Insight Global

HIPAA
Privacy and Security
Policy and Procedures Manual

September 8, 2014

HIPAA Privacy and Security Overview

Insight Global provides an array of services to meet their clients' staffing needs including providing temporary, temporary-to-hire, and direct placement services. Some of these clients are "Covered Entities" or "Business Associates" under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively, "HIPAA"). When these Covered Entity or Business Associate customers use Insight Global's temporary or temporary-to-hire staffers and these staffers have access to Protected Health Information ("PHI"), Insight Global becomes a "Business Associate" under HIPAA. In its capacity as a Business Associate, Insight Global and its Workforce Members must comply with HIPAA as set forth in this HIPAA Privacy and Security Policy and Procedures Manual ("Manual"). All capitalized terms are defined below in the "Definitions" section.

Services Provided

As a staffing provider currently focused on information technology ("IT") staffing, Insight Global provides its clients with IT professionals to meet their short or long term needs. To perform their job functions and support the client, these IT professionals may have access to the client's PHI and, when appropriate, will store this PHI on their Insight Global provided laptops. Insight Global does not, however, have access to this PHI as it is not stored on the Insight Global servers. The PHI remains in the client's information system and on the client's servers. Because the Covered Entity or Business Associate client retains ultimate control over the data that it provides to Insight Global Workforce Members, Insight Global expects that the customer will be HIPAA compliant.

Given that each Covered Entity or Business Associate client will itself have to be HIPAA compliant, the client maintains control over access to the information provided to Insight Global Workforce Members and any PHI provided to Insight Global Workforce Members is only accessible through the Workforce Member's Insight Global-provided laptops, this Manual focuses on the steps that Insight Global and its Workforce Members will take protect PHI that is stored on or accessible through Insight Global-provided hardware.

HIPAA Privacy Regulations

The *Standards for Privacy of Individually Identifiable Health Information*, found at 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E (the "HIPAA Privacy Regulations"), provide rules regarding the use and disclosure of PHI, and other rules regarding an individual's rights to access PHI about himself contained in certain records. Because it provides IT services to Covered Entities and Business Associates, and as a result may be provided with access to PHI in connection with those services, Insight Global and its Workforce Members are required by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") to follow many of the same requirements of the HIPAA Privacy Regulations that apply to

Covered Entities. Insight Global's Privacy Officer will oversee Insight Global's efforts to comply with the HIPAA Privacy Regulations and its efforts to protect the privacy of all PHI that Insight Global creates, transmits, maintains, and/or accesses on behalf of Covered Entities. Insight Global will consistently monitor and periodically audit its Privacy practices to ensure compliance with the Privacy Policies and Procedures.

HIPAA Security Regulations

Under the *Security Standards for the Protection of Electronic Protected Health Information,* found at 45 C.F.R. Part 164, Subpart C (the "HIPAA Security Regulations"), Covered Entities and Business Associates are required to implement administrative, physical, and technical safeguards that ensure the confidentiality, integrity, and availability of electronic PHI ("ePHI"). These safeguards are designed to:

1. Ensure the confidentiality, integrity, and availability of all ePHI it 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 by the HIPAA Privacy Regulations and
4. Ensure compliance with the HIPAA Security Regulations by its workforce.

The Security Policies and Procedures in this manual address Insight Global's obligations under the HIPAA Security Regulations. In designing these policies and procedures, Insight Global has considered:

1. Insight Global's size, complexity, and capabilities;
2. Insight Global's technical infrastructure, hardware, and software security capabilities;
3. The costs of security measures; and
4. The probability and criticality of potential risks to ePHI.

As part of its compliance with the HIPAA Security Regulations, Insight Global has installed a Security Officer who will oversee Insight Global's efforts to create and maintain appropriate and reasonable policies, procedures, and controls to protect the security of ePHI that Insight Global creates, receives, maintains, or transmits and Workstations that Insight Global provides to its Workforce Members.

Education and Compliance with the HIPAA Privacy and Security Policies and Procedures

Insight Global will provide training for all Workforce Members who are reasonably expected to come in contact with PHI regarding the Privacy and Security Policies and Procedures included in this manual. All such Workforce Members are required to certify in writing, by signing the Workforce Member Compliance Statement included in this manual, that they have received, read, received training on, understand and agree to follow the applicable policies in this manual and all applicable provisions of HIPAA and the HITECH Act. Also, as part of their compliance with these Policies and Procedures, such Workforce Members must certify that they will protect the confidentiality of PHI, including ePHI, and that they will report any unauthorized disclosures of PHI, ePHI or other Security Incidents to the appropriate Insight Global personnel, as specified in this manual. To the extent that any Client requests certification of related matters to conform to the Client's HIPAA practices, those certifications shall be in addition to those required by these Policies and Procedures. The Privacy Officer will maintain a record on each Covered Workforce Member that includes his or her signed Workforce Member Compliance Statement. Any violations of these Policies and Procedures on the part of any Covered Workforce Member may lead to the imposition of sanctions, including termination.

Policy and Procedure Documentation and Revision

Insight Global will continue to review, and as necessary, revise and update these Policies and Procedures to comply with HIPAA; to incorporate new technologies that protect the confidentiality, integrity and availability of ePHI; and to address any threats to the privacy or security of PHI that Insight Global may encounter in the future. Insight Global will make these HIPAA Policies and Procedures easily accessible to all Workforce Members. Also, Insight Global will document any revisions made to these Policies and Procedures and will notify its workforce of such changes. Documentation recording any changes or modifications to these Policies and Procedures will be maintained for at least 6 years.

TABLE OF CONTENTS

POLICY/PROCEDURE		RESPONSIBILITY
16.	Malicious Software	Security Officer
17.	Password Management	Security Officer; Workforce Members
18.	Contingency Plan	Security Officer; Other Insight Global Officials as deemed necessary
19.	Data Backup Plan	Security Officer
20.	Disaster Recovery Plan	Security Officer
21.	Emergency Mode Operations Plan	Security Officer
22.	Applications and Data Criticality Analysis	Security Officer
Physical Safeguards		
23.	Facility Access and Security	Security Officer
24.	Workstation Use and Security	Security Officer; Workforce Members
25.	Device and Media Controls	Security Officer; Workforce Members
Technical Safeguards		
26.	Technical Access Controls	Security Officer; Workforce Members
27.	Integrity	Security Officer
28.	Person or Entity Authentication	Security Officer
29.	Transmission Security	Security Officer; Workforce Members
30.	Availability	Security Officer

DEFINED TERMS

Addressable: As currently described in 45 C.F.R. § 164.306, Addressable refers to implementation specifications contained within certain HIPAA Regulations which Insight Global is not required to implement. Insight Global must perform an assessment to determine whether the addressable implementation specification is a reasonable and appropriate safeguard for implementation in its efforts to protect unauthorized use, disclosure, and access of PHI or ePHI. If it is not reasonable and appropriate, Insight Global must document the reasons supporting this conclusion.

Administrative Safeguards: As currently defined in 45 C.F.R. § 164.304, Administrative Safeguards are actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of Insight Global's Workforce Members in relation to the protection of ePHI.

Breach: As currently defined in 45 C.F.R. § 164.402, Breach means the means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Regulations which compromises the security or privacy of PHI, except in the case of (1) any unintentional acquisition, access, or use of PHI, made in good faith and in the scope of the professional relationship, by a Workforce Member or individual acting under the authority of Insight Global or a Covered Entity and the PHI is not further used, acquired, or disclosed; (2) any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by Insight Global or a Covered Entity to another similarly situated individual at the same facility and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person; or (3) a disclosure of PHI where Insight Global has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate: As currently defined in 45 C.F.R. 160.103, a Business Associate is a person or entity who, on behalf of a Covered Entity or another Business Associate, creates, receives, maintains, or transmits PHI for a function or activity under the Privacy Rule, or who performs or assists in the performance of a function or activity involving the use or disclosure of PHI, including, but not limited to, claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; or practice management.

Business Associate Agreement: A contract or other arrangement between a Covered Entity and Business Associate or a Business Associate and a Subcontractor that meets the requirements of 45 C.F.R. § 164.504(e).

Client: For purposes of this Manual, a Client is a Covered Entity or Business Associate that purchases staffing services from Insight Global, which require Workforce Members to have

access to the Client's PHI.

Contingency Event: A Contingency Event is an unplanned for event, such as an emergency or disaster, which may require the activation of Insight Global's Contingency Plan, Data Back-Up Plan, Disaster Recovery Plan, or Emergency Operations Plan.

Covered Entity: As currently defined in 45 C.F.R. 160.103, a Covered Entity is (i) a health plan, (ii) a health care clearinghouse, or (iii) a health care provider who transmits any health information in any form, including in electronic form.

Covered Workforce Member: A Covered Workforce Member is a Workforce Member who is reasonably expected to have access to PHI or who will supervise those Workforce Members who are reasonably expected to have access to PHI.

Designated Record Set: As currently defined in 45 C.F.R. § 164.501, a Designated Record Set means a group of records maintained by or for a Covered Entity that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the Covered Entity to make decisions about individuals. For purposes of this definition, the term record means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.

Electronic Media: As currently defined in 45 C.F.R. § 160.103, Electronic Media means (1) electronic storage media on which data is or may be recorded electronically, including, for example, hard drives, removable storage devices or memory cards; and (2) transmission media used to exchange information already in electronic storage media, including, for example, the internet, an extranet or intranet, or transmission lines, and the physical movement of removable electronic storage media.

Electronic Protected Health Information or ePHI: As currently defined in 45 C.F.R. § 160.103, Electronic PHI means PHI which is either transmitted by electronic media or maintained in electronic media.

HIPAA Breach Notification Rule: The HIPAA Breach Notification Rule is the section of HIPAA at 45 C.F.R. § 164.400 et seq. that contains requirements for reporting, investigating, and making notifications of Breaches of PHI.

Physical Safeguards: As currently defined in 45 C.F.R. § 164.304, Physical Safeguards are physical measures, policies, and procedures to protect Insight Global's Workstations and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy Officer: As currently described in 45 C.F.R. § 164.530(a), Privacy Officer means the

designated employee of Insight Global who is responsible for the development and implementation of the Privacy Policies and Procedures, as required by the HIPAA Privacy Regulations.

Protected Health Information or PHI: As currently defined in 45 C.F.R. § 160.103, PHI means health information that is individually identifiable.

Required: As currently described in 45 C.F.R. § 164.306, Required refers to implementation specifications contained within certain HIPAA regulations with which Insight Global must comply.

Risk Analysis: As currently described in 45 C.F.R. § 164.308(a)(ii)(A), Risk Analysis means the process by which Insight Global will conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI accessed by Workforce Members.

Risk Management Plan: As currently described in 45 C.F.R. § 164.308(a)(ii)(B), Risk Management Plan means the plan to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable level to ensure the confidentiality and integrity of ePHI and to protect against reasonably anticipated threats, hazards, or uses and disclosures that are not permitted or required by the HIPAA Privacy Regulations.

Secretary: As currently defined in 45 C.F.R. § 160.103, Secretary means Secretary of the Department of Health and Human Services (HHS) or any other officer or employee of HHS to whom the authority involved has been delegated.

Security Incident: As currently defined in 45 C.F.R. § 164.304, Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in ePHI systems.

Security Officer: As currently described in 45 C.F.R. § 164.308(a)(2), Security Officer means the designated employee of Insight Global who is responsible for the development and implementation of the Policies and Procedures required by the HIPAA Security Regulations.

Subcontractor: As currently defined in 45 C.F.R. § 160.103, Subcontractor means a person to whom Insight Global, as a Business Associate of a Covered Entity, delegates a function, activity, or service, other than in the capacity of a Workforce Member.

Technical Safeguards: As currently defined in 45 C.F.R. § 164.304, Technical Safeguards means the technology and the policy and procedures that Insight Global has to protect ePHI and control access to it.

Workforce Member: All persons who are under the direct control of Insight Global, including, but not limited to, employees, volunteers, trainees, interns, and temporary

personnel, regardless of whether they are paid by Insight Global.

Workstation: As currently defined in 45 C.F.R. § 164.304, 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. As used in these Policies and Procedures, Workstations generally refer to Workstations provided to Covered Workforce Members by Insight Global. To the extent that Workstations are provided to Covered Workforce Members by a Client, the Client shall be responsible for ensuring that such Workstations are configured and used in accordance with Client's HIPAA policies and procedures.

General HIPAA Policies and Procedures

Insight Global	General HIPAA Policies	Procedure No.: **1**
Title: **Workforce Member Confidentiality and Compliance Statement**	Revision:	Effective Date:

Purpose Statement

All Covered Workforce Members are required to certify in writing, by signing the Workforce Member Compliance and Confidentiality Statement provided below, that they have received, read, received training on, understand and agree to follow the applicable policies in this manual and all applicable provisions of HIPAA and the HITECH Act. Also, as part of their compliance with these Policies and Procedures, Covered Workforce Members must certify that they will protect the confidentiality of PHI, including ePHI, and that they will report any unauthorized disclosures of PHI or ePHI and other Security Incidents to their respective Account Manager, Privacy Officer or Security Officer, as specified in this manual.

Policy/Procedure

1. All Covered Workforce Members will sign the Workforce Member Compliance and Confidentiality Statement provided below prior to being given access to PHI or ePHI and annually thereafter.
2. The Privacy Officer will maintain a record on each Covered Workforce Member that includes the original, signed Workforce Member Compliance and Confidentiality Statements.
3. The Privacy Officer will return a copy of the signed Workforce Member Compliance and Confidentiality Statements to the Covered Workforce Member.
4. Any Covered Workforce Member that refuses to sign the Workforce Member Compliance and Confidentiality Statement will be sanctioned in accordance with the Workforce Member Discipline Policy.

HIPAA Workforce Member Compliance and Confidentiality Statement

I, _____, acknowledge that I have received, read, received training on, understand and agree to follow the Insight Global HIPAA Privacy and Security Policies and Procedures. Also, I acknowledge that during the course of performing my assigned duties at Insight Global, I may have access to, use, or disclose Protected Health Information (PHI) or electronic PHI (ePHI). I agree to handle such information in a confidential manner at all times during and after my employment and commit to the following obligations:

1. I will use and disclose PHI, including ePHI, only in connection with and for the purpose of performing my assigned job functions.
2. I will request, obtain, or communicate PHI, including ePHI, only as necessary to perform

my assigned job functions and will refrain from requesting, obtaining or communicating more PHI, including ePHI, than is necessary to accomplish such functions.

3. I will take reasonable care to properly secure PHI, including ePHI, on my Workstation and will take steps to ensure that others cannot view or access such information.
4. I will use and disclose PHI, including ePHI, solely in accordance with the applicable federal and state laws and regulations and all Insight Global HIPAA Privacy and Security Policies and Procedures. I also agree, in a timely manner, to familiarize myself with any periodic updates or changes to these policies that are communicated to me.
5. I will immediately report any unauthorized use or disclosure of PHI, including ePHI, that I become aware of to the appropriate Insight Global Official.
6. I understand and agree that my failure to fulfill any of the obligations set forth in this Statement and any failure to comply with Insight Global's HIPAA Privacy and Security Policies and Procedures will result in my being subject to appropriate disciplinary action, up to and including, the termination of my employment.
7. I will comply with each of the technical safeguards outlined on Exhibit A to this certification with respect to the use of any equipment that is provided to me by Insight Global or the Client and my access, use, or transmission of PHI, including ePHI.

_____

Workforce Member's Signature

_____

Workforce Member's Printed Name

_____

Date

Responsibility: Privacy Officer; Workforce Members
Regulatory Category: Privacy Regulations; Security Regulations

EXHIBIT A
TECHNICAL SAFEGUARDS TO BE FOLLOWED BY COVERED WORKFORCE MEMBERS

1. WORKSTATION USE AND SECURITY

a. Insight Global's Workstations may only be used for business purposes.

b. The same permissible and prohibited uses of Workstations apply to all Workstations regardless of their location.

c. Each Covered Workforce Members will locate his/her Workstation in physically secure areas and will physically position their Workstations in ways that minimize unauthorized viewing of ePHI. A Covered Workforce Member must not locate his/her Workstations in any of the following locations: public walkway, hallways, waiting areas or any other area where unauthorized viewing of ePHI may occur.

d. Each Covered Workforce Member will be required to use a unique user identifier and passwords to gain access to his/her Workstation.

e. A Covered Workforce Member must activate Workstation locking software upon leaving a Workstation for more than ten (10) minutes.

f. A Covered Workforce Member must log off from his/her Workstation when their work-day shift is complete.

g. A Covered Workforce Member must physically secure a portable Workstation at all times when not in the Workforce Member's immediate possession.

2. PASSWORDS

a. Once a Workforce Member receives his or her temporary password to access an Insight Global Workstation, the Workforce Member will select and secure a new password.

b. In addition, Covered Workforce Members must re-set their passwords at least every 60 days.

c. To maintain accountability, each Covered Workforce Member will keep his/her passwords confidential and will not share his/her password with anyone. If the confidentiality of a password is compromised, the Covered Workforce Member must immediately change his/her password.

d. Passwords must be 7-16 characters in length, including at least one numeric and other character (e.g. #, $, or &).

e. The same password cannot be reused.

f. Passwords cannot include a Workforce Member's name.

g. Passwords must be committed to memory or, if stored in written, tangible format, in a place to which only the Covered Workforce Member has access.

3. *Malware*

a. A Covered Workforce Member must not bypass or disable anti-virus software installed on his/her Workstation unless he/she is properly authorized to do so.

b. Each Covered Workforce Member must scan email attachments and downloads before they are opened.

c. Each Covered Workforce Member must immediately report suspected or confirmed malicious software to the Insight Global Security Officer.

4. *Encryption*

A Covered Workforce Members must take all necessary steps to encrypt email through the encryption software pre-loaded on any Workstation provided to a Covered Workforce Member. In the alternative, a Covered Workforce Member may encrypt email using the Client's systems if the email is transmitted through the Client's system and the Client's system is known to have appropriate substitute encryption.

5. *Data Back-Ups*

To the extent that a Covered Workforce Member stores ePHI on a Workstation, this ePHI must be an exact copy of the ePHI maintained by the Client such that the ePHI on the Workstation is a redundant duplicate of the ePHI maintained by the Client but not the Client's sole back-up of such ePHI. If the Covered Workforce Member needs to retrieve a back-up of the ePHI maintained on his/her Workstation, he/she will retrieve such a copy from the Client's systems.

6. *Destruction of PHI*

A Covered Workforce Member must not destroy ePHI without first providing notice to and receiving authorization from the Security Officer or the Client if the ePHI to be destroyed is within the Client's information system.

7. *Report of Theft or Loss*

Each Covered Workforce Member must immediately report to the Security Officer the loss or theft of any Workstation or device, such as a facility access card or identification badge, that allows them physical access to an Insight Global facility and/or to areas where ePHI is contained or Workstations that can access ePHI are located.

Insight Global	General HIPAA Policies	Procedure No.: **2**
Title: **Workforce Member Discipline**	Revision:	Effective Date:

Purpose Statement

Insight Global will apply sanctions against Workforce Members, as appropriate, for violations of these HIPAA Privacy and Security Policies and Procedures.

Policy/Procedure

Minor Occurrences

If the Privacy Officer or Security Officer determines that a Workforce Member's acts or omissions resulted in a relatively minor violation of these HIPAA Privacy and Security Policies and Procedures and no significant violation of any law or regulation, the respective Officer will determine whether or not further education, clarification, or other corrective actions are needed.

Significant Violations

If the Privacy Officer or Security Officer determines that a Workforce Member's acts or omissions resulted in a significant violation of these HIPAA Privacy and Security Policies and Procedures or a violation of any law or regulation, the respective Officer will report the findings to the applicable Account Manager and the General Counsel. The applicable Account Manager and General Counsel will determine the scope of any disciplinary steps to be taken.

Disciplinary Action

Disciplinary action should be imposed commensurate with the seriousness of the security or privacy violation. Discipline may take one or more forms, including, but not limited to:

a. Oral counseling and admonishment
b. Written reprimand
c. Requiring the Workforce Member to attend training
d. Reassignment
e. Demotion and/or reduction in pay
f. Suspension without pay
g. Termination of employment

Responsibility: Privacy Officer; Security Officer; Account Manager; Legal
Regulatory Category: Privacy Regulations

Regulatory Reference: 45 C.F.R. §164.308(a)(1)(ii)(C), Sanction Policy [Implementation Specification; Required]

HITECH Act Language

"A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."

"For purposes of this section, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred."

"Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b))."

HIPAA Breach Notification Rule Language

"Except as set forth in the definition of "Breach" (see Definitions), an acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(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; and
(iv) The extent to which the risk to the protected health information has been mitigated."

HIPAA Security Rule Language

"Implement policies and procedures to address security incidents."

Purpose Statement

In the unlikely event that Insight Global experiences a Breach, it will take all reasonable and appropriate steps to protect the confidentiality, integrity, and availability of PHI. Insight Global will promptly identify, report, track, and respond to all potential Security Incidents and Breaches. Awareness of, response to, and creation of reports about Security Incidents and Breaches are integral parts of Insight Global's efforts to comply with the HIPAA Regulations.

Policy/Procedure

Security Incidents

1. A "Security Incident" is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations.
2. The following incidents are examples of potential Security Incidents. The list is not exclusive. The Security Officer will determine when a Security Incident has occurred.
    a. Stolen or otherwise inappropriately obtained passwords that are used to access Workstations that contain ePHI;
    b. Virus attacks that interfere with the operations of Insight Global's Workstations;
    c. Physical break-ins to Insight Global's facilities which may lead to the theft of electronic media containing ePHI; and/or
    d. Allowing electronic media containing ePHI, such as a computer hard drive or laptop, to be accessed by any person who is not authorized to access such ePHI prior to removing the ePHI stored on the media.

Breaches

1. For the purposes of the HIPAA Breach Notification Rule, "Breaches" only involve PHI that is "unsecured." "Unsecured" PHI is PHI which is not secured through a technology or methodology that the Department of Health and Human Services (HHS) has stated renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.
2. According to guidance issued by HHS in August 2009 (the most recent guidance issued by HHS at the time of this Policy), PHI is secured through encryption (for ePHI) or destruction (for PHI in all other formats).
3. Insight Global will take all measures necessary to secure PHI in accordance with the Device and Media Controls and Technical Access Controls Policies (Procedure Nos. 25 & 26) included in this manual.

4. A Breach is defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information. The following occurrences are not Breaches that must be reported under the HITECH Act and implementing HIPAA Regulations:

    a. Any unintentional acquisition, access, or use of PHI by a Workforce Member or individual acting under the authority of Insight Global or the Covered Entity if:

        i. Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such Workforce Member or individual, respectively, with Insight Global; and

        ii. Such information is not further acquired, accessed, used, or disclosed by any person.

    b. Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by Insight Global or the Covered Entity to another similarly situated individual at the same facility and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

    c. A disclosure of PHI where the Workforce Member or individual acting on behalf of Insight Global or Covered Entity has a good faith belief that an unauthorized person receiving the PHI was made would not reasonably have been able to retain such information.

DISCOVERY AND REPORTING OF SECURITY INCIDENTS OR BREACHES

1. Any Workforce Member, including Insight Global management, who discovers a suspected Security Incident, Breach or any other potential threat to the confidentiality, integrity or availability of ePHI, must immediately report the threat to the applicable Account Manager or the Privacy or Security Officer. If the Account Manager receives the report, the Account Manager will forward the report to the Privacy or Security Officer.
2. The Workforce Member may provide notice of the potential Security Incident, Breach, or other threat in any format, including in writing, electronically, or orally.
3. The Privacy or Security Officer will document the report of a potential Security Incident, Breach, or other threat along with the date and time that he or she was notified of such event.
4. Insight Global will not take any retaliatory measures against an individual who reports a potential Security Incident, Breach, or threat.

RESPONSE TO SECURITY INCIDENT OR BREACH AND NOTICE TO COVERED ENTITIES

1. The Privacy Officer and the Security Officer will work together to respond to a potential Security Incident or Breach as follows:

    a. The Privacy Officer will immediately notify Insight Global senior management and

legal counsel upon becoming aware of a potential or suspected Security Incident or Breach.

b. Legal counsel will review the applicable Business Associate Agreement to determine whether and how the potential Security Incident or Breach should be reported to the applicable Covered Entities(s). Legal counsel will also determine whether any additional notifications are required pursuant to applicable breach notification laws.

c. If the incident is identified as a potential Breach:

   1. In consultation with legal counsel and Insight Global senior management, the Privacy and Security Officers will conduct a "risk assessment" of a suspected Breach or Security Incident to determine whether there is more than a low probability that the information was compromised. In this risk assessment, the Security Officer and the Privacy Officer will evaluate the following factors:

      i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

      ii. The unauthorized person who used the PHI or to whom the disclosure was made;

      iii. Whether the PHI was actually acquired or viewed; and

      iv. The extent to which the risk to the PHI has been mitigated.

   2. Insight Global will use all appropriate measures to conduct and complete its review of the suspected Breach within a reasonable time after discovery, but in no case later than 5 business days after discovery. Insight Global will record and maintain documentation of its decision and any justification for that decision, including the analysis of the four factors listed above.

d. If the incident is identified as a Security Incident but not a Breach, the Privacy and Security Officers will investigate the incident to determine the cause, the information involved in the incident, and take appropriate steps to mitigate any harm arising from the incident. Insight Global will use all appropriate measures to conduct and complete its review of the suspected Security Incident within a reasonable time after discovery, but in no case later than 5 business days after discovery.

e. The Privacy and Security Officers will present their initial findings to Insight Global senior management within 24 hours of completing their initial investigation and will update those findings as more information becomes available and at the conclusion of the "risk assessment" or investigation.

f. If the Privacy and Security Officers determine that no Security Incident or Breach has occurred, the Privacy and Security Officers will document this along with all of the information that supports such conclusion and no further investigations or procedures are required.

g. If the Privacy and Security Officers determine that a Breach or Security Incident has occurred, he or she will convene a workgroup, in accordance with the Security Risk

Management Policy, to review the Privacy and Security Officer's initial report to Insight Global senior management and the risk assessment and develop a risk management plan that sufficiently responds to the Security Incident or Breach.

i. The workgroup must analyze the Security Incident or Breach and deliver its response and recommendations to Insight Global senior management within a reasonable time after being convened, but no longer than three (3) business days after the date that the Privacy and Security Officers initially convene the workgroup, unless such time period is extended by the Privacy or Security Officer.

ii. The workgroup's response and recommendations must address the cause of the Security Incident or Breach, mechanisms for mitigating the harmful effects of the Security Incident or Breach, and ways to remediate the vulnerability that lead to the Security Incident or Breach.

h. The Privacy Officer will retain all documentation regarding the Security Incident or Breach in accordance with the Insight Global Documentation Retention Policy.

CONTENTS OF NOTICE

1. Pursuant to its Business Associate Agreements with Clients, Insight Global must notify the Client of a successful Security Incident or a Breach. When Insight Global notifies the Client of a Breach, it must provide the identity of any individual whose information was affected or is believed to be affected by the Breach and any information the Covered Entity is required to provide in its notice to individuals, as described below.
2. Each Breach notification will include, to the extent possible, the following information:
   a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.
   b. If known, a description of the types of unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
   c. If known, the steps affected individuals should take to protect themselves from potential harm resulting from the Breach.
   d. A brief description of what Insight Global is doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches.

METHODS OF NOTICE

As a Business Associate, Insight Global is not responsible for providing notice to the Secretary, affected individuals, or the media pursuant to 45 C.F.R. §§ 164.404, 164.406, and 164.408 unless the Covered Entity delegates such responsibility to Insight Global in the Business Associate Agreement. If that duty is so delegated, Insight Global will follow the following notice procedures:

1. Notice to the Secretary

a. Insight Global will provide written notice to the Secretary for every Breach that Insight Global, or any of Insight Global's Business Associates, discovers and confirms.

b. If the Breach affects 500 or more individuals, Insight Global must provide immediate notice to the Secretary.

c. If the Breach affects fewer than 500 individuals, Insight Global will maintain a log of any such Breach that has occurred and will submit such log annually to the Secretary documenting Breaches discovered during the year involved.

2. Individual Notice

   a. Subject to appropriate coordination with any notification to be provided by the Client, Insight Global will provide a written notification by first-class mail to the individual at the last known address of the individual, or, if specified as a preference by the individual, by electronic mail. Insight Global may provide the notification in one or more mailings as subsequent information regarding the Breach becomes available.

   b. In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or electronic) notification to the individual, Insight Global will provide a substitute form of notice. In instances where ten (10) or more individuals have been affected by the Breach and all contact information regarding such individuals is out-of-date, Insight Global, in its discretion, and for a period of time as determined by the Secretary, will either:

      i. Post notice of the Breach on Insight Global's website; or

      ii. Provide notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the Breach likely reside.

      iii. All methods of notice provided in (i) and (ii) above will include a toll-free number where an individual can learn whether or not the individuals unsecured PHI is possibly included in the Breach.

   c. In any case deemed by Insight Global to require urgency because of possible imminent misuse of unsecured PHI, Insight Global, in addition to the methods of notice provided in (a) and (b) above, may provide information to individuals by telephone or other means, as appropriate.

3. Media Notice Regarding Breaches Affecting 500 or More Individuals

   a. In the event that a Breach, either confirmed, or reasonably believed to have occurred, affects 500 or more individuals in a State or jurisdiction, Insight Global will provide notice to prominent media outlets serving all States or jurisdictions where such affected individuals may reside.

OTHER MEASURES REGARDING SECURITY INCIDENTS AND BREACHES

1. Insight Global will provide training and awareness materials to its Workforce Members, as appropriate, regarding the process for promptly identifying, reporting, tracking, and

responding to potential Security Incidents or Breaches in accordance with this Policy.

2. Workforce Members whose actions lead to or cause a Security Incident or Breach may be subject to sanctions, including termination, as provided in the Workforce Member Discipline Policy (Procedure No. 2).
3. No Workforce Member who reports a suspected Breach or Security Incident that is caused by another Workforce Member will face retaliation from Insight Global.

SECURITY INCIDENTS AND BREACHES CAUSED BY BUSINESS ASSOCIATES OF INSIGHT GLOBAL

1. If a Business Associate of Insight Global causes a Security Incident or Breach, or becomes aware of a possible Security Incident or Breach, regarding PHI that it uses, accesses, discloses, or maintains on behalf of Insight Global, the Business Associate will report its discovery of such Security Incidents or Breaches pursuant to the terms of its Business Associate Agreement with Insight Global.
2. Insight Global will be responsible for forwarding the report on the Security Incident or Breach discovery to the Covered Entity, who is ultimately responsible for providing notice to individuals regarding Breaches caused by its Business Associates in accordance with the procedures provided above, unless otherwise specified in the Business Associate Agreement.

Responsibility: Privacy Officer; Security Officer; Workforce Members
Regulatory Category: HIPAA Breach Notification Regulations
Regulatory Reference:

- 45 C.F.R. §164.400 et seq., Breach Notification
- 45 C.F.R. §164.308(a)(6)(i), Security Incident Procedures [Standard]

HITECH Act Language

"In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e)."

HIPAA Privacy Rule Language

Uses and Disclosures of Protected Health Information: General Rules – § 154.502

"A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor."

"A business associate may disclose PHI to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information."

Uses and Disclosures: Organizational Requirements; Standard: Business Associate Contracts -- § 164.504

"The contract or other arrangement between the covered entity and the business associate required by §164.502(e) must meet the requirements of paragraph (e)(2), (e)(3) [governmental agencies], or (e)(5), as applicable."

"A covered entity is not in compliance with the standards of §164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful, terminated the contract or arrangement, if feasible."

"A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or

arrangement, if feasible."

"The requirements of §164.504(e)(2) through (e)(4) apply to the contract or other arrangement between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate."

"A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(a) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with [the Security Rule] with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with §164.502(e)(1)(ii), ensure that any subcontractors create, receive, maintain or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information to provide an accounting of disclosures in accordance with §164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information, or if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible."

HIPAA Security Rule Language

Administrative Safeguards; Standard: Business Associate Contracts and Other Arrangements -- § 164.308(b)

"A covered entity may permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor."

"A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a) that the subcontractor will appropriately safeguard the information."

"Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a)."

Organizational Requirements; Standard: Business Associate Contracts and Other Arrangements -- § 164.614(a)

"The contract must provide that the business associate will:

(A) Comply with the applicable requirements of this subpart [the Security Rule];

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive,

maintain, or transmit electronic PHI on behalf of a business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and
(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

Purpose Statement

Insight Global is a Business Associate under the HIPAA Privacy Regulations. As a result, Insight Global will enter into Business Associate Agreements with each of its Clients. Insight Global will also enter into agreements with its Subcontractors that are Business Associates pursuant to which the Subcontractor agrees to protect the privacy and security of PHI that it creates, receives, maintains, or transmits on behalf of Insight Global.

Policy/Procedure

Business Associate Agreements with Covered Entities

Insight Global will enter into a Business Associate Agreement with each Client for which it acts as a Business Associate. The Business Associate Agreement will contain all required obligations and assurances in compliance with the HIPAA Privacy and Security Regulations. The agreement also will specify any responsibilities that the Client must fulfill with respect to HIPAA compliance.

Business Associate Agreements with Subcontractors that are Business Associates

Insight Global will enter into a Business Associate Agreement with each Subcontractor that creates, receives, maintains, or transmits PHI provided or received on behalf of Insight Global. To the extent, that such Subcontractors or their personnel have access to PHI and are performing the same job functions as Workforce Members, the Procedures set forth in this Manual that apply to Workforce Members will also be applied to such Subcontractors or their personnel.

Responsibility: Legal
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §§164.308(b)(1)-(b)(4), Business Associate Contracts and Other Arrangements [Standard; Required]
- 45 C.F.R. §164.314(a), Organizational Requirements
- 45 C.F.R. §§ 164.502(e) and 164.504(e), Uses and Disclosures of Protected Health Information: General Rules; Uses and Disclosures: Organizational Requirements

HIPAA Privacy Policies and Procedures

Insight Global	HIPAA Privacy	Procedure No.: **5**
Title: **Uses and Disclosures of PHI**	Revision:	Effective Date:

HIPAA Privacy Rule Language

Permitted Uses and Disclosures -- § 164.506

"Except with respect to uses or disclosures that require an authorization under §164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations…provided that such use or disclosure is consistent with other applicable requirements of this subpart."

Uses and Disclosures for which an Authorization is Required -- § 164.508

"Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization."

Uses and Disclosures of Protected Health Information: General Rules -- § 164.502(3)

"A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement."

Uses and Disclosures: Organizational Requirements -- § 164.504(e)(2)

A contract between the covered entity and a business associate must:

(i) "Establish the permitted uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity…"

Purpose Statement

Insight Global is permitted to use or disclose PHI as described in the Business Associate Agreements with its Clients and as otherwise provided in the Privacy Rule or required by law.

Policy/Procedure

1. Insight Global may use or disclose PHI as set forth in its agreements with its Clients.
2. Insight Global may use or disclose PHI as required by law.
3. Insight Global may use PHI for Insight Global's proper management and administration in accordance with the Agreement between Insight Global and its Client; or to carry out Insight Global's legal responsibilities.
4. Insight Global may disclose PHI for Insight Global's proper management and administration or to carry out the legal responsibilities of Insight Global, provided the disclosures are required by law, or Insight Global obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only a required by law or for the purposes for which it was disclosed to the person, and the person notifies Insight Global of any instances of which it is aware in which the confidentiality of the information has been breached.

REQUIRED USES AND DISCLOSURES

1. Insight Global will disclose PHI when the Secretary demands the PHI as a part of an investigation or determination of Insight Global's compliance with the Privacy Rule.
2. Insight Global will respond to requests by an individual for a copy of his PHI in accordance with the Access of Individuals to and Amendment of PHI Procedure (Procedure No. 8).

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.506, Uses and Disclosures to Carry Out Treatment, Payment, or Healthcare Operations [Standard; Required]
- 45 C.F.R. §164.508, Uses and Disclosures for which an Authorization is Required [Standard; Required]
- 45 C.F.R. § 164.504(e)(2)(i), Uses and Disclosures: Organizational Requirements

Insight Global	HIPAA Privacy	Procedure No.: **6**
Title: **Minimum Necessary Standard**	Revision:	Effective Date:

HIPAA Privacy Rule Language

Uses and Disclosures of Protected Health Information: General Rules--§ 164.502(b)
"When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purposes of the use, disclosure or request."

Other Requirements Relating to Uses and Disclosures of Protected Health Information; Standard: Minimum Necessary Requirements--§ 164.514(d)
"In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

"For any type of disclosure that it makes on a routine or recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure."

"A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.

"For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

"For all other requests, a covered entity must: (A) develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and (B) review requests for disclosure on an individual basis in accordance with such criteria."

Purpose Statement

Insight Global will use reasonable efforts to limit PHI or ePHI to the least amount necessary (the "minimum necessary") to accomplish the intended purpose of the use, disclosure, or request.

Policy/Procedure

Insight Global will limit all uses and disclosures of or requests for PHI to the minimum necessary to achieve the purpose of the use, disclosure or request, except for:

a. Disclosures made to the Secretary of Health and Human Services;

b. Uses or disclosures required by law; or

c. Uses or disclosures required for compliance with HIPAA.

INTERNAL USES

1. The Privacy Officer maintains a record of those Workforce Members who require access to PHI in order to carry out their job functions (e.g. a list of "Covered Workforce Members").
2. Each Client will be responsible for providing a Covered Workforce Member with access to the Client's PHI and ensuring that reasonable efforts are used to limit the access to the types of PHI which are needed to carry out the Covered Workforce Member's job functions.

DISCLOSURES

1. For any disclosure that Insight Global requests or makes on a routine and recurring basis, Insight Global will implement protocols that establish the minimum necessary amount of PHI that may be disclosed to achieve the purpose of the disclosure.
2. For all non-routine disclosures that are not exempted from the minimum necessary standard, the disclosure request must be sent to the Privacy Officer for review and determination for compliance with the minimum necessary standard.
3. The following disclosures do not have to be reviewed by the Privacy Officer for determination, and any such request will be deemed to be the minimum necessary for the requested disclosure:

   a. Disclosures made to public officials as required by or in accordance with the law, if the public official represents that the information requested is the minimum necessary for the stated purpose(s); or

   b. Disclosures made in response to a request from the Covered Entity to whom the PHI belongs; or

   c. The information is requested by a professional Workforce Member or by a Business Associate for providing professional services.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.514(d)(1)-(d)(3), Other Requirements Relating to Uses and Disclosures of PHI:

Minimum Necessary Requirements

- 45 C.F.R. § 164.502(b), Standard: Minimum Necessary

Insight Global	HIPAA Privacy	Procedure No.: **7**
Title: **De-identification of PHI**	Revision:	Effective Date:

HIPAA Privacy Rule Language

"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 not individually identifiable health information."

Purpose Statement

After PHI is de-identified, it is no longer considered "PHI" and is therefore no longer subject to the requirements of the HIPAA Privacy Regulations. PHI may only be de-identified by a Business Associate pursuant to a Business Associate Agreement.

Policy/Procedure

Insight Global Workforce Members will only de-identify PHI if requested to do so by the Client as part of the services being provided by Insight Global. The Workforce Member will follow the Client's procedure for such de-identification. Insight Global and its Workforce Members will not de-identify PHI for any other reason.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference: 45 C.F.R. §164.514(a)-(c), De-Identification

Insight Global	HIPAA Privacy	Procedure No.: **8**
Title: **Access of Individuals to PHI and Amendment of PHI**	Revision:	Effective Date:

HIPAA Privacy Rule Language

"Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set."

"An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set."

Purpose Statement

An individual has the right to inspect or obtain PHI about the individual in a designated record set, with certain limited exceptions. An individual also has the right to a request an amendment to his/her PHI in a Designated Record Set. The Client is responsible for evaluating requests for access or amendment, and either rejecting or accepting such requests.

Policy/Procedure

1. Insight Global does not maintain and manage Designated Record Sets on behalf of its Clients; therefore, Insight Global is unable to respond to requests for access or amendment.
2. If Insight Global does receive a request for access or amendment directly from an individual, it will forward such request to the respective Client as soon as practicable.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference:

- 45 C.F.R. §164.524, Access of Individuals to PHI [Standard; Required]
- 45 C.F.R. §164.526, Amendment of Protected Health Information [Standard; Required]

Insight Global	HIPAA Privacy	Procedure No.: **9**
Title: **Accounting of Disclosures of PHI**	Revision:	Effective Date:

HIPAA Privacy Rule Language

"An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested."

HITECH Act Language

"In response to a request from an individual for an accounting, a covered entity shall…provide an accounting, as specified under paragraph (1), for disclosures of protected health information that are made by such covered entity and by a business associate acting on behalf of the covered entity."

Purpose Statement

Individuals have a right to receive an accounting of disclosures of their protected health information made for the six years prior to their request. As a Business Associate, Insight Global must provide information to its Clients that will allow such Clients to respond to requests for accountings made by individuals. To be able to provide relevant information to its Clients, Insight Global must document each disclosure of PHI that it makes including the date, purpose, and recipient of the PHI and the type of PHI disclosed.

Policy/Procedure

REQUESTS FOR ACCOUNTING MADE BY COVERED ENTITY

1. Given the nature of the staffing services provided by Insight Global to its Clients, most disclosures of PHI made by Workforce Members will be at the direction of the Client and through the Client's systems. If a Client requests an accounting of disclosures from Insight Global, Insight Global will notify the Client that disclosures made by Workforce Members were made through the Client's systems and the Client is, therefore, responsible for documenting these disclosures. If Insight Global makes any disclosures that are not at the Client's direction, Insight Global will document these disclosures.
2. Upon receiving a request for an accounting of disclosures from a Client, the Privacy Officer will review the Business Associate Agreement between Insight Global and the Client to identify any timeframes in which Insight Global must respond.
3. Unless otherwise specified in the Business Associate Agreement, within 20 days of receiving the accounting request from the Client, Insight Global will provide the Client with an accounting of all disclosures of that individual's PHI made by Insight Global during the six years (or such shorter time as requested by the individual) prior to the request,

which were not made at the direction of the Client or through the Client's systems. Such response will include the following:

a. The date of the disclosure.

b. The name and address, if known, of the recipient of the PHI.

c. A brief description of the PHI disclosed.

d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure. Alternatively, Insight Global may include a written request from the third party for the information disclosed.

4. If Insight Global is unable to act on the accounting request within 20 days or the time period provided in the Business Associate Agreement, Insight Global may extend the deadline by no more than 30 additional days if, prior to the expiration of the initial timeframe days, Insight Global provides the Client with an explanation for the delay and an estimated date of completion. The Client will then notify the individual of the reason for the delay. Insight Global may only exercise one such extension.

5. The following disclosures of PHI are not required to be included in a requested accounting:

   a. Disclosures made to carry out treatment, payment, and healthcare operations.

   b. Disclosures made to individuals of PHI about them.

   c. Disclosures made incident to a use or disclosure otherwise permitted or required by HIPAA.

   d. Disclosures made pursuant to an authorization.

   e. Disclosures made for the Covered Entity's facility directory or to persons involved in the individual's care.

   f. Disclosures made for national security or intelligence purposes.

   g. Disclosures made to correctional institutions or law enforcement officials.

   h. Disclosures made as part of a limited data set.

   i. Disclosures that occurred 6 years prior to the request.

6. Insight Global must suspend an individual's right to receive an accounting of disclosures made to a health oversight or law enforcement agency if that agency requests that Insight Global do so.

   a. The agency requesting suspension must submit a written statement that Insight Global's provision of a requested accounting to an individual would be reasonably likely to impede the activities of the agency. The statement must also state the duration of the requested suspension.

   b. If the agency requesting suspension does not submit a written statement, but rather requests the suspension orally, Insight Global must:

i. Document the identity of the agent and agency requesting the suspension and the reason for it. Insight Global will include the badge number or a copy of the agent's credentials in the documented record.

ii. Effect a temporary suspension of the individual's right to an accounting of disclosures made to that agency.

iii. Limit the duration of the suspension to 30 days or less from the time of the oral request, unless a written request is provided during that time.

REQUESTS FOR ACCOUNTING MADE BY AN INDIVIDUAL DIRECTLY TO INSIGHT GLOBAL

If an individual presents a request for an accounting of disclosures directly to Insight Global, Insight Global shall, within ten (10) business days, forward the request to the Client.

DOCUMENTATION AND RETENTION

Insight Global must retain the following documents for at least six years:

a. The information required to be included in a requested accounting.

b. Copies of written accountings provided to Clients.

c. Designation of persons responsible for processing requests for accountings.

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference: 45 C.F.R. §164.528, Accounting of Disclosures of Protected Health Information [Standard; Required]

Insight Global	HIPAA Privacy	Procedure No.: **10**
Title: **Assigned Privacy Responsibility**	Revision:	Effective Date:

HIPAA Privacy Rule Language

"A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity."

Purpose Statement

Insight Global will install a Privacy Officer who will be responsible for the implementation and day-to-day administration and oversight of Insight Global's compliance with the HIPAA Privacy Regulations. The Privacy Officer will also develop Workforce Training programs regarding the privacy of PHI, update and implement these Privacy Policies and Procedures, and serve as the designated decision-maker for issues and questions involving interpretation of the HIPAA Privacy Regulations.

Policy/Procedure

1. The Privacy Officer is responsible for the following tasks:
    a. Inventorying the uses and disclosures of all PHI;
    b. Working with Insight Global's Legal team to ensure that legal issues in drafting compliance documents are addressed or engage appropriate legal counsel to draft such documents;
    c. Administering sanctions upon Workforce Members for violations of these Privacy Policies and Procedures (Procedure No. 2);
    d. Developing, updating, and revising these Privacy Policies and Procedures as necessary to comply with the HIPAA Privacy Regulations;
    e. Developing a privacy training program;
    f. Establishing procedures to monitor internal privacy compliance;
    g. Keeping up to date on the latest privacy developments and federal and state laws and regulations;
    h. Coordinating with the Security Officer in evaluating and monitoring operations and systems development for compliance with the HIPAA Privacy and Security Regulations;
    i. Serving as Insight Global's liaison to the Office of Civil Rights for matters relating to HIPAA and, in some cases, other regulatory bodies for matters related to privacy;
    j. Coordinating any audits of the Secretary of HHS or any other governmental or

accrediting organization regarding Insight Global's compliance with state or federal privacy laws or regulations; and

k. Other tasks that are necessary to ensure the privacy of PHI.

2. Insight Global's Privacy Officer's name and contact information is:

David C. Lowance, Jr.
General Counsel
Insight Global, LLC
4170 Ashford Dunwoody Road
Atlanta, Georgia 30319
David.lowance@insightglobal.net
(404) 335-7347 (office) (IG Ext: 1517)
(404) 797-5846 (mobile)
(404) 257-1070 (fax)

Responsibility: Privacy Officer
Regulatory Category: Privacy Regulations
Regulatory Reference: 45 C.F.R. §164.530(a), Personnel Designations [Standard; Required]

HIPAA Security Policies and Procedures

Insight Global	HIPAA Security	Procedure No.: **11**
Title: **Security Risk Management**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement policies and procedures to prevent, detect, contain, and correct security violations."

Purpose Statement

Insight Global, under the HIPAA Security Regulations, is required to implement a security management process. Implementation of this security management process will assist Insight Global in ensuring the confidentiality, integrity, and availability of ePHI. Insight Global will create and maintain appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations.

Policy/Procedure

RISK ANALYSIS

1. At least once per year, Insight Global will convene a workgroup to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI to which Insight Global Workforce Members have access through Insight Global Workstations.
2. The workgroup may consider:
    a. Potential security risks to ePHI, including those Security Incidents specifically identified in the Breach and Security Incident Response Procedures Policy;
    b. The probability of the occurrence of risks which may affect Insight Global's Workstations;
    c. The magnitude of the identified risks;
    d. The criticality of ePHI to Insight Global's operations during or after an emergency or disaster (see Applications and Data Criticality Analysis (Procedure No. 22));
    e. The frequency of reviews and audits of Insight Global's Workstations pursuant to the Information System Activity Review Policy;
    f. The training, and the frequency of such training, to be offered to Insight Global's Workforce Members regarding the security of ePHI;
    g. The need to do penetration testing of the security of Insight Global's Workstations; and
    h. The need to engage third parties to evaluate the risks and vulnerabilities to the Workstations.

RISK MANAGEMENT

1. In an effort to reduce risks and vulnerabilities to ePHI maintained on or accessed through Insight Global Workstations, Insight Global will update its Security Policies and Procedures if the results of the assessment show that such updates are needed and revise, as needed, its Risk Management Plan to address risks identified in the annual Risk Analysis.
2. In addition to updating the Security Policies and Procedures and Risk Management Plan after each Risk Analysis if necessary, Insight Global will also update the Policies and Procedures and Plan as needed:
    a. After any Security Incident to minimize the likelihood of a similar Security Incident occurring in the future;
    b. After a new functionality or use is added to Workstations provided to Covered Workforce Members and such functionality or use would reasonably be expected to have a material impact on the security of any PHI, including ePHI; and
    c. In response to environmental or operational changes (e.g. significant new threats or risks to the security of ePHI; changes to Insight Global's organizational or technical infrastructure; changes to Insight Global's information security requirements or responsibilities; or availability of new security technologies or recommendations).
3. In developing each Risk Management Plan, Insight Global will consider the following:
    a. The security measures that are already in place to address the risk;
    b. Additional security measures that can reasonably and appropriately be put in place to address the risk;
    c. Communication of the security measures and Risk Management Plan to Insight Global's Workforce Members where appropriate; and
    d. The need to engage other resources to assist in the implementation of the Risk Management Plan.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(1)(i), Security Management Process [Standard; Required]
- 45 C.F.R. §164.308(a)(1)(ii)(A), Risk Analysis [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(1)(ii)(B), Risk Management [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(8), Evaluation [Standard; Required]
- 45 C.F.R. §164.316(b)(2)(iii), Updates [Implementation Specification; Required]

Insight Global	HIPAA Security	Procedure No.: **12**
Title: **Information System Activity Review**	Revision:	Effective Date:

HIPAA Security Rule Language

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

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

Purpose Statement

Insight Global will implement hardware, software, and/or procedural mechanisms that record and examine activity on those of its Workstations used by Covered Workforce Members and connected to the Insight Global network to enable Insight Global to detect potentially problematic activity. These audit controls will allow Insight Global to:

1. Identify questionable data access activities on Workstations;
2. Investigate Breaches; and
3. Respond to potential weaknesses in Workstation architecture.

Policy/Procedure

AUDIT LOGS

1. The following activity audit logs may be generated and reviewed for each Workstation that is used by a Covered Workforce Member and connected to the Insight Global network:
   a. Log-on attempts;
   b. Failed authentication attempts after a three (3) unsuccessful attempts; and
   c. Automatic sign-offs.
2. The Workstation activity auditing mechanisms may generate the following information for each audit log:
   a. Date and time of activity;
   b. Descriptions of each attempted or completed activity;
   c. Identification of the Workforce Member performing the activity; and/or
   d. Origin of the activity, such as the I/P address or workstation identification number.
3. Insight Global will secure access to audit logs so they cannot be altered, overwritten, or erased, and will limit viewing of audit logs to those with a job-related need.

4. Insight Global will promptly back up audit logs to a centralized log server or other secured media.

FREQUENCY OF INFORMATION SYSTEM ACTIVITY REVIEW

1. Insight Global will use its findings from the Risk Analysis conducted pursuant to the Security Risk Management Procedure (Procedure No. 11) to help determine the frequency of its activity review of each security measure.
2. Insight Global will identify and document the names of Workforce Members who will review audit logs.
3. Insight Global will retain audit logs for six (6) years after the date they are created.

IDENTIFICATION OF INAPPROPRIATE ACTIVITY

1. As patterns are identified and anomalous behavior becomes more apparent, Insight Global may establish thresholds for each audit report. The thresholds will signify the level at which certain behavior warrants further inspection and may signal a Security Incident or failure to comply with Insight Global's policies and procedures. As thresholds are established, this policy will be revised accordingly.
2. If Security Incidents are identified, they will be addressed in accordance with the Breach and Security Incident Response Procedure (Procedure No. 3).
3. If the audit logs reveal that a Workforce Member failed to comply with Insight Global's policies and procedures, appropriate sanctions may be imposed upon the Workforce Member pursuant to the Insight Global Workforce Member Discipline Policy (Procedure No. 2).

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164308(a)(1)(ii)(D), Information System Activity Review [Implementation Specification; Required]
- 45 C.F.R. §164.312(b), Audit Controls [Standard; Required]

Insight Global	HIPAA Security	Procedure No.: **13**
Title: **Assigned Security Responsibility**	Revision:	Effective Date:

HIPAA Security Rule Language

"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

Purpose Statement

Insight Global's Security Officer is responsible for the development and implementation of the Security Policies and Procedures in this Manual. In addition, the appointment of the Security Officer will provide organizational focus to, and highlight the importance of, Insight Global's efforts to protect the confidentiality, privacy and security of its ePHI and Workstations.

Policy/Procedure

1. The Security Officer will perform the following duties, including taking all reasonable and appropriate measures to:
    a. Ensure and confirm that Insight Global is compliant with applicable federal, state, and local laws pertaining to the security of ePHI;
    b. Guide the development, documentation, and dissemination of appropriate security policies and procedures for the Workforce Members and administrators of Insight Global;
    c. Ensure that newly acquired Workstations have options that support required and/or addressable implementations of the HIPAA Security Regulations and Insight Global's internal security requirements;
    d. Approve and oversee the administration, implementation, and selection of Insight Global's security controls for Workstations;
    e. Implement and oversee the security training of Insight Global's Workforce Members, and ensure that Workforce Members receive such training on a periodic basis as deemed necessary pursuant to Insight Global's Security Risk Management Policy (Procedure No. 11);
    f. Facilitate the yearly Risk Analysis and creation of a Risk Management Plan under Insight Global's Security Risk Management Policy (Procedure No. 11);
    g. Ensure that Workstation activity is monitored and audited to identify Security Incidents and malicious activity as set forth in the Information System Activity Review Policy (Procedure No. 12);
    h. Ensure that the threats and risks to the confidentiality, integrity, and availability of ePHI are monitored and evaluated; and

i. Oversee the development and implementation of an effective Security Incident response policy and related procedures as set forth in Insight Global's Breach and Security Incident Response Procedures Policy (Procedure No. 3).

2. Insight Global's Security Officer's name and contact information is:

   David C. Lowance, Jr.
   General Counsel
   Insight Global, LLC
   4170 Ashford Dunwoody Road
   Atlanta, Georgia 30319
   David.lowance@insightglobal.net
   (404) 335-7347 (office) (IG Ext: 1517)
   (404) 797-5846 (mobile)
   (404) 257-1070 (fax)

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference: 45 C.F.R. §164.308(a)(2), Assigned Security Responsibility [Standard; Required]

Insight Global	HIPAA Security	Procedure No.: **14**
Title: **Workforce Member Security and Information Access Management**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI, as provided under paragraph (a)(4) [information access management] of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic PHI."

"Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of subpart E of this part."

Subpart E refers to the HIPAA Privacy rules, located at 45 C.F.R. §164.500 et seq.

Purpose Statement

To protect the confidentiality, integrity, and availability of ePHI, Insight Global will implement reasonable and appropriate safeguards to prevent unauthorized access to ePHI while ensuring that properly authorized Covered Workforce Members' access to ePHI is permitted.

Policy/Procedure

WORKFORCE CLEARANCE

1. A Workforce Member's Account Manager will identify and define security privileges for a Workforce Member who is granted access to PHI in connection with an assignment for a specific Client.
2. Based on the level of privileges to be granted to candidates for employment, Human Resources personnel will perform appropriate and reasonable verifications checks on the candidate.
3. Verification checks may include, but are not limited to:
    a. Character references;
    b. Confirmation of claimed academic and professional qualifications;
    c. Credit checks;
    d. Criminal background checks; or
    e. Exclusion testing by reference to databases maintained by the Office of the Inspector General of the United States Department of Health & Human Services.
4. Upon accepting an offer of employment, each Covered Workforce Member will sign the Workforce Member Confidentiality and Compliance Statement as required pursuant to the Insight Global Workforce Member Confidentiality and Compliance Statement Policy

(Procedure No. 1).

SUPERVISION OF WORKFORCE MEMBERS

1. Each Account Manager will take reasonable and appropriate steps to ensure that Workforce Members under the Account Manager's control who have the ability to access ePHI or those who work in areas where ePHI might be accessed will be properly supervised. Insight Global will coordinate with the Client to ensure that Workforce Members only access such ePHI that they are authorized to access pursuant to their job responsibilities.
2. In accordance with the Insight Global Workforce Member Discipline Procedure (Procedure No. 2), Insight Global will ensure that appropriate sanctions are taken against Workforce Members when appropriate.

ESTABLISHING ACCESS TO EPHI

1. Each Client will determine to level of access to ePHI to provide to each Insight Global Workforce Member. Insight Global will coordinate with the Client to ensure that only those Workforce Members authorized by the Client will have access to ePHI.
2. Workforce Members will not be granted access to, and must not attempt to access, ePHI until the Workforce Member has been properly authorized.
3. Each Covered Workforce Member will be assigned a unique username and temporary password to activate the Covered Workforce Member's access to his/her Workstation.
4. Once the Covered Workforce Member receives his or her temporary password, the Covered Workforce Member will select and secure a new password in accordance with the Insight Global Password Management Policy (Procedure No. 17).

REVIEW OF WORKFORCE MEMBERS' ACCESS TO EPHI

1. Insight Global will periodically review Covered Workforce Members' access privileges to ePHI.
2. Insight Global may modify, if necessary, a Covered Workforce Member's access privileges to ePHI.

MODIFICATION OF WORKFORCE MEMBERS' ACCESS TO EPHI

1. When a Covered Workforce Member's access to ePHI must be modified, either because of a change in the Covered Workforce Member's job function or the Covered Workforce Member's termination, Insight Global will document such modifications.
2. Such documentation may include:
    a. The date and time of the modification;
    b. The identification of the Workforce Member whose access is being modified;
    c. A description of the Workforce Member's modified access rights; and

d. The reason for the modification of the Workforce Member's access rights.

TERMINATION PROCEDURES UPON A WORKFORCE MEMBER'S TERMINATION BY INSIGHT GLOBAL

1. When Covered Workforce Members are terminated, Insight Global will promptly remove or disable the Covered Workforce Member's access privileges to the applicable Insight Global systems before the Covered Workforce Member is notified of his or her termination, when feasible (noting that most Covered Workforce Members will not generally have access to Insight Global's information systems in the routine course of their duties).
2. Such system access privileges include, but are not limited to:
    a. Workstations and server access;
    b. Data access, particularly access to data contained within the applicable Workstation;
    c. Insight Global network access;
    d. Email accounts; and/or
    e. Inclusion on group email lists.

GENERAL RESIGNATION AND TERMINATION PROCEDURES

1. Insight Global will terminate, as appropriate, a departing or terminated Workforce Member's physical access to areas where ePHI is located within Insight Global's facilities (if any).
2. Insight Global will collect, and document the collection of, equipment and property that contains ePHI, which were used by the terminated or departing Covered Workforce Member.
    a. Such documentation will include:
        i. The Workforce Member's name;
        ii. The date and time the equipment and property were returned; and
        iii. The identification of the returned property and equipment.
    b. Insight Global will securely maintain such documentation.
3. Equipment that may contain, allow, or enable the Covered Workforce Member to access ePHI, and which must be returned upon the Covered Workforce Member's termination or departure, include, but is not limited to:
    a. Portable computers;
    b. Personal Digital Assistants (PDAs);
    c. Name tags or name identification badges;
    d. Security tokens; and/or
    e. Facility access cards, building, desk, or office keys.

LOG-IN MONITORING

1. The Covered Workforce Member log-in process for each Workstation will use at least one of the following:
   a. Limitations on the number of unsuccessful log-in attempts; and/or
   b. Software to record failed log-in attempts to the Workstation.
2. If applicable, the Security Officer will determine the standard for the number of log-in attempts allowed for each Workstation before such failure triggers a lock-out and is logged.
3. If a Covered Workforce Member is accidentally locked out of a Workstation, he or she will have his or her password reset by the Insight Global Help Desk.
4. Insight Global will monitor the log-ins of Covered Workforce Members into Workstations in accordance with the Information System Activity Review Procedure (Procedure No. 12).

Responsibility: Security Officer; Workforce Members
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(3)(i), Workforce Security [Standard; Required]
- 45 C.F.R. §164.308(a)(3)(ii)(A), Authorization and/or Supervision [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(3)(ii)(B), Workforce Clearance Procedure [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(3)(ii)(C), Termination Procedures [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(4)(i), Information Access Management [Standard; Required]
- 45 C.F.R. §164.308(a)(4)(ii)(B), Access Authorization [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(4)(ii)(C), Access Establishment and Modification [Implementation Specification; Addressable]
- 45 C.F.R. §164.308(a)(5)(ii)(C), Log-In Monitoring [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **15**
Title: **Security Awareness, Training and Reminders**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement a security awareness and training program for members of its workforce (including management)."

"Implement periodic security updates."

Purpose Statement

Insight Global has the responsibility under the HIPAA Security Regulations for providing and documenting security awareness and training for Insight Global Covered Workforce Members in order that those persons can properly carry out their functions while appropriately safeguarding ePHI. This policy reflects Insight Global's commitment to comply with such Regulations.

Policy/Procedure

1. Insight Global will provide training and supporting reference materials to its Covered Workforce Members, as appropriate, to carry out their functions with respect to the security of ePHI. As part of its Risk Analysis, pursuant to its Security Risk Management Policy (Procedure No. 11), Insight Global will determine how often such training will be required for its Covered Workforce members and the method of such training.
2. Insight Global will maintain sufficient records that document and confirm a Covered Workforce Member's completion of security awareness training.
3. Security awareness training should include information to make Covered Workforce Members aware of and familiar with Insight Global's HIPAA Security Policies and Procedures, which will be made available to Covered Workforce Members for reference and review.
4. Insight Global shall use reasonable efforts to cause each Covered Workforce Member to comply with any HIPAA training provided by Client.
5. Insight Global's Security Officer will periodically, as needed, issue security information and awareness reminders to Covered Workforce Members.
6. Insight Global will issue security reminders immediately upon, or within a reasonable time following, the occurrence of any of the following events:
    a. Substantial revisions are made to Insight Global's Security Policies and Procedures;
    b. Substantial new security controls are implemented or significant changes are made to existing security controls; or
    c. Substantial changes are made to Insight Global's legal or business responsibilities including.

7. Means of providing security information and awareness reminders and updates may include a newsletter or any other mechanisms used by Insight Global to communicate with Covered Workforce Members.

Responsibility: Security Officer; Workforce Members
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(5)(i), Security Awareness and Training [Standard; Required]
- 45 C.F.R. §164.308(a)(5)(ii)(B), Security Reminders [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **16**
Title: **Malicious Software**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement procedures for guarding against, detecting, and reporting malicious software."

Purpose Statement

Insight Global will implement and periodically review its process and implemented safeguards for guarding against, detecting, and reporting malicious software that pose risks to ePHI or Workstations.

Policy/Procedure

1. Insight Global will take all necessary and reasonable measures to protect its Workstations from malicious software, including:
    a. Installing anti-virus software on all media devices and hardware containing ePHI or which have access to ePHI;
    b. Mitigating the harm of malicious software attacks by recovering ePHI and other data contained on all media devices and hardware that has been attacked by malicious software; or
    c. Requiring all Covered Workforce Members to scan email attachments and downloads before they are opened.
2. Insight Global Covered Workforce Members must not bypass or disable anti-virus software installed on Workstations unless they are properly authorized to do so.
3. Insight Global will provide periodic training and awareness to its Covered Workforce Members about guarding against, detecting, and reporting malicious software, including:
    a. How to discover malicious software;
    b. How to report malicious software;
    c. How to scan for malicious software that may be contained in email attachments; and/or
    d. How to use anti-virus software.
4. Covered Workforce Members must immediately report suspected or confirmed malicious software to the Security Officer.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference: 45 C.F.R. §164.308(a)(5)(ii)(B), Protection from Malicious Software [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **17**
Title: **Password Management**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement procedures for creating, changing, and safeguarding passwords."

Purpose Statement

To prevent unauthorized access to and use of ePHI contained within its Workstations, Insight Global requires Covered Workforce Members to take appropriate measure to select and secure passwords that allow such access to Workstations.

Policy/Procedure

1. Passwords must be re-set at least every 60 days.
2. To maintain accountability, passwords must be individualized and kept confidential by each Covered Workforce Member.
3. Covered Workforce Members must create and change their own passwords.
4. The same password cannot be reused.
5. Passwords cannot be displayed in clear text when inputting them into the Workstation.
6. Passwords must be 7-16 characters in length, including at least one numeric and other character (e.g. #, $, or &).
7. Passwords cannot include a Workforce Member's name.
8. Passwords must be committed to memory or if stored in written, tangible format, in a place to which only the Covered Workforce Member has access.

Responsibility: Security Officer; Workforce Members
Regulatory Category: Administrative Safeguards
Regulatory Reference: 45 C.F.R. §164.308(a)(5)(ii)(D), Password Management [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **18**
Title: **Contingency Plan**	Revision:	Effective Date:

HIPAA Security Rule Language

"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 PHI."

Purpose Statement

Insight Global's Covered Workforce Members may have access to a Client's systems that contain PHI through an Insight Global Workstation, but Insight Global does not maintain such PHI or systems. Nevertheless, Insight Global has developed and implemented a Contingency Plan that establishes procedures to recover Workstations and help ensure continuity of operations following a disruption. Insight Global has established the following objectives for this Contingency Plan:

1. Maximize the effectiveness of Insight Global's contingency operations through an established plan that consists of the following phases:
    a. Notification and Activation Phase to detect and assess damage and to activate the plan;
    b. Recovery phase to recover damage done to Workstations and provide access to temporary Workstations, if warranted; and
    c. Reconstitution phase to restore each Workstation to normal operations.
2. Identify the activities, resources, and procedures needed to meet Insight Global's obligations to its Clients during prolonged interruptions to normal operations.
3. Assign responsibilities to designated Workforce Members who will participate in the contingency planning strategies, and provide guidance for recovering each Workstation during prolonged periods of interruption to normal operations.
4. Ensure coordination with external points of contact and Subcontractors who will participate in the contingency planning strategies.

This Insight Global Contingency Plan Policy applies to the functions, operations, and resources necessary to restore and resume the operations of Insight Global's Workstations after an emergency or disaster. This Policy does not apply to any functions and operations for restoring information systems owned and operated by other parties (e.g., Clients) and to which Insight Global only has access.

Policy/Procedure

CONTINGENCY PLAN TRIGGERS

This Contingency Plan will be activated upon the occurrence of an emergency or disaster that impacts the availability of Covered Workforce Members or Workstations for a prolonged

period.

MITIGATION MEASURES

Insight Global will implement the following measures to mitigate any damage caused to ePHI as a result of an emergency or disaster and to continue operations after such an event:

a. Identify key personnel and train such personnel in how to perform his or her emergency response and recovery roles.
    1. Insight Global will identify the roles that particular Workforce Members will serve while Insight Global is operating in disaster mode.
    2. Insight Global will identify designated Workforce Members who will be permitted to administer or modify processes and controls that protect the security of ePHI while Insight Global is operating in disaster mode.
b. To the extent that Workstations are maintained in Insight Global facilities, Insight Global will ensure that preventative controls, such as generators, waterproof tarps, sprinkler systems, and fire extinguishers will be fully operational at the time of an emergency or disaster. To the extent that Workstations are maintained in Client's facilities, Client will be responsible for ensuring that such preventative controls are in place.
c. Ensure that Insight Global will maintain service agreements with hardware, software, and communications providers to support the Workstation recovery.

CONTINGENCY PLAN TEAMS

1. Insight Global has established the following teams to participate in recovering the operations of the affected Workstations and Workforce Members:
    a. Management Team;
    b. Application Recovery Team;
    c. Operating System Team;
    d. Network Operations Team;
    e. Site Restoration/Salvage Team;
    f. Procurement Team;
    g. Damage Assessment Team; and
    h. Communications Team.
2. The Security Officer will determine, based on the system environment and scope of the recovery effort, which team(s) will be necessary to execute the plan.
3. The Security Officer will maintain a documented list of all Contingency Plan Teams, team Leaders, and additional team members.

NOTIFICATION PROCEDURES

1. A first responder, or other Insight Global personnel who discovers that Insight Global's facilities or Workstations have been affected by an emergency or disaster, must notify the appropriate Insight Global official, by telephone, pursuant to the following sequence:
    a. Security Officer, David C. Lowance, Jr., (404) 335-7437;
    b. Chief Operations Officer/Chief Information Officer, Christopher W. Vogel, (404) 335-7297
    c. Any President or Vice President of Insight Global;
    d. The Chief Financial Officer, Michael B. Lewis;
    e. The Senior Vice President of Human Resources, Kevin M. Ingham.
2. When activated, members of the Communications Team will contact Insight Global's Workforce Members to notify them of the general status of the contingency event and any next steps.

DAMAGE ASSESSMENT PROCEDURES

As determined by the Security Officer, or other Insight Global Official, upon his or her initial review of the situation, he or she may activate the Damage Assessment Team to assess the following:

a. The cause of the disruption;
b. The potential for additional disruption or damage;
c. The affected physical area and the status of physical infrastructure;
d. The status of Workstation functionality and inventory, including items that may need to be replaced; and
e. The estimated time to repair services to normal operations.

ACTIVATION OF CONTINGENCY PLAN

1. If the Contingency Plan is to be activated, the Security Officer, or other Insight Global Official as identified above, will notify all Contingency Plan team leaders and inform them of the details of the event and whether relocation of Workstations or Workforce Members to another facility is required.
2. If necessary, the Security Officer, or other Insight Global Official, will notify Insight Global's designated offsite storage facility that a Contingency Event has been declared and to ship the required materials, as determined by the Security Officer's initial review of the situation, to an alternate site.
3. If necessary, the Security Officer, or other Insight Global Official, will notify the designated alternate site that a Contingency Event has been declared and to prepare the facility for Insight Global's arrival.

RECOVERY OPERATIONS

Insight Global will restore its Workstations and recover ePHI in accordance with the following Policies and Procedures:

a. Data Backup Plan Policy;

b. Disaster Recovery Plan Policy; and

c. Emergency Mode Operation Plan.

RECONSTITUTION TO NORMAL OPERATIONS

1. Once the affected Workstation(s) becomes operational or Insight Global's facility can be accessed, Insight Global will take all reasonable steps to provide a seamless transition of operations from the alternate site to its facility.
2. Insight Global will designate a team, or engage a third party, to clean the alternate site of any equipment or other materials belonging to Insight Global and ensure the safe handling of ePHI.
3. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to Insight Global's facility.
4. Insight Global will then instruct its Workforce Members to return to Insight Global's facility.

OTHER CONTINGENCY PLAN PROCEDURES

1. Insight Global will perform a criticality analysis to determine the importance of Workstations and Workforce Members to Insight Global's operations during or after a disaster in accordance with the Insight Global Security Risk Management Policy and as outlined in the Insight Global Applications and Data Criticality Analysis Policy (Procedure No. 22).
2. Insight Global will provide periodic training materials regarding its disaster and emergency response procedures to Workforce Members, as appropriate.
3. Insight Global will periodically test its Contingency Plan to ensure that critical business processes can continue in a satisfactory manner. If necessary, Insight Global may revise the Contingency Plan, and the occurrence of any of the following events may result in a revision of the Contingency Plan:
    a. Disaster recovery role and responsibility changes, including changes to contact information;
    b. Changes to Insight Global's physical or technical infrastructure or operating systems;
    c. Changes in threats to Workstations and ePHI; or
    d. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.

Responsibility: Security Officer; other Insight Global Officials as deemed necessary
Regulatory Category: Administrative Safeguards
Regulatory Reference: 45 C.F.R. §164.308(a)(7)(i), Contingency Plan [Standard; Required]

Insight Global	HIPAA Security	Procedure No.: **19**
Title: **Data Backup Plan**	Revision:	Effective Date:

HIPAA Security Rule Language

"Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI."

Purpose Statement

Insight Global is not responsible for maintaining ePHI on behalf of its Clients. Any ePHI maintained by a Covered Workforce Member on a Workstation must be an exact copy of the ePHI maintained by the Client. This will enable the Covered Workforce Member to retrieve an exact copy of the ePHI if so required.

Policy/Procedure

1. To the extent that a Covered Workforce Member stores ePHI on a Workstation, this ePHI must be an exact copy of the ePHI maintained by the Client such that the ePHI on the Workstation is a redundant duplicate of the ePHI maintained by the Client but not the Client's sole back-up of such ePHI.
2. The Client is responsible for ensuring that it has proper back-ups of its ePHI and must not rely on Insight Global to provide this service; provided, however, Client may assign a Covered Workforce Member to create data back-ups for Client using Client's information systems.
3. If the Covered Workforce Member needs to retrieve a back-up of the ePHI maintained on his/her Workstation, he/she will retrieve such a copy from the Client's systems.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(A), Data Backup Plan [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(7)(ii)(D), Testing and Revision Procedures [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(d)(2)(iv), Data backup and storage [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **20**
Title: **Disaster Recovery Plan**	Revision:	Effective Date:

HIPAA Security Rule Language

"Establish (and implement as needed) procedures to restore any loss of data."

Purpose Statement

Insight Global will implement a disaster recovery plan to restore or recover any loss of ePHI and to restore its Workstations from damage caused by an emergency or disaster, such as fire, vandalism, terrorism, system failure, or natural disaster.

Policy/Procedure

1. Insight Global will restore any loss of data through use of the Client's information systems.
2. Insight Global will periodically test its Disaster Recovery Plan to ensure that critical business processes can continue in a satisfactory manner. If necessary, Insight Global may revise the Disaster Recovery Plan, and the occurrence of any of the following events may result in a revision of the Disaster Recovery Plan:
    a. Disaster recovery role and responsibility changes, including changes to contact information.
    b. Changes to Insight Global's physical or technical infrastructure or operating systems.
    c. Changes in threats to ePHI or Workstations.
    d. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(B), Disaster Recovery Plan [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(7)(ii)(D), Testing and Revision Procedures [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **21**
Title: **Emergency Mode Operation Plan**	Revision:	Effective Date:

HIPAA Security Rule Language

"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."

Purpose Statement

Insight Global will develop and implement an Emergency Mode Operation Plan to enable the continuation of its critical business processes and to protect the security of ePHI while Insight Global operates in emergency mode. Insight Global's Emergency Mode Operation Plan will permit authorized Workforce Members to access and use ePHI contained within the affected Workstations during and immediately following an emergency or disaster. Emergency mode operation procedures detailed in the Emergency Mode Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while Insight Global operates in emergency mode.

Policy/Procedure

1. Insight Global's emergency Mode Operation Plan will:
    a. Define and categorize reasonably foreseeable emergencies and/or disasters that could have an impact on the confidentiality, integrity, and availability of ePHI within each Workstation.
    b. Include a procedure that specifies how Insight Global will react to emergencies and disasters.
    c. Include a procedure that outlines how Insight Global will maintain HIPAA security processes and controls during and immediately following an emergency or disaster.
    d. Authorize designated Workforce Members to enter Insight Global's offices and facilities and any offsite location where electronic media are stored to maintain the security process and controls of the affected Workstations.
    e. Identify the roles that particular Insight Global Workforce Members will serve while Insight Global is operating in emergency mode.
    f. Identify the roles that designated Workforce Members who will be permitted to administer or modify processes and controls that protect the security of ePHI while Insight Global is operating in emergency mode.
2. Insight Global will make its Emergency Mode Operations Plan easily available to its Workforce Members at all times.

3. Insight Global will periodically test its Emergency Mode Operations Plan to ensure that critical business processes can continue in a satisfactory manner. If necessary, Insight Global may revise the Emergency Mode Operations Plan, and the occurrence of any of the following events may result in a revision of the Emergency Mode Operations Plan:
    a. Disaster recovery role and responsibility changes, including changes to contact information.
    b. Changes to Insight Global's physical or technical infrastructure or operating systems.
    c. Changes in threats to ePHI or Workstations.
    d. Results of testing that indicate that the plan needs to be modified to ensure that it is sufficient, accurate, and up-to-date.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference:

- 45 C.F.R. §164.308(a)(7)(ii)(C), Emergency Mode Operation Plan [Implementation Specification; Required]
- 45 C.F.R. §164.308(a)(7)(ii)(D), Testing and Revision Procedures [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **22**
Title: **Applications and Data Criticality Analysis**	Revision:	Effective Date:

HIPAA Security Rule Language

"Assess the relative criticality of specific applications and data in support of other contingency plan components."

Purpose Statement

The purpose of the criticality analysis is for Insight Global to document the impact to its services, processes, and operating objectives if a disaster or other emergency causes any or all of Insight Global's Workforce Members and Workstations to become unavailable for a documented period of time. The criticality analysis will serve as the basis for the prioritization of each Workstation and the importance of its functionality to Insight Global's business operations during a disaster.

Policy/Procedure

1. To prioritize Insight Global's Workstations for disaster recovery, the Information Technology Department will develop a matrix, which:
   a. Inventories all Workstations; and
   b. Determines the necessity of each Workstation to the operation of Insight Global's critical business functions.
2. The matrix will be used to determine which Workstations are most important to the operation of Insight Global's critical business functions and thereby determine how disaster recovery efforts will be focused during a Contingency Event or other disaster.
3. The matrix may direct:
   a. Which Workstations will be restored first; and/or
   b. Which Workstations will receive the first line of assistance during a disaster.
4. Insight Global will conduct a yearly data criticality analysis as part of its risk assessment in accordance with the Security Risk Management Policy (Procedure No. 11).
5. The Security Officer, or his/her designee, will be responsible for documenting all activities relating to the data criticality analysis, and such documentation will be maintained and retained by the Security Officer for six years from the date of creation.

Responsibility: Security Officer
Regulatory Category: Administrative Safeguards
Regulatory Reference: 45 C.F.R. §164.308(a)(7)(ii)(E), Applications and Data Criticality Analysis [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **23**
Title: **Facility Access and Security**	Revision:	Effective Date:

HIPAA Security Rule Language

"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."

Purpose Statement

Insight Global will limit physical access to its facilities in which Workstations or ePHI is located or accessible. Such access will be granted only to those Covered Workforce Members and individuals who have been authorized to access Insight Global's facilities and areas where Workstations or ePHI are contained or accessible. During a Contingency Event, Insight Global will allow physical access to its facilities that contain Workstations or ePHI only to those authorized pursuant to its Contingency Plan. Insight Global will implement facility security controls to protect its facilities from unauthorized physical access, tampering, and theft. Insight Global will maintain records documenting any repairs or modifications that impact the physical security of its facilities or equipment.

Policy/Procedure

1. Insight Global will validate a Covered Workforce Member's access to facilities and areas with access to ePHI or Workstations in accordance with the Insight Global Information Access Management Policy (Procedure No. 14)
2. In the event of an emergency or disaster, only those authorized Insight Global Workforce Members who are identified in the Contingency Plan, Disaster Recovery Plan or Emergency Mode Operations Plan, will be permitted to access areas of Insight Global's facilities that contain ePHI or Workstations.

Facility Security Controls

1. Covered Workforce Members must immediately report to the Security Officer the loss or theft of any device, such as a facility access card or identification badge, that allows them physical access to an Insight Global facility and/or to areas where ePHI is contained or Workstations that can access ePHI are located.
2. Insight Global will supervise all visitors and Subcontractors while they are physically present in its facilities where PHI may be located or stored in hardcopy or electronic format.
3. Insight Global may install the following security controls to protect its facilities from unauthorized access, tampering and theft based on its risk analysis:

a. Signs warning that access to an area is restricted

b. Surveillance cameras

c. Alarms

d. Private security services or patrol officers

4. Insight Global may either apply tracking number tags or engrave tracking numbers on all hardware and Workstations on which ePHI is stored or can be accessed.

FACILITY REPAIRS AND MODIFICATIONS

1. Insight Global does not maintain ePHI on its premises. To the extent that any ePHI is maintained, it is maintained by Covered Workforce Members at the direction of the Client on a Workstation. In light of the scope of Insight Global's operations, it is not reasonable or appropriate for Insight Global to document every repair or modification to the physical components of its facilities. Instead, Insight Global has procedural mechanisms for all of its facilities to ensure that only proper repairs and modifications are made to such facilities.
2. If repairs or modifications are made to Workstations, Insight Global will document such repairs and modifications. The Security Officer will maintain documentation on each repair or modification to a Workstation which includes the following information:
   a. Name of the Workforce Member who authorized the repair or modification;
   b. Date and time of the repair or modification;
   c. Reasons for the repair or modification, including any damage from a Security Incident;
   d. Person(s) performing the repair or modification; and
   e. The outcome of the repair or modification.

Responsibility: Security Officer
Regulatory Category: Physical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.310(a)(1), Facility Access Controls [Standard; Required]
- 45 C.F.R. §164.310(a)(2)(i), Contingency Operations [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(ii), Facility Security Plan [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(iii), Access Control and Validation Procedures [Implementation Specification; Addressable]
- 45 C.F.R. §164.310(a)(2)(iv), Maintenance Records [Implementation Specification; Addressable]

Title: **Workstation Use and Security**	Revision:	Effective Date:

HIPAA Security Rule Language

"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 PHI."

"Implement physical safeguards for workstations that access electronic PHI to restrict access to authorized users."

Purpose Statement

Insight Global's Workstations will be used in a manner that is consistent with Insight Global's business purposes. Insight Global requires the implementation of reasonable physical safeguards to protect all Workstations and other electronic devices that access, store or transmit ePHI from theft or unauthorized use. Insight Global will periodically review, and may modify as appropriate, the permitted and prohibited uses of Workstations and the security controls implemented to protect Workstations in accordance with the Security Risk Management Policy (Procedure No. 11). Insight Global will periodically distribute training and education materials to Covered Workforce Members regarding the use and security of Workstations.

Policy/Procedure

WORKSTATION USE

1. Insight Global's Workstations may only be used for business purposes.
2. The same permissible and prohibited uses of Workstations apply to all Workstations regardless of their location.

WORKSTATION SECURITY

1. Insight Global Covered Workforce Members are required to locate their Workstations in physically secure areas and will physically position their Workstations in ways that minimize unauthorized viewing of ePHI.
2. Covered Workforce Members will not locate Workstations in any of the following locations:
    a. Public walkways
    b. Hallways
    c. Waiting areas
    d. Any other area where unauthorized viewing of ePHI may occur
3. Insight Global will require Covered Workforce Members to have unique user identifiers

and passwords to gain access to their Workstations in accordance with the Information Access Management, Password Management, and Technical Access Controls Policies (Procedure Nos. 14, 17 and 26).

4. Covered Workforce Members must activate Workstation locking software upon leaving a Workstation for more than ten (10) minutes.
5. Covered Workforce Members must log off from their Workstations when their work-day shift is complete.
6. Insight Global will install anti-virus software, which is configured to receive anti-virus updates, on all Workstations in accordance with the Malicious Software Policy (Procedure No. 16).
7. All Workstations provided to Covered Workforce Members will be encrypted in accordance with the Technical Access Controls Policy (Procedure No. 26).
8. These same Workstation security procedures apply to all Workstations regardless of the Workstation's location.
9. Portable Workstations must be physically secured at all times when not in the Covered Workforce Member's immediate possession.

Responsibility: Security Officer; Workforce Members
Regulatory Category: Physical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.310(b), Workstation Use [Standard; Required]
- 45 C.F.R. §164.310(c), Workstation Security [Standard; Required]

Insight Global	HIPAA Security	Procedure No.: **25**
Title: **Device and Media Controls**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility."

Purpose Statement

Insight Global will take reasonable and appropriate steps to control its hardware and Electronic Media containing ePHI throughout the media's entire lifecycle, from initial receipt to final removal. Such control includes reasonably and appropriately protecting, accounting for, storing, and disposing of its hardware and Electronic Media in accordance with specific control procedures and tracking all incoming hardware and Electronic Media and transfers of hardware and Electronic Media as they are moved into, out of, and within its facilities.

Policy/Procedure

INVENTORY AND MOVEMENT OF HARDWARE AND ELECTRONIC MEDIA

1. Insight Global will undertake reasonable efforts to assemble and maintain an inventory of hardware and Electronic Media that contain or provide access to ePHI.
2. Electronic media may include, but is not limited to, the following devices:
    a. Hard disks
    b. Magnetic tapes
    c. Optical storage disks
    d. Compact disks
    e. Videotapes
    f. Audiotapes
    g. Digital memory cards
    h. Floppy disks
    i. Zip drives
    j. USB drives
3. Insight Global will maintain documented records regarding the movement, including, but not limited to disposal, of hardware or Electronic Media that contains ePHI. Documentation regarding the movement of hardware or electronic media will be required only for desktop computers, laptops, and other media storage devices that can

be tracked.

DISPOSAL OF EPHI, HARDWARE AND ELECTRONIC MEDIA

1. ePHI: Insight Global will render ePHI unusable, unreadable, and indecipherable in accordance with the Technical Access Controls Policy (Procedure No. 26).
2. Hardware and Electronic Media
    a. Insight Global will take all reasonable and appropriate steps to remove ePHI from hardware and electronic media prior to the final disposal of the hardware or Electronic Media.
    b. The Security Officer or designee will determine which sanitization method is appropriate for the removal of ePHI from hardware and/or electronic media.
    c. The following sanitization methods may be used to remove ePHI from hardware and/or Electronic Media:
        i. Clearing
            1. Overwrites storage space on the hardware or electronic media with non-sensitive data.
            2. The hardware and/or electronic media type and size may influence whether overwriting is a suitable sanitization method.
            3. Insight Global will consult the National Institute of Standards and Technology (NIST) *Guidelines for Media Sanitization*, Publication 800-88 regarding its recommendations for clearing different media types.
        ii. Purging
            1. Degaussing is an acceptable method of purging.
            2. Degaussing exposes the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.
            3. Degaussing cannot be used to purge nonmagnetic media, such as optical media or compact discs (CDs).
            4. Insight Global will consult the National Institute of Standards and Technology (NIST) *Guidelines for Media Sanitization*, Publication 800-88 regarding its recommendations for clearing different media types.
    d. If hardware and/or Electronic Media cannot be cleared or purged, the only method of disposal is to physically destroy the hardware and/or Electronic Media. Acceptable methods of destroying hardware and/or Electronic Media include:
        i. Disintegration
        ii. Incineration
        iii. Pulverization
        iv. Melting

v. Shredding

e. Insight Global will document the disposal of all hardware and Electronic Media disposal and the steps taken to remove ePHI prior to the disposal of such hardware and Electronic Media.

f. The Security Officer or his or her designee will inspect all hardware and Electronic Media to ensure that all ePHI has been removed from the hardware or Electronic Media prior to disposal.

MEDIA RE-USE

For re-use of hardware and/or Electronic Media (e.g. donation or return of leased hardware), Insight Global will completely and permanently remove ePHI from the hardware and/or Electronic Media in accordance with the Disposal procedures of this Procedure.

Responsibility: Security Officer
Regulatory Category: Physical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.310(d)(1), Device and Media Controls [Standard; Required]
- 45 C.F.R. §164.310(d)(2)(i), Disposal [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(ii), Media Re-Use [Implementation Specification; Required]
- 45 C.F.R. §164.310(d)(2)(iii), Maintenance of Records regarding Movements of Hardware and Media [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **26**
Title: **Technical Access Controls**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R. §164.308(a)(4)."

45 C.F.R. §164.308(a)(4) states, "Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of subpart E of this part."

Purpose Statement

To protect the confidentiality, integrity, and availability of ePHI, Insight Global has taken reasonable and appropriate steps to ensure that its Workstations provided to Covered Workforce Members are installed with technical safeguards to control and restrict access to such Workstations to persons who are authorized to have such access.

Policy/Procedure

Insight Global will implement appropriate technical security controls and methods that permit only authorized persons to access the Workstation and any ePHI contained therein. Such controls and methods include, but are not limited to, the following:

a. Issuance of unique user identifications (user IDs) for each Covered Workforce Member to be used in conjunction with passwords as part of Insight Global's authentication measures.

b. Emergency access procedures that enable authorized Workforce Members to obtain access to necessary ePHI during a disaster or other emergency.

c. Activation of password protected screensaver on Workstations after a designated period of inactivity.

d. Requiring Covered Workforce Members to logoff or lock Workstations upon leaving their work areas.

e. Encryption of all Workstations that contain or may contain ePHI.

Unique User IDs

1. Insight Global will control access to Workstation by assigning each Covered Workforce Member who is granted access to a Workstation, in accordance with the Workforce Member Security and Information Access Management Policy (Procedure No. 14), a unique user ID that:

   a. Identifies the individual Workforce Member; and

b. Permits activities performed on the Workstation to be traced to the individual Workforce Member.

2. The user ID itself should not indicate the individual's access privileges but should be tied to the Workforce Member's privileges.
3. The user ID only allows the Workforce Member to have the appropriate access required to perform his or her job function.
4. User IDs may consist of, but are not limited to:
   a. Workforce Members' names
   b. Workforce Members' employee identification numbers
   c. Biometric identification

EMERGENCY ACCESS PROCEDURE

Insight Global may not need to access ePHI during an emergency or disaster. However, if Insight Global does require such access during an emergency or disaster, Insight Global will follow the procedures outlined in its Contingency Plan (Procedure No. 18) and Emergency Mode Operations Plan (Procedure No. 21) regarding who has access to ePHI.

WORKSTATION SCREENSAVERS

All Workstations provided to Covered Workforce Members will be equipped with screensavers that will automatically activate after a defined period of inactivity. Covered Workforce Members can only deactivate the Workstation screensaver by entering his or her confidential password when prompted.

LOGOFFS

Covered Workforce Members must logoff from or lock their Workstations when their shifts are completed or when they expect to be away from their Workstation for an extended period of time in accordance with the Workstation Use and Security Policy (Procedure No. 24).

ENCRYPTION AND DECRYPTION

1. Based on its risk analysis in accordance with the Security Risk Management Policy (Procedure No. 11), Insight Global will determine when to implement encryption for Workstations and the type and quality of the encryption algorithm and cryptographic key length for data that Insight Global controls and maintains.
2. The Security Officer will approve the encryption mechanism that Insight Global will use.
3. When encryption is used, Insight Global will:
   a. Protect its cryptographic keys against modification and destruction, and protect its private keys against unauthorized disclosure.
   b. Manage the cryptographic keys used to encrypt ePHI stored or maintained on or

accessible through Workstations.

c. Periodically determine activation and deactivation dates for its cryptographic keys.

4. ePHI that is electronically transmitted outside of Insight Global must be encrypted in accordance with the Transmission Security Policy.

Responsibility: Security Officer; Workforce Members
Regulatory Category: Technical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.312(a)(1), Access Control [Standard; Required]
- 45 C.F.R. §164.312(a)(2)(i), Unique User Identification [Implementation Specification; Required]
- 45 C.F.R. §164.312(a)(2)(ii), Emergency Access Procedure [Implementation Specification; Required]
- 45 C.F.R. §164.312(a)(2)(iii), Automatic Logoff [Implementation Specification; Required]
- 45 C.F.R. §164.312(a)(2)(iv), Encryption and Decryption [Implementation Specification; Required]
- 45 C.F.R. §164.312(e)(1), Transmission Security [Standard; Required]
- 45 C.F.R. §164.312(e)(2)(i), Integrity Controls [Implementation Specification; Addressable]
- 45 C.F.R. §164.312(e)(2)(ii), Encryption During Transmission [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **27**
Title: **Integrity**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement policies and procedures to protect electronic PHI from improper alteration or destruction."

Purpose Statement

To safeguard ePHI, it is important to ensure that ePHI has not been altered or destroyed in an unauthorized manner. Therefore, Insight Global will take reasonable and appropriate steps to protect the integrity of ePHI that Insight Global creates, receives, maintains, or transmits.

Policy/Procedure

1. Generally, Covered Workforce Members will have only read-only access to ePHI. If, however, a Covered Workforce Member's job function requires the alteration of ePHI, he or she will be granted read/write access to ePHI by the Client in the Client's information system.
2. Each Client will be responsible tracking and logging any changes to ePHI made by a Covered Workforce Member.
3. Covered Workforce Members will not destroy ePHI without first providing notice to and receiving authorization from the Security Officer in accordance with the Device and Media Controls Policy (Procedure No. 25) or the Client if the ePHI to be destroyed is within the Client's information system.
4. It is not reasonable or appropriate for Insight Global to authenticate ePHI for the following reasons:
   a. The amount of ePHI that Insight Global creates and retains is limited.
   b. Insight Global's level of access to ePHI in the Client's information systems is dictated by the Client and monitored by the Client as part of the Client's HIPAA compliance program.
   c. Insight Global has sufficient policies in place that minimizes the need to authenticate ePHI.

Responsibility: Security Officer
Regulatory Category: Physical Safeguards
Regulatory Reference:

- 45 C.F.R. §164.310(c)(1), Integrity [Standard; Required]
- 45 C.F.R. §164.310(c)(2), Mechanisms to Authenticate Electronic PHI [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **28**
Title: **Person or Entity Authentication**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed."

Purpose Statement

To protect the confidentiality, integrity, and availability of ePHI, Insight Global will maintain a documented process for verifying the identity of any person or entity prior to granting access to ePHI.

Policy/Procedure

1. Insight Global requires the use of user ID and password authentication before access to Workstations is granted.
    a. User IDs are assigned in accordance with the Technical Access Controls Policy (Procedure No. 26).
    b. Workforce Members choose complex and confidential passwords in accordance with the Password Management Policy (Procedure No. 17).
2. Insight Global will not allow redundant authentication credentials.
3. When feasible, Insight Global will mask, suppress, or otherwise obscure the passwords of persons and entities seeking access to ePHI so that unauthorized persons are not able to observe such passwords.
4. Insight Global will limit the authentication attempts of persons and entities seeking access to ePHI a set number of attempts at one time or within an established time period. Authentication attempts that exceed this limit may result in:
    a. Logging of the event for review;
    b. Locking out of the User or Workforce Member; or
    c. Notifying the Security Officer or other appropriate Insight Global official.

Responsibility: Security Officer
Regulatory Category: Technical Safeguards
Regulatory Reference: 45 C.F.R. §164.312(d), Person or Entity Authentication [Standard; Required]

Insight Global	HIPAA Security	Procedure No.: **29**
Title: **Transmission Security**	Revision:	Effective Date:

HIPAA Security Rule Language

"Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network."

Purpose Statement

To ensure the confidentiality, integrity, and availability of ePHI, Insight Global will implement technical security measures to guard against unauthorized access to ePHI while it is transmitted over electronic communications networks.

Policy/Procedure

1. Insight Global requires the encryption of all ePHI that is electronically transmitted outside of Insight Global via email or other electronic transmission mechanisms.
2. Encryption of emails containing ePHI will prevent the unauthorized access of ePHI during transmission.
3. Covered Workforce Members will take all necessary steps to encrypt email through the encryption software pre-loaded on any Workstation provided to a Covered Workforce Member. In the alternative, a Covered Workforce Member may encrypt email using the Client's systems if the email is transmitted through the Client's system and the Client's system is known to have appropriate substitute encryption.
4. Covered Workforce Members who fail to activate the encryption mechanism for emails containing ePHI will be sanctioned in accordance with the Workforce Member Discipline Policy.

Responsibility: Security Officer; Workforce Members
Regulatory Category: Technical Safeguards
Regulatory Reference:

- 45 C.F.R. §312(e)(1), Transmission Security [Standard; Required]
- 45 C.F.R. §312(e)(2)(i), Integrity Controls [Implementation Specification; Addressable]
- 45 C.F.R. §312(e)(2)(ii), Encryption During Transmission [Implementation Specification; Addressable]

Insight Global	HIPAA Security	Procedure No.: **30**
Title: **Availability**	Revision:	Effective Date:

HIPAA Security Rule Language

"Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."

Purpose Statement

Insight Global will make all documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Policy/Procedure

1. Insight Global will make the following documentation available:
    a. Policies and procedures regarding the security of ePHI and Workstations.
    b. All documentation that records any updates, revisions, modifications, or deletions made to existing Security Policies and Procedures.
    c. All policies and procedures no longer in effect for a certain Security Regulation requirement or implementation specification.
    d. Any other documentation that the Security Officer deems appropriate to retain and to make available to its Covered Workforce Members regarding Insight Global's Security Policies and Procedures.
2. The Security Officer will be responsible for ensuring that such documentation as required by the HIPAA Security Regulations is made available to its Covered Workforce Members and Users.
3. All documentation specified in this policy will be available on Insight Global's intranet and will be maintained for six years from the date of creation.

Responsibility: Security Officer
Regulatory Category: Policies, Procedures, and Documentation
Regulatory Reference: 45 C.F.R. §164.316(b)(2)(ii), Availability [Implementation Specification; Required]