who is the subject of PHI.

13. **Individually Identifiable Health Information.** A subset of Health Information, including demographic information, (1) that is created or received by a health care provider, health plan, or health care clearinghouse; 2) that relates to the physical or mental health or condition of an individual, the provision of health care to an individual or the payment for the provision of health care to an individual; and (3) that identifies the individual, or might reasonably be used to identify the individual.

14. **Marketing.** Marketing means to communicate about a product or service that encourages recipients of the communication to purchase or use the product or service.

15. **Minimum Necessary.** The least information reasonably necessary (i.e., minimum amount) to accomplish the intended purpose of the use, disclosure, or request. Unless an exception applies, this standard applies when using or disclosing PHI or when requesting PHI.

16. **OCR.** Office of Civil Rights, the branch of the HHS that is responsible for federal oversight of the privacy and security regulations.

17. **Personally Identifiable Information (PII).** Information related to an individual that is sensitive information, such as credit card numbers, social security numbers, drivers' license numbers or other information that could be used to facilitate identity theft of the individual.

18. **Privacy Rule.** The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.

19. **Protected Health Information (PHI).** Any information, whether oral or recorded in any form or medium that is created or received by a Covered Entity that identifies an Individual or might reasonably be used to identify an Individual and relates to:

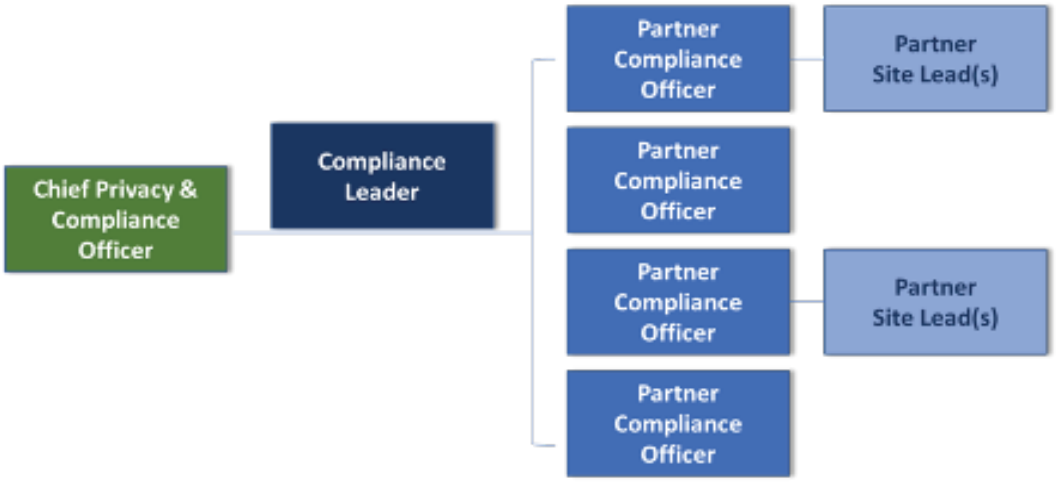
    - The individual's past, present or future physical or mental health; OR
    - The provision of health care to the individual; OR
    - The past, present or future payment for health care

    Information is deemed to identify an Individual if it includes either the patient's name or any other information that taken together or used with other information could enable someone to determine an Individual's identity. (For example: date of birth, medical record number, health plan beneficiary number, address, ZIP code, phone number, email address, fax number, IP address, license number, full-face photographic images or Social Security number.)

20. **Use.** With respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

C. PRIVACY PROGRAM OVERSIGHT: ROLE OF THE CHIEF PRIVACY AND COMPLIANCE OFFICER, COMPLIANCE LEADERS, COMPLIANCE OFFICERS AND SITE LEADS

Integrity's Chief Compliance and Privacy Officer (i.e., CCPO or Chief Privacy Officer), Chief Information Security Officer, Compliance Leaders, along with Partner Compliance Officers and Compliance Site Leads are responsible for maintaining and overseeing Integrity's HIPAA Privacy Program.



THE CHIEF PRIVACY AND COMPLIANCE OFFICER

Integrity's leadership or board of directors will formally designate the Chief Compliance and Privacy Officer to oversee the compliance program for all of Integrity's platform partners, including our organization. The Chief Privacy and Compliance Officer will formally designate the Compliance Officer(s) and Site Lead(s) as needed to support the business.

COMPLIANCE LEADERS

The Chief Privacy and Compliance Officer will designate Compliance Leaders to help administer Integrity's compliance program within each Integrity platform partner. The Chief Privacy and Compliance Officer and Compliance Leaders will hold quarterly conference calls, or ad hoc calls as needed, to discuss ongoing and potential issues affecting the operations of our organization and the effectiveness of the Privacy Program.

Compliance Leaders shall be responsible for the following:

- Report directly to the CCPO
- Work with the CCPO to update policies and procedures and oversee distribution of updated policies and procedures to Site Compliance Officers and Site Leads on an annual basis

- Work with the CCPO and Site Compliance Officers, and when applicable Site Leads, to draft **Individual Site Plans**, which prioritize action items specific to each of Integrity's Partner offices
- Oversee Individual Site Plans for Integrity Partner offices. This task includes, but is not limited to:
    - Assistance with prioritizing action items
    - Follow-up on progress and completion
    - Ad hoc calls with our organization's Compliance Officer to effectively manage and monitor our compliance program
- Attend regular teleconferences with Integrity's compliance team
- To the extent the site handles Medicare Advantage and/or Prescription Drug Plans, the Compliance Leader or CMS Compliance Leader will assist in the development and implementation of policies and procedures directly related to CMS regulations and offer ongoing assistance with maintaining an effective compliance program in regard to CMS requirements
- Receive and respond to escalated privacy questions from Compliance Officers
- Help Compliance Officers with incident and breach investigations, escalating to the CCPO as needed after at least seven (7) days of investigation
- Monitor the site-specific compliance email inbox whenever a Compliance Officer is out of the office or otherwise unavailable

PARTNER COMPLIANCE OFFICERS

The CCPO (Chief Compliance and Privacy Officer) will designate at least one Compliance Officer at each Integrity platform partner office that will be responsible for administering and managing the compliance program at their office.

The Compliance Officer or Partner may designate additional compliance program leaders as Site Leads who will support the Compliance Officer in fulfilling the following responsibilities:

- Fully support and administer the Compliance Program, which includes a HIPAA Privacy Program and elements required by CMS—Centers for Medicare & Medicaid Services (when applicable), Telephone Consumer Protection Act (TCPA), California Consumer Privacy Act (CCPA) and other regulatory elements as applicable
- Administration of the program includes all required employee training to be completed during initial 90 days of hire and annually. Compliance Officer will ensure the partner workforce training completion is tracked and incomplete training is resolved on a timely basis

- If a specific Partner is contracted with MA/PDP insurance carriers, the Site Compliance Officer and Site Leads are also responsible for CMS compliance regulations, and will ensure that the site is complying with all CMS and carrier-mandated requirements
- Address and implement action items specified in the Individual Site Plan
- Monitor the site-specific compliance email box daily, and escalate any incidents to the Compliance Leader as needed
- Act as the first responder to any reported privacy incidents. This includes ensuring that the CCPO and Compliance Leader are notified of the incident, as well as ensuring that a Privacy Incident Form is completed within twenty-four (24) hours of an incident being reported and an internal investigation is at least preliminarily completed within seven (7) days
- Update the **Privacy Incident Log** whenever a privacy incident is reported or discovered, regardless of the result of the incident's investigation;
    - After an incident is logged and an investigation occurred, create a report that details investigation strategy, action taken, planned mitigation steps, and any appropriate follow-ups
- Retain and record all privacy, security and Medicare-related products (including marketing materials) documentation for ten (10) years on the respective business unit secure network, or indefinitely if a legal hold is put in place, and in accordance with the **Record Retention Guidelines**
- Escalate communication from OCR (including letters and complaints) or other federal or state entities to the designated Compliance Leader and the Chief Compliance and Privacy Officer immediately
- Log all "Accounting for Disclosures" requests and provide a copy annually to the Chief Compliance and Privacy Officer
- Attend regular teleconferences with the entire Integrity Compliance Team
- Identify and update all contracts and agreements, including template agreements, signed by our organization
- Conduct a physical security/clean desk review of employees on a regular basis. Please refer to the **Compliance Review Spreadsheet**
- Complete an annual **Risk Assessment** to identify risk areas within the site's privacy and security program and derive a plan for needed mitigation or remediation steps. Please refer to the **Risk Assessment Questionnaire**

SECTION 2. POLICY: REPORTING & RESPONDING TO COMPLAINTS & VIOLATIONS

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

This section describes security and Medicare-related policy regarding the filing of complaints by individuals with respect to the Partner's privacy policies and procedures, compliance with such policies and procedures, and/or compliance with federal or state law applicable to the confidential nature of PHI or PII.

The Compliance Officer is responsible for developing and implementing a process whereby individuals may register complaints concerning its privacy policies and procedures and compliance with those policies and procedures.

A. REPORTING COMPLAINTS AND VIOLATIONS

Organization encourages and welcomes workforce members and customers to report all suspected or known complaints and violations of its privacy policies or procedures. Violations of the privacy policies should be immediately reported via one of the prescribed methods below or through another approved method.

We will establish formal mechanisms for reporting privacy concerns, including but not limited to Chief Compliance and Privacy Officer, Chief Information Security Officer, Compliance Officer, Site Leads and managers, or by filing an anonymous complaint through a third-party reporting system or sending an email to our organization's Compliance Mailbox.

We will educate employees on this policy per Section 8: Workforce Training Policy.

Several options are available to employees for reporting privacy policy or procedure violations or concerns, including contacting our organization's Compliance Officer, contacting the compliance hotline (Lighthouse), emailing the Compliance Mailbox, submitting an incidence report through our online resource center, or making reports to a workforce member's manager. Violations of the privacy policies or procedures should be immediately reported to one of the methods described above.

B. RESPONDING TO REPORTED COMPLAINTS AND VIOLATIONS

All reports of suspected or known violations of our privacy policies and procedures will be investigated by the Compliance Officer. The identity of reporting individuals is kept confidential to the extent permitted by law, unless doing so would prevent a full and effective investigation. Disciplinary action will be taken in accordance with Section 10 (Sanctions) and HIPAA requirements.

DOCUMENTATION

The Compliance Officer or his/her delegate (Site Lead) is responsible for documenting all complaints related to the compliance with the privacy policies and procedures and/or applicable state or federal law. The Compliance Officer shall keep a record of all complaints and the outcome of the investigation for a period of ten (10) years.

ANTI-RETALIATION

No adverse action or retaliation of any kind shall be taken against a workforce member who reports, in good faith, a suspected violation of our organization's privacy policies or other irregularity. Our organization takes all reports of wrongdoing seriously.

Our organization will not retaliate against any employees, individuals or others for:

- Exercising any right under, or participating in any process established by, federal, state or local law, regulation or policy
- Filing a complaint with our organization and/or the Department of Health and Human Services
- Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing
- Opposing in good faith any act or practice made unlawful by federal, state or local law, regulation or policy, if the manner of the opposition is reasonable and does not itself violate the law

At all times, the Compliance Officer and Site Leads should limit the Protected Health Information (PHI) shared to the minimum necessary to effectively respond to a violation. Our organization will maintain the confidentially of all complaints and protect the identity of all individuals who have made a report to the maximum extent possible, consistent with fair and rigorous enforcement of this Policy in accordance with state and/or federal law and regulations.

SECTION 2. PROCEDURES: REPORTING & RESPONDING TO COMPLAINTS & VIOLATIONS

A. REPORTING COMPLAINTS AND VIOLATIONS

FORMAL REPORTING

Our organization maintains a formal reporting system. Workforce members may report directly 24 hours/7 days a week to:

- (1) a compliance hotline or *Resource Center*
- (2) utilizing Lighthouse, our organization's anonymous reporting hotline: *reports@lighthouse-services.com*

INFORMAL REPORTING

Compliance Officers and Site Leads will also encourage workforce members to report complaints or violations informally. The Compliance Officer and/or Site Leads will communicate during workforce training, whether through training modules or in-person sessions, that all violations must be reported immediately through one of the two formal reporting channels (third-party compliance hotline or Lighthouse) or informally to the workforce member's manager or to the Compliance Mailbox.

1. The site-specific compliance email accounts will be monitored by the Compliance Officer or Site Lead on a daily basis.

B. RESPONDING TO REPORTED COMPLAINTS AND VIOLATIONS

INVESTIGATION

1. Once the Compliance Officer has received notice of a possible security incident or breach, he/she must complete the **Incident Response Form** and document it on the **Privacy Incident Log** within twenty-four (24) hours and notify the Chief Compliance and Privacy Officer.

2. If the Compliance Officer suspects that the reported incident could be a reportable Security Incident or Breach as defined by HIPAA, then complete the HIPAA Breach Risk Assessment Form. The Compliance Officer will immediately (within twenty-four (24) hours):

    - Contact the Chief Compliance and Privacy Officer and Compliance Lead
    - Work with the designated Compliance Leader to begin an investigation into the complaint

3. The Compliance Officer, together with the Integrity Compliance Team will work together to conduct the investigation, and the investigation must be completed within seven (7) calendar days after the Compliance Leader was notified of the incident or breach. During this period, the Compliance Officer and Compliance Leader will:

- Conduct an internal investigation to determine the degree and scope of the incident or breach, including individuals affected, type of PHI disclosed without authorization and any mitigation actions taken
- Interview individuals affected by the incident or breach
- Review documentation related to the incident or breach

4. At the end of the seven (7) calendar days, regardless of whether the investigation is complete, the Compliance Officer must notify the Chief Compliance and Privacy Officer if the investigation results to date show a Security Incident or Breach could have occurred.

5. At this point, the Chief Compliance and Privacy Officer will determine whether:

   - to continue investigating the complaint internally,
   - to bring in outside counsel, or
   - to report the incident to appropriate government agencies (e.g. U.S. Department of Health and Human Services Office for Civil Rights ("OCR"), state attorney generals offices, etc.)

6. If the Chief Compliance and Privacy Officer decides to continue conducting an investigation into the facts and circumstances surrounding the alleged violation, a formal report must be written at the end of the investigation documenting the investigation steps taken and any corrective action needed. A copy of this final report must be provided to the Director of Human Resources and other appropriate management personnel to be stored in the employee's personnel file.

DOCUMENTATION

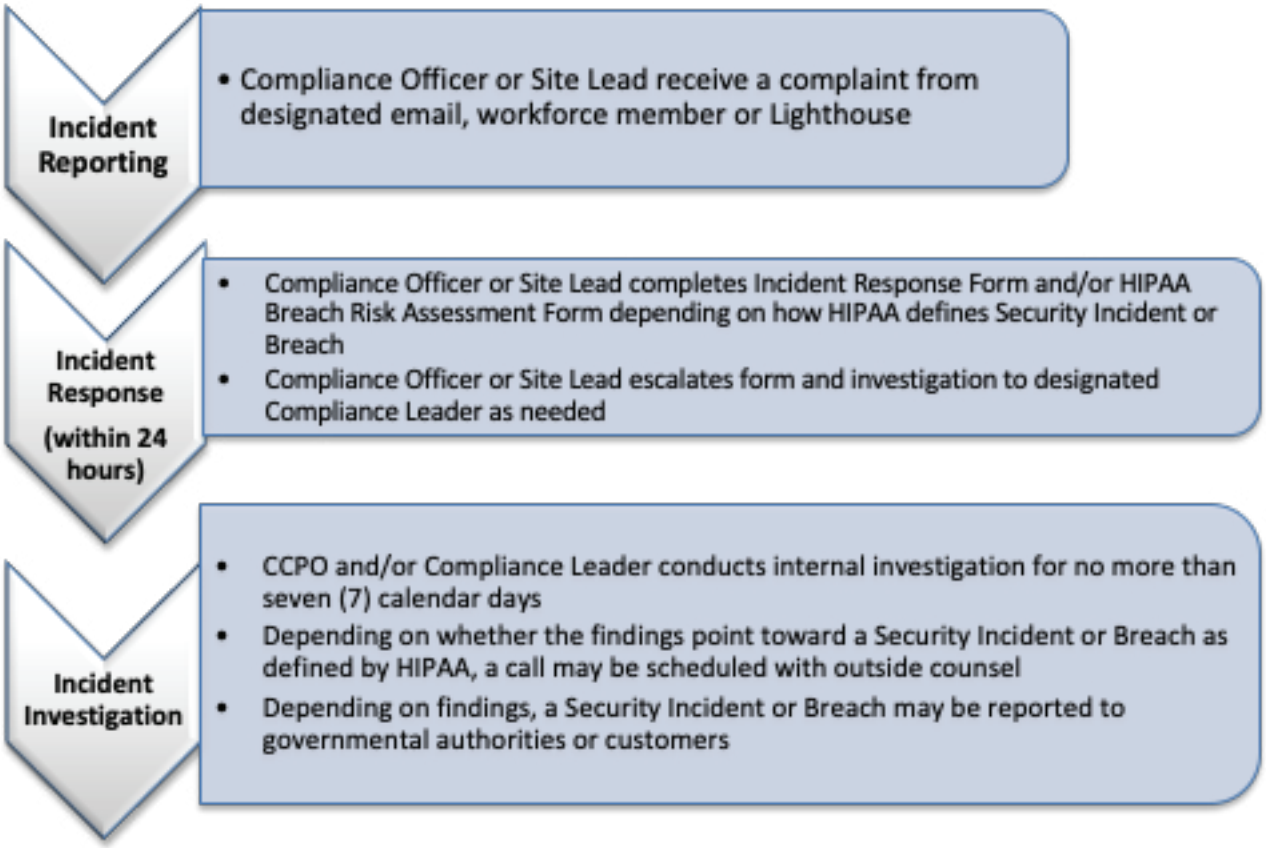
1. The compliance hotline will record all violations and complaints it receives on a log that will be sent electronically to the Compliance Officer.

2. The Compliance Officer or Site Lead will log all privacy incidents and breaches, regardless of degree, scope or further investigation, onto the **Privacy Incident Log.**

ANTI-RETALIATION

1. Any complaints regarding adverse action or retaliation taken against a workforce member due to a report must be sent directly to the Chief Compliance and Privacy Officer. The Chief Compliance and Privacy Officer will investigate the allegation and document all findings.

INCIDENT RESPONSE TIMELINE



C. RESPONDING TO REGULATORY NOTICES AND INVESTIGATIONS

1. **ESCALATION** If [PARTNER] should receive a notice of any real or threatened litigation or arbitration proceedings or any investigation or audit requests from a third party or government agency (excluding Carriers and contracted partners), employees should escalate to their respective Compliance Officer immediately. Compliance Officers will then escalate through the normal chain of communication within the Integrity Compliance Team by notifying their Compliance Leader. They will then work together to ensure it is reported to the CCPO and General Counsel as soon as possible.

   Examples of such notices or requests can include but are not limited to contract disputes, intellectual property rights, employment discrimination, immigration issues, wrongful termination claims, violations of law, Department of Insurance investigations and CMS investigations.

SECTION 3. POLICY: HANDLING CONFIDENTIAL INFORMATION

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

Our organization requires that all members of its workforce, including its employees, consultants, vendors, contractors, etc., who are performing services on our behalf, treat all Confidential Information, including non-PHI data, in a manner that maintains the confidentiality of the information.

All Confidential Information, regardless if it is verbal, electronic or hard copy, must be handled and maintained in a confidential manner, and will be shared applying the Minimum Necessary requirements. For additional reference, please see our organization's Information Security and Data Security Policies.

CLEAN DESK. All workforce members will keep Confidential Information, including passwords and PHI-containing documents, in locked drawers and away from public viewings or access when unattended.

STORAGE/QUESTIONS. In the event the original documents contain PHI or PII, the staff member should consult with our Compliance Officer to determine the appropriate method of storage and/or destruction of records as described below. Storage may also be indicated in the applicable Business Associate Agreement.

SECTION 3. PROCEDURES: HANDLING CONFIDENTIAL INFORMATION

Workforce members are prohibited from sharing Confidential Information, including PHI, beyond what is minimally necessary to perform job duties. All transfers of PHI must be done in accordance with the Business Associate Agreement.

Without a signed Business Associate Agreement with our organization or evidence that the insurance agent maintains a Business Associate Agreement with the insurance carrier or the completion of the HIPAA Personal Representatives Form, client's Protected Health Information, including Social Security numbers, shall not be released to insurance agents through verbal, hard copy or electronic means.

VERBAL COMMUNICATION OF SENSITIVE INFORMATION/PHI

1. If PHI must be communicated verbally for business needs, workforce members should take reasonable measures to ensure that the transaction occurs: (a) in a private space and not in public places; and (b) is spoken at a reasonable volume to minimize disclosures to third parties and limit the information that is heard.
2. If the caller insists that he/she is the patient/customer's HIPAA Personal Representative, then the workforce member will electronically send the caller a **HIPAA Personal Representative Form** for the client to complete.
    a. The HIPAA Personal Representative Form should be sent to our organization's Compliance Email. Upon receipt of the HIPAA Personal Representative Form, the Compliance Officer must review the form within three (3) business days to decide whether to approve the release of the sensitive information to the agent.
3. If a client calls our organization asking for his/her own information, any workforce member must verify the client before providing any sensitive information or PHI regarding the client. The workforce member should ask the caller to confirm three pieces of sensitive information about him/herself: (1) date of birth; (2) home address; and (3) last four digits of his/her Social Security number.
    a. The workforce member should document the disclosure through an email to our Compliance Email with the following information: date of request; identity of caller; caller's contact method and contact information; client information released (date of birth, address, etc.).
    b. The Compliance Officer or Site Lead will log the request in the Incident Log.

HANDLING HARD-COPY SENSITIVE INFORMATION/PHI

1. Unless an exception is approved and documented by the Compliance Officer, all hard-copy sensitive information/PHI, including commission statements, applications and agent information, should be scanned into our organization's system upon arrival and then shredded immediately after scanning or stored in a locked shred bin.
2. If hard-copy sensitive information containing PHI/PII cannot be scanned and stored electronically, it must be stored securely in a locked desk, file cabinet, room, etc., that is

away from public viewing or access. When hard-copy information is no longer required to be stored to meet its intended business purpose, it should be securely disposed of to mitigate the risk of housing it on premise.

3. All documents containing PHI/PII or other sensitive business information, whether electronic or hard copy, should only be stored for the duration or time frame needed to satisfy its business purpose. Please be aware of all regulatory, legal and/or carrier requirements pertaining to duration of document retention and storage (e.g., documents related to the Federal Medicare Program—MA/PDP plan business—need to be stored for a duration of 10 years). Once a document is no longer necessary for its intended business purpose and has met all storage duration time frames, documents should be disposed of securely. Destruction certificates should be completed whenever possible and saved in the shared Compliance Team drive/folder.

4. Hard-copy documents containing the PHI of 500 or more individuals should not be created without the explicit approval of the Chief Compliance and Privacy Officer or his/her delegate. To the extent that an exception is necessary for business purposes and approved by the Compliance Officer, all PHI within workforce members' possession should be maintained in a locked area (desk, cabinet, room, etc.) or stored in a locked shred bin. The Site Lead will maintain a copy of the recycling/destruction vendor's Certification of Destruction to show the document was properly destroyed.

5. Before hard-copy PHI is mailed using U.S. postal mail or another sending source, the workforce member will review the postal address for accuracy and will ensure that any PHI is going to the correct recipient. Also, employees should ensure that any incoming or outgoing mail containing PHI is stored in a secure or private area that is not accessible to the general public and should never be left unattended in a public area of the office building. See Section 4: Physical Security, for differentiation of public and private zones.

ELECTRONIC SENSITIVE INFORMATION/PHI

1. All electronic sensitive information/PHI, including commission statements, applications and agent information, must be stored on an encrypted drive.

   If the Compliance Officer, with guidance from the Compliance Leaders or Chief Compliance and Privacy Officer, determines that a set of information of the PHI of 500 or more individuals is necessary for business purposes, the document must be password protected, and the data must be encrypted at rest and in transit in accordance with industry guidelines (e.g., NIST, ISO, etc.). When the document is no longer in use, the document must be securely destroyed by the IT department in accordance with industry guidelines (e.g., NIST, ISO, etc.).

2. All removable media (USB drives, CD-ROMs, etc.) that contain Confidential Information must be encrypted. All information on removable media should be backed up to a secure server at least monthly at the direction of the IT department. The IT department will maintain an inventory log of all encrypted removable media pieces in use within our environment.

3. All hardware (server, network drives, printers or workstations) containing PHI must be stored in a locked room. Surplus equipment containing PHI will be securely sanitized for reuse or destroyed by a recycling/destruction vendor, and Certificates of Destruction will be provided for all hardware collected by recycling/destruction vendor. The Site Lead will store all Certificates of Destruction in the Egnyte folder.
4. Electronic files such as CD-ROMs must be destroyed as unreadable.

CLEAN DESK

1. All workspaces must be clean of PHI (papers, passwords, etc.) at the end of the workday.
2. The Compliance Officer will conduct a random **Monthly Compliance Review** of all workspaces and provide the report to the Compliance Leader during their touch-base phone calls.
    a. Continued violations of the Monthly Compliance Review are considered a Level 1 Sanction. Please see section 11: Sanctions and Disciplinary Action.

STORAGE/QUESTIONS

1. Questions regarding disposal or storage of all Confidential Information should be directed to the Compliance Officer, who shall discuss the issue with Compliance Leaders, legal counsel, HR staff and/or the Chief Compliance and Privacy Officer.
2. All electronic Confidential Information shall be stored on company servers and databases (not on local computers) and maintained for at least ten (10) years.

SECTION 4. POLICY: MINIMUM NECESSARY; ACCEPTABLE USES OF PHI

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

A. MINIMUM NECESSARY

This policy ensures that our organization's workforce members only use PHI as necessary in order to perform services on our behalf. **This applies to all forms of PHI whether it is oral, written or electronic.** All staff members are also required to abide by our Acceptable Use Policy and Email Use Policy.

In accordance with Minimum Necessary, only the minimum amount of PHI should be used, disclosed or otherwise accessed. Furthermore, only those employees who have a "need to know" should have access to PHI.

B. ACCEPTABLE USES OF PHI

Our organization may contract with a client to provide services, where the arrangement will involve the use, disclosure or maintenance of PHI. Unless restricted under the Business Associate Agreement, company workforce members may use or have access to PHI to perform the following services:

a. To conduct its work with its clients including the evaluation of patient-provider encounters or other information necessary for us to deliver contracted services and provide results to clients

b. For the proper management and administration (e.g., providing information if necessary, for business purposes, such as to legal counsel or to an accounting firm)

c. For data aggregation purposes (e.g., in performing data analytics for population health statistics or reporting performance measures)

d. For de-identification purposes (e.g., PHI would be de-identified before performing data analytics for calculating performance measures)

e. As otherwise permitted under the HIPAA Privacy Rule

SECTION 4. PROCEDURES: MINIMUM NECESSARY; ACCEPTABLE USES OF PHI

A. MINIMUM NECESSARY

1. Access to, use of or disclosure of PHI will be limited to the minimum necessary amount of access to accomplish the specific purpose to select individuals ("Minimum Necessary"). Individuals within our workforce who typically will have access to PHI include, but is not limited to:

    a. Board of directors and senior executives

    b. Finance department

    c. Sales department

    d. Marketing department

    e. Operations department

    f. Licensing department

    g. New business department

    h. Commissions department

2. Minimum Necessary will not apply in the following circumstances:

    a. Uses or Disclosures that are required by law (e.g., in response to a subpoena or other order of a court provided that the disclosure is limited to the PHI that is expressly authorized by such an order).

    b. Uses or Disclosures made to the individual who is subject to this PHI

    c. Uses or Disclosures made pursuant to an individual's authorization

    d. Disclosures to a health care provider for treatment purposes

    e. Disclosures to the Secretary of the Department of Health and Human Services for enforcement purposes

    f. Uses or Disclosures that are required for compliance with HIPAA requirements (e.g., disclosing PHI to a Covered Entity client for purposes of allowing the client to respond to an individual's request for access to PHI).

3. Exceptions to Minimum Necessary may be granted. Individuals whose job responsibilities change and need access to PHI added or retracted shall send an email to their supervisor, who will escalate the request, if warranted, to the Compliance Officer. The Compliance Officer will communicate the request with the Compliance Leader and CCPO, who will approve or deny the request and direct the Compliance Officer to put in a ticket with the IT department.

B. ACCEPTABLE USES OF PHI

1. If our organization is acting under a Business Associate Agreement ("BAA"), the use or disclosure of PHI must be in accordance with that BAA. If an organization workforce member needs to utilize PHI in a manner that is not allowed under the applicable client arrangement or the BAA, the workforce member should contact his/her supervisor, who will escalate the issue up to the Compliance Officer for further instructions and directions.

    a. If an agent requests a client list, the agent must be acting under a BAA as evidenced with an active carrier appointment. The employee should confirm the agent's appointment status on the carrier agent portal.

    b. Transmission of the list must be securely transmitted in an encrypted format; see Encryption Guidelines.

2. If an organization workforce member needs to use or disclose PHI for any other purpose, the workforce member will contact the Compliance Officer before undertaking the task. The Compliance Officer, with the help of his/her Compliance Leader or CCPO, will confirm that such use or disclosure is appropriate.

3. Our workforce members will not use or disclose PHI for any of the purposes listed below without the explicit and written approval of the Compliance Officer.

    a. Marketing: Workforce members will not use or disclose PHI for any marketing purposes.

    b. Fundraising: Workforce members will not use or disclose PHI for any fundraising efforts.

    c. Remuneration and Sale of PHI: Our organization will not receive any remuneration for the use or disclosure of PHI, unless it would be allowed under the Privacy Rule. The Compliance Officer, working with the Chief Compliance and Privacy Officer and legal department, will determine whether any proposed practices comply with federal or state law.

SECTION 5. POLICY: ACCESS, AMENDMENT & ACCOUNTING OF DISCLOSURES

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

Covered Entity clients of our organization are required to provide individuals with access to PHI, an Accounting of certain Disclosures of PHI and to amend PHI under certain circumstances. Our organization will provide access, amendment and Accounting of Disclosures as agreed upon in Business Associate Agreements. When company is providing services to these Covered Entity clients, it shall keep track of certain Disclosures of PHI and be able to provide an Accounting of such Disclosures to the client or directly to the Individual.

This section sets forth our policy in regard to access, amendment of PHI and for Accounting for Disclosures of PHI. For Individuals who reach out directly, our organization will:

- Respond to requests for PHI or amendment of PHI in a manner agreed upon in the applicable Business Associate Agreement
- Upon request from a Covered Entity, provide an Accounting of Disclosures of the following items:
    - Disclosures required by the secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with the Privacy Rules
    - Disclosures made for public health purposes
    - Disclosures to a health oversight agency for purposes of oversight activities authorized by law. For example, Disclosures of PHI to government entities for purposes of audits, investigations, inspections, licensure or disciplinary actions are all subject to the accounting requirement
    - Disclosures made in the course of judicial or administrative proceeding. For example, Disclosures made in response to a court or administrative tribunal order, subpoena or discovery request must be accounted for
    - Disclosures of PHI for law enforcement purposes when not pertaining to a patient in legal custody. For example, Disclosures made to law enforcement officials for purposes of identifying or locating a suspect, fugitive, witness or missing person
    - Disclosures for research purposes made pursuant to an institutional review board or privacy board approval of a waiver of authorization and Disclosures made for purposes of research preparation
    - Disclosures made to prevent or lessen a serious threat or harm to the health or safety of a person or the public
    - Disclosures related to armed services personnel made for activities deemed necessary by military command authorities to assure the proper execution of a military mission
    - Disclosures that are required by law (e.g., Disclosures of PHI in response to a subpoena)

Workforce members will be trained on this procedure during onboarding and annual training. Individuals who fail to comply with this policy will face sanctions, up to and including termination.

Our organization shall document, and maintain a record of, all Accounting of Disclosures for a period of ten (10) years.

SECTION 5. PROCEDURES: ACCESS, AMENDMENT & ACCOUNTING OF DISCLOSURES

A. ACCESS: RESPONDING TO REQUESTS FOR PHI

1. Since our organization is not the system of record to an individual's PHI, workforce members shall direct all requests for PHI to the appropriate Covered Entity client (i.e., carrier) unless otherwise specified in the Business Associate Agreement.

2. If a member of our workforce receives a request for access to PHI from a Covered Entity client (i.e., carrier) or an individual by phone, the workforce member should ask the caller to confirm three pieces of sensitive information about him/herself: (1) date of birth; (2) home address; and (3) last four digits of his/her Social Security number. The workforce member shall record a method to get back in touch with the requester and send the requester an **Access to PHI Request Form** to be filled out by requester. Workforce members shall not provide any carriers with a list of their customers, including PHI (e.g., Social Security numbers). See Section 3 Procedures (Handling Confidential Information).

3. If a workforce member receives the request to access PHI in writing, the workforce member shall notify the Compliance Officer via the local Compliance Mailbox within twenty-four (24) hours of that request with a copy of the request, the details surrounding the request, the result of the phone confirmation if applicable and/or requester's contact details (phone number, address, email, etc.).

4. The Compliance Officer shall review the request and escalate the request to the designated Compliance Leader with a recommendation on next steps (whether to grant the access) within twenty-four (24) hours of receiving the request.

5. The CCPO and Compliance Leader will work with the Compliance Officer to review the appropriate Business Associate Agreement to confirm the access to PHI.

    i. If the request is from an individual, the Compliance Officer will use best efforts to notify the applicable organization's Covered Entity client within five (5) business days of the request or the shorter period required under the applicable Business Associate Agreement.

    ii. If the request is from a Covered Entity client and the Business Associate Agreement does not require a specific time frame, the Compliance Officer will use his/her best efforts to respond to the carrier within fifteen (15) business days.

6. If the request for access of PHI is approved, the Compliance Officer will provide access to PHI in an encrypted format for all electronic PHI.

7. If the request for access of PHI is denied, the Compliance Officer shall document the reason for denial.

B. AMENDMENT: RESPONDING TO AMENDMENT OF PHI

1. Since our organization is not the system of record to an individual's PHI, workforce members shall direct all requests for amendments for PHI to the appropriate Covered Entity client (i.e., carrier) unless otherwise specified in the Business Associate Agreement.

2. If a workforce member receives the request to amend PHI in writing, the workforce member shall notify the Compliance Officer via our organization's Compliance Mailbox within twenty-four (24) hours of that request with a copy of the request, the details surrounding the request, the result of the phone confirmation if applicable and/or requester's contact details (phone number, address, email, etc.).

3. The Compliance Officer shall review the request and escalate the request to the designated Compliance Leader with a recommendation on next steps within twenty-four (24) hours of receiving the request.

4. The Compliance Leader will work with the Compliance Officer to review the appropriate Business Associate Agreement to confirm applicable obligations regarding amendment to PHI including, but not limited to, time frame for response.

    i. If the request is from an individual, the Compliance Officer will use best efforts to notify the applicable Covered Entity client within five (5) business days of the request or the shorter period required under the applicable Business Associate Agreement.

5. If the request is from a Covered Entity client and the Business Associate Agreement does not require a specific time frame to carry out the amendment of PHI, the Compliance Officer will use his/her best efforts to carry out the amendment to PHI in our organization's system, if applicable, within fifteen (15) business days.

C. ACCOUNTING: ACCOUNTING FOR DISCLOSURES

1. All Accounting for Disclosures of PHI will be logged by the Compliance Officer for each site in the Privacy Incident Log on the Accounting of Disclosure tab and reported to the Chief Compliance and Privacy Officer each year to aggregate into one list.

    i. The Disclosures log will contain: (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed (if known); (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for disclosure. For multiple disclosures of information to the same person or entity for a single purpose, the Compliance Officer and/or the Chief Compliance and Privacy Officer may indicate the frequency of disclosure on the entry.

SECTION 6. POLICY: BUSINESS ASSOCIATES; BUSINESS ASSOCIATE AGREEMENTS

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

Our organization shall execute a Business Associate Agreement (BAA) with its Covered Entity clients when company will use, have access to, disclose, create and/or receive PHI from those Covered Entity clients. Our organization will not sign a BAA with a Covered Entity client where our company is not creating, receiving, maintaining or transmitting PHI in order to provide services to the Covered Entity client.

As a Business Associate, we shall also enter into written Business Associate Agreements with its vendors, contractors and consultants to whom company discloses or provides access to PHI that it receives from its Covered Entity clients.

Exceptions to these policies require written approval from our organization's Compliance Officer.

Our organization may Use and disclose PHI only as necessary to provide services to the Covered Entity client and as described in the underlying services agreement; as permitted by the applicable BAA; in compliance with the HIPAA Privacy Rule; and as otherwise required by law. A BAA may not authorize our organization to Use or disclose PHI in a manner that would violate the HIPAA Privacy Rule.

All workforce members shall be trained to report Uses or Disclosures of PHI not authorized by the Business Associate Agreement to our organization's Compliance Mailbox. Workforce members who fail to follow this policy will face sanctions, up to and including termination. See Sanctions and Disciplinary Action Policy.

SECTION 6. PROCEDURES: BUSINESS ASSOCIATES; BUSINESS ASSOCIATE AGREEMENTS

A. STANDARD FORM BUSINESS ASSOCIATE AGREEMENT

1. The Compliance Officer and his/her delegate(s) will develop and revise, as necessary, a standard form Business Associate Agreement to be entered into with each Covered Entity client from which our organization receives, creates or maintains PHI. The form Business Associate Agreement shall contain the required provisions under the HIPAA privacy and security regulations, as well as other protections considered to be prudent, including:

   a. Use and disclose PHI in compliance with the Privacy Rule.

   b. Comply with the Security Rule with respect to ePHI.

   c. Not Use or further disclose the PHI other than as permitted or required by the agreement or as required by law.

   d. Use appropriate Safeguards to prevent Use or Disclosure of the PHI other than as provided for by its agreement.

   e. Report to the client any Use or Disclosure of the PHI not provided for by its agreement and any security incident of which it becomes aware with respect to ePHI.

   f. Ensure that any subcontractor who creates, receives, maintains or transmits PHI on behalf of our organization in its role as a Business Associate for the client, agrees to the same restrictions and conditions that apply to our organization with respect to such information.

   g. Following discovery of a Breach of unsecured PHI, notify the affected client in accordance with the requirements of 45 CFR § 164.410 or the terms of the BAA if the terms of the BAA are more stringent.

   h. Make its internal practices, books and records relating to the Use and Disclosure of PHI received from, or created or received by our organization on behalf of, the client available to the secretary of HHS for purposes of determining the client's compliance with the HIPAA Privacy Rule.

   i. To the extent our organization is carrying out any of the client's obligations under the HIPAA Privacy Rule, comply with the requirements of the Privacy Rule that apply to the client when performing such obligations.

   j. Respond to Individual requests for access to their PHI in accordance with the HIPAA Privacy Rule and the applicable BAA.

   k. Respond to Individual requests for amendment of their PHI in accordance with the HIPAA Privacy Rule and the applicable BAA.

   l. Make available information required to provide an accounting of Disclosures consistent with the requirements of the HIPAA Privacy Rule and the applicable BAA.

m. At termination of the services contract, terminate access to the client's PHI and to the extent our organization has any of the client's PHI, return or destroy all such PHI; or, if such return or destruction is not feasible, extend the protections of the applicable BAA to the information and limit further Uses and Disclosures to those purposes that make the return or destruction infeasible. Our organization does not return data provided, but instead destroys it upon termination or when feasible. Any return of data requires the approval of the Chief Compliance and Privacy Officer.

B. PROCEDURES PRIOR TO SIGNING A COVERED ENTITY BUSINESS ASSOCIATE AGREEMENT

1. Stand-alone Business Associate Agreements with Covered Entity clients (i.e., carriers) shall only be signed after prior review, negotiation and approval by the Compliance Officer. The Chief Compliance and Privacy Officer may use Compliance Leaders, Compliance Officers and legal reviewers as a resource when negotiating terms to ensure that our organization attempts to procure similar terms or protections from its Covered Entity clients.

C. PROCEDURES PRIOR TO SIGNING A VENDOR BUSINESS ASSOCIATE AGREEMENT

1. Our organization requires all vendors who may create, receive, maintain or transmit PHI on behalf of company to complete a **Vendor Security Questionnaire** prior to providing such vendor with PHI or other sensitive information.

2. The Compliance Officer or his/her delegate, with support from the Chief Information Security Officer or his/her delegate, will review the completed Vendor Security Questionnaire to determine if vendor has appropriate physical, administrative and technical safeguards required to serve as our organization's Business Associate as defined by HIPAA.

3. After review of a Vendor's Questionnaire, the Chief Compliance and Privacy Officer and Chief Information Security Officer will make a recommendation as to whether our organization should sign a Business Associate Agreement and contract with the vendor, contract with the vendor with a mandated corrective action plan or not contract with the vendor. The Compliance Officer is responsible for signing all Business Associate Agreements when executed using our organization's BAA form. If the vendor requests to use their Business Associate Agreement, the Compliance Officer should escalate to the Chief Compliance and Privacy Officer and general counsel for review. Once approval is received, the Compliance Officer may then sign the vendor's Business Associate Agreement.

4. In the event a vendor refuses to complete the Vendor Security Questionnaire, the Chief Compliance and Privacy Officer, with support from the Chief Information Security Officer, will make a good faith effort to collect the information needed to complete the vendor survey from publicly available documents (e.g., security white papers). In the event that the Chief Privacy Officer and Chief Information Security Officer cannot substantiate the vendor's security and compliance posture in a manner reasonably consistent with the Vendor Questionnaire, the Chief Privacy Officer and Chief Information Security Officer will recommend against contracting with the vendor.

5. The Chief Compliance and Privacy Officer may accept current industry standard security certifications (e.g., HITRUST or ISO 27001) as an alternative to the Vendor Questionnaire.

D. PROCEDURES TO AUDITING VENDORS AFTER BUSINESS ASSOCIATE AGREEMENT SIGNED

1. The Compliance Officer will periodically audit its relationship with all vendors that maintain, create, transmit or store PHI or other sensitive information. The periodic audit will require the vendor to, at minimum, re-complete the Vendor Questionnaire. In the event the vendor's questionnaire is insufficient for our organization to evaluate vendor's security or contains material deficiencies, the Compliance Officer or his/her delegate may immediately terminate the relationship, engage in additional fact-finding or continue the relationship with mandated corrective actions.

E. DOCUMENTATION

1. Copies of all executed Business Associate Agreements should be kept with the underlying services agreement. The Chief Compliance and Privacy Officer shall have access to all Business Associate Agreements executed by our organization, but the Compliance Officer shall maintain the Business Associate Agreements in the appropriate shared Compliance Team folder.
2. The Chief Compliance and Privacy Officer will be responsible for reviewing Business Associate Agreement templates at least annually to determine whether alterations are necessary to reflect how business is conducted.

SECTION 7. POLICY: DE-IDENTIFICATION & DATA AGGREGATION OF PHI

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

Our organization is committed to ensuring the privacy and confidentiality of PHI. The HIPAA Privacy Rule permits creation of "de-identified" information without an Individual's authorization if such right is authorized in an applicable Business Associate Agreement. The HIPAA Privacy Rule also permits the aggregation of PHI on behalf of Covered Entity clients for health care operations if such right is authorized in an applicable Business Associate Agreement.

If our organization is providing services to a Covered Entity client, our organization must sign a Business Associate Agreement if BAA language is not included within the contract. The Business Associate Agreement between our organization and that Covered Entity client must provide Company with the right to de-identify the PHI and/or the right to aggregate data before our organization engages in such activities.

A. DE-IDENTIFICATION OF PHI

The HIPAA Privacy Regulation permits using PHI to create de-identified information. PHI that has been appropriately de-identified is not subject to the protection requirements of the Privacy Regulation and is no longer considered PHI.

B. DATA AGGREGATION

Under HIPAA, data aggregation does not include aggregating financial records without PHI for our organization's own reporting. To the extent that data aggregation is conducted, the Compliance Officer is responsible to ensure that data aggregation rights are granted in a Business Associate Agreement if a workforce member engages in any work activities that involve combining one client's PHI with that of another client.

SECTION 7. PROCEDURES: DE-IDENTIFICATION & DATA AGGREGATION OF PHI

A. DE-IDENTIFICATION OF PHI

1. To the extent that our organization uses de-identified PHI, the Compliance Officer and the Compliance Leader, with input and feedback from the Chief Compliance and Privacy Officer, will ensure that de-identification rights are explicitly granted in contracts to permit our organization to use PHI to create de-identified information.

2. To the extent that our organization uses de-identified PHI, the Chief Compliance and Privacy Officer shall oversee that the de-identified information must be de-identified in accordance with HIPAA's de-identification methodology as described in Section 6 of our organization's HIPAA Policies and Procedures. This may require the expertise of outside specialists.

3. PHI may be de-identified by one of the two following methods:

    i. The PHI can be de-identified in a manner that a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

        a. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an Individual who is a subject of the information; and

        b. Documents the methods and results of the analysis that justify such determination.

    ii. The PHI can be de-identified according to the *safe harbor method* outlined in the HIPAA Privacy Rule, but only if our organization workforce members confirm that our organization has no actual knowledge that the de-identified PHI could be used to re-identify:

        a. Names or any party of names (e.g., first letter of first name and last name).

        b. All geographic subdivisions smaller than a state (including street address, city, county, precinct, ZIP code and their equivalent geocodes except for the initial three digits of a ZIP code if according to the current publicly available data from the Bureau of the Census).

        c. All elements of dates (except year) for dates directly related to an Individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

        d. Telephone numbers.

        e. Fax numbers.

        f. Electronic mail addresses.

        g. Social Security numbers.

        h. Medical record numbers.

i. Health plan beneficiary numbers.

j. Account numbers.

k. Certificate/license numbers.

l. Vehicle identifiers and serial numbers, including license plate numbers.

m. Device identifiers and serial numbers.

n. Web Universal Resource Locators (URLs).

o. Internet Protocol (IP) address numbers.

p. Biometric identifiers, including finger and voice prints.

q. Full-face photographic images and any comparable images.

r. Any other unique identifying number, characteristic or code.

4. Our organization may assign a code or other means of identification to allow de-identified information to be re-identified by our organization provided that: (1) The code or other means of record identification is not derived from or related to information about the Individual/patient, and is not otherwise capable of being translated so as to identify the Individual; and (2) our organization does not use or disclose the code or other means of record identification for any purpose, and the mechanism for re-identification is not disclosed.

B. DATA AGGREGATION

1. To the extent our organization may aggregate data on behalf of the Covered Entity client, the Compliance Officer and the Compliance Leader, with input and feedback from the Chief Compliance and Privacy Officer, shall ensure that our organization maintains data aggregation rights in and that the aggregated data is only used for the rights given in the contract. Data aggregation process will be modified per client through the Individual Site Plan.

2. To the extent our organization may aggregate data on behalf of the Covered Entity client, the Chief Compliance and Privacy Officer is responsible for ensuring that the data is aggregated in accordance with HIPAA.

SECTION 8. POLICY: BREACH REPORTING REQUIREMENTS

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

The HIPAA Breach Notification Rules related to the Privacy and Security Rules have certain requirements regarding the notification of clients when there has been a breach of unsecured PHI. Our organization must adhere to these rules by either notifying clients or its carriers (i.e., Covered Entities) depending on the contractual obligations if there has been a breach or unauthorized disclosure of unsecured PHI — PHI that has not been encrypted or de-identified.

The Breach reporting requirements apply to: (1) an impermissible Use or Disclosure of PHI; (2) a potential breach involving ePHI; (3) a Breach of unsecured PHI.

If PHI or PII was inappropriately accessed, used or disclosed, workforce members must report the issue immediately through one of the procedures outlined in Reporting Complaints and Violations (Section 2(A) Procedures). All potential breaches should be reported 24/7 to our organization through formal or informal channels, such as the third-party anonymous compliance hotline or directly to the Compliance Officer through the local compliance email box.

A. Examples of Potential Breaches: The following are examples of the types of occurrences that organization workforce members should report as potential breaches:

- Emails including identifying information or being sent to or intercepted by an unintended party
- Sharing systems logon pass codes or leaving them in plain sight
- Faxing identifying information to the wrong fax number
- Staff member's computer is running a strange process
- Someone trying to log in to a staff member's computer
- That a staff member's computer has a virus
- Lost, stolen or missing equipment
- New unauthorized equipment suddenly appears

B. In making his/her determination on whether a Breach has occurred, the Chief Compliance and Privacy Officer will take into consideration the four-factor Breach Notification Test:

1. The type of information inappropriately used or disclosed.
2. The characteristics of the recipient of the information.
3. Whether the PHI was actually acquired or viewed.
4. The ability to mitigate the inappropriate disclosure.

C. Our organization considers an unauthorized access, Use or Disclosure of unsecured PHI as a presumptive breach unless the Compliance Officer and Chief Compliance and Privacy Officer determine that there is a low probability after conducting a risk assessment that the unsecured PHI has been compromised, or

1. The incident was an unintentional acquisition, access or Use of PHI by a workforce member acting under our organization's authority and acted in good faith within the scope of authority and does not result in further Uses or Disclosures not permitted by HIPAA; or

2. The incident was a disclosure of PHI where our organization has a good faith belief that the unauthorized person who received the PHI would not reasonably have been able to retain such information (e.g., a misdirected letter or email containing PHI was returned as undeliverable; PHI retrieved before the unauthorized recipient has an opportunity to view the information).

SECTION 8. PROCEDURES: BREACH REPORTING REQUIREMENTS

A. The following employees in our organization will have a role and responsibility in helping identify PHI/PII events:

1. Compliance Officer.
2. Compliance Site Lead(s) (if applicable).
3. Human Resources representative.
4. Chief Information Security Officer or his/her delegate.
5. Chief Compliance and Privacy Officer or his/her delegate.

B. All suspected or actual PHI/PII privacy or security incidents should be reported to a member of our organization's Compliance Team.

C. After receiving the report of a suspected or actual Breach from the Compliance Officer after at most seven (7) days of investigation since the potential breach was reported, the Chief Compliance and Privacy Officer, with help from the Chief Information Security Officer and/or outside legal or forensics counsel if necessary, will investigate the incident as quickly as reasonably possible and document their findings, using the following factors:

1. Determine whether there has been an unauthorized acquisition access, Use or Disclosure of PHI or other forms of PII.
2. Determine whether the data involved was secured or unsecured PHI/PII.
3. Determine who acquired, accessed, Used or received the affected PHI/PII and to whom the PHI/PII may have been impermissibly Disclosed, if applicable.
4. Identify the number of individuals that may be affected, and the specific elements of the data involved.
5. Determine if steps have been taken (or should have been taken) to mitigate the risk (e.g., requesting a written statement from the person who received the PHI/PII stating that he/she has not, and will not, use or further disclose the PHI/PII, obtaining the return or confirmation of destruction of the PHI/PII).

The Compliance Officer will evaluate any applicable state reporting requirements and any relevant client contractual provisions, including requirements under the Business Associate Agreement regarding mandatory client notification needs and the period required for that notification.

D. Our organization's Compliance Officer and the Chief Compliance and Privacy Officer will conduct a **HIPAA Breach Risk Assessment** to determine whether the reported PHI event qualifies as a Breach of unsecured PHI for which notification requirements may apply within seven (7) business days, including, but not limited to, the following factors:

1. The nature and extent of the data involved, including types of identifiers and the likelihood of re-identification.
2. The unauthorized person(s) who accessed or used the data, or to whom it was disclosed.

3. Whether the data was actually acquired, accessed or used.
4. Whether the data was encrypted or otherwise undecipherable.
5. The extent to which the risk to the data has been mitigated.
6. Other factors that may affect the risk of compromise of the PHI.

E. If the Chief Compliance and Privacy Officer determines that a Breach occurred, the CCPO will report this Breach to Covered Entity clients as per the breach notification clauses in all applicable Business Associate Agreements and contracts.

F. If a law enforcement official states to our organization that a notification, notice or posting otherwise required by law would impede a criminal investigation or cause damage to national security, our organization will comply with the following standards:

1. If the statement is in writing and specifies the time for which a delay is required, the Chief Compliance and Privacy Officer will delay such notification, notice or posting for the time period specified by the law enforcement official; or
2. If the statement is made orally, the Chief Compliance and Privacy Officer will document the statement, including the identity of the official making the statement, and delay the notification, notice or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless the law enforcement official provides a written statement as described above.

G. The Chief Compliance and Privacy Officer may need to make the following notifications:

1. Notifications to the affected carriers (i.e., Covered Entities) when required by contractual agreement upon discovery of a breach. In most cases, the carrier is responsible for notification of the individuals and governing bodies below, unless otherwise stated within the contractual agreement.
2. Notifications to the affected individuals on behalf of the Covered Entity client when required to do so by the contractual agreement.
    i. Time frame: Without unreasonable delay, and no later than sixty (60) days following the discovery of the Breach. Discovered, for the purposes of this policy, is considered the first day the breach is known, or by exercising reasonable diligence, should have been known by our organization.
3. Notifications to HHS (if Breach affects more than 500 individuals) when required to do so by the contractual agreement with the covered entity.
    i. Time: Without unreasonable delay and no later than sixty (60) days following a Breach. If Breach is less than 500 individuals, then notify within 60 days following the end of the calendar year in which the Breach occurred.

4. Notifications to state regulators when required to do so by the contractual agreement with the covered entity.
    i. Time: Without unreasonable delay (depends on state regulation).
5. Notifications to media (if breach affects over 500 individuals) when required to do so by the contractual agreement with the covered entity.
    i. Time: Without unreasonable delay, and no later than sixty (60) days following the discovery of the Breach.
6. Notification to an international body (if PHI/PII is obtained from a source outside the United States) when required to do so by the contractual agreement with the covered entity.
    i. Time: Depends on regulation.

H. In all cases (PHI and PII) our organization's Compliance Officer will log all pertinent information regarding the situation including date and times and people contacted. If electronic information or systems are involved, the Compliance Officer will note what applications or repositories may be affected. As appropriate, the Compliance Officer will record the following details into the **Privacy Incident Log:**

1. The current status of the situation.
2. A summary of the situation.
3. Actions taken related to the situation.
4. Contact information for other involved parties.
5. A list of documents and information gathered during the review of the situation.
6. Next steps to be taken.

SECTION 9. POLICY: WORKFORCE TRAINING

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

Our organization is committed to ensuring that workforce members are aware of all established HIPAA policies and procedures, as well as other applicable compliance-related requirements and regulations. Our organization will provide compliance and HIPAA training to all workforce members, as appropriate and necessary.

All workforce members will receive training upon onboarding and annually thereafter through a learning management system, which will cover topics such as:

- HIPAA Privacy and Security Rule, including:
  - Minimum Necessary requirements for PHI
  - Safeguarding PHI
  - Disclosure or amendment of PHI upon request
  - Retaining PHI
  - Transmitting PHI via email, fax or by mail
  - Business Associate Agreements
- Phishing
- Incident and Breach reporting
- IT policies and procedures
- Acceptable behaviors (i.e., code of conduct)
- CMS training — Medicare General Compliance and Medicare Fraud, Waste and Abuse (for applicable sites handling MA/PDP products)

Depending on a workforce member's job responsibilities and access to PHI, he/she may receive additional specific HIPAA training.

SECTION 9. PROCEDURES: WORKFORCE TRAINING

A. DEVELOPMENT/CONTENT

1. Our organization's Compliance Officer and Site Leads (if applicable), along with Integrity's compliance team, will be responsible for the development of compliance training. The IT department and Human Resources (HR) department may also be involved with respect to HIPAA Privacy and Security training.

B. DELIVERY OF TRAINING

1. Initial Training. All new hires will receive compliance and HIPAA training in the learning management system as part of their orientation within ninety (90) days of hire. This introductory HIPAA training will be provided via learning management system modules that are assigned to each workforce member dependent on their job responsibilities and access to PHI. Introductory Privacy training is mandatory for all workforce members, contractors, volunteers and senior leadership. Failure to complete HIPAA training is grounds for sanctions and disciplinary action.

2. Specific Training. The Compliance Officer will approve all additional specific HIPAA training given to workforce members based upon job responsibilities or changing privacy regulations, including additional conferences, seminars or ad hoc programs. The Compliance Officer, Compliance Leaders and Site Leads will receive specialized HIPAA and leadership training on an annual basis to support the Chief Compliance and Privacy Officer's oversight of the privacy compliance program.

3. Ongoing Training. Education and awareness of our organization's privacy policies and procedures will be incorporated into overall compliance education and will be provided on an ongoing basis. This may include information and articles posted to the intranet, or other ways of communicating privacy standards. The Compliance Officer will oversee these activities. Ongoing training will include, but not be limited to:

    - Security reminders distributed monthly
    - Privacy and security posters posted in common spaces
    - Notification of new threats or risks that may arise (e.g., phishing, ransomware)
    - Information on how to report privacy concerns or risks to managers or the privacy team
    - Compliance awareness activities, such as hardware drives to recycle and securely dispose of old equipment.

4. As-Needed Refresher Training. HIPAA refresher training will be provided to all workforce members on an "as-needed" basis, such as when a workforce member is sanctioned for violating a HIPAA privacy policy or procedure.

5. Targeted Specialized Training. Additional specialized training for targeted high-risk areas, or in response to concerns that have arisen, will be provided by the Compliance Officer in collaboration with the CCPO, Compliance Leaders and Site Leads.

C. TRAINING EVALUATION AND DOCUMENTATION

1. After completing HIPAA training upon onboarding and annually, all workforce members will complete a **Training Attestation** certifying that they have completed the training, the topics covered in the training, and that they understand their obligations to safeguard and protect PHI. The Training Attestation will be documented by the learning management system.
2. The learning management system will maintain documentation of the various training modules/materials provided to workforce members. This includes documentation of targeted specialized training, changes in any training programs, reasons for the training and/or changes, etc.
3. The compliance team will periodically review training content and methodology to evaluate its effectiveness, as well as to establish ongoing training goals. Training content and/or mechanisms will be revised as appropriate with guidance from the Chief Compliance and Privacy Officer on an annual basis.

SECTION 10. POLICY: SANCTIONS & DISCIPLINARY ACTION

Cornerstone Senior Marketing
AN INTEGRITY COMPANY

Issue Date: 4/24/2020
Last Revised: 2/22/2022

Our organization has adopted this Sanctions Policy to comply with HIPAA regulations in order to fulfill its duty to protect the confidentiality and integrity of personal and confidential medical information as required by law. Our organization also has developed appropriate, fair and consistent disciplinary actions for workforce members and agents who fail to follow established policies, procedures and guidelines.

Violation of our organization's policies and procedures shall constitute grounds for disciplinary action up to and including termination, and/or professional discipline as well as possible referral for legal and/or criminal action if required.

Violations include, but are not limited to, the following:

- Unauthorized disclosure of an individual's PHI
- Inappropriate use of, or theft, of a computer from our organization
- Destruction of data or computer equipment
- Moving of protected data to a personal mobile device or laptop
- Tampering or destruction of physical security
- Violation of HIPAA or other federal or state laws that protect an individual's privacy of PHI
- Noncompliance with our organization's policies

REPORTING VIOLATIONS. Any workforce member who believes that a violation has occurred as a result of his/her own actions or through the actions of another workforce member should immediately report the incident to his/her supervisor and the Compliance Officer (especially if the violation involves PHI). The Compliance Officer shall promptly conduct a thorough and confidential investigation.

PENALTIES. Our organization may terminate a workforce member's employment if a violation is egregious, exhibits willful misconduct or gross negligence, or constitutes an intentional act that seriously violates the privacy policies and procedures. For less serious violations, management may respond with a verbal or written warning or reprimand, mandatory training, or may recommend suspension without pay, demotion or other sanctions commensurate with the violation.

SECTION 10. PROCEDURES: SANCTIONS & DISCIPLINARY ACTION

1. After the Compliance Officer conducts a thorough investigation of the violation and reviews all applicable facts and circumstances, Human Resources will recommend a sanction from the following two levels for the violation:

   a. Level 1 Sanctions.

      i. Description. Infractions that unintentionally or mistakenly violate our organization's privacy policies and procedures, but do not otherwise involve law enforcement or violation of federal/state laws (e.g., leaving PHI on desk at end of the day, not completing annual privacy training).

      ii. Possible penalties. (Sanctions can include one or all of the items on this list.)

         - Verbal reprimand.
         - Written reprimand.
         - Repeat or additional HIPAA Privacy and Security Training.
         - Discussion with Compliance Officer regarding violation.
         - Record of incident and written warning in workforce member's Human Resources file.

   b. Level 2 Sanctions.

      i. Description. Infractions that are egregious, exhibit willful misconduct or gross negligence, or constitute an intentional act that seriously violates the privacy policies and procedures. These infractions may require notification to clients, vendors, and state or federal law enforcement based on contractual or legal requirements (e.g., stealing company devices or laptops with PHI; selling PHI information to third parties).

      ii. Possible penalties. (Sanctions can include one or all of the items on this list.)

         - Any Level 1 Sanction penalties.
         - Dock in salary.
         - Reporting of behavior to appropriate outside third-party agency/regulatory body (e.g., licensing board).
         - Termination of systems access privilege.
         - Suspension without pay.
         - Termination.

2. **NON-RETALIATION.** Our organization will not retaliate or mandate sanctions against any individual who reports an incident or suspected behavior in good faith. Our organization encourages all workforce members to report any suspected incidents or potential wrongdoings that violate the HIPAA privacy policies and procedures.

3. **APPROVAL AND APPEALS.** The Compliance Officer is responsible for approving Human Resource's recommended sanction for the violation. If the sanction is approved by the Compliance Officer, but the workforce member believes that he/she was wrongly sanctioned, the workforce member may appeal the decision within 10 (ten) days to the Chief Compliance and Privacy Officer, for further consideration. The CCPO may choose to uphold the sanction given; to vacate the sanction given; or to apply a new sanction. The CCPO's decision is final and is not appealable.