Cognixia
A Digital Workforce Solutions Company

# HIPAA Compliance

- **What is HIPAA?**

**HIPAA = Health Insurance Portability and Accountability Act (1996)**

- Protects health insurance coverage for workers and their families when they change or lose their jobs (prevents pre-existing condition limitations when new coverage is obtained within 62 days of losing other similar creditable coverage)
- Administrative Simplification (AS) — requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.
- AS also addresses the security and privacy of health data.

**HIPAA Compliance**

HIPAA defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information as well as outlining numerous offenses relating to health care and sets civil and criminal penalties for violations.

Employers, like Collabera, who offer health plan coverage, must comply with HIPAA.

Our clients, all large employers who offer health plan coverage, must also comply with HIPAA.

Some of our clients such as IBM face a unique challenge as it relates to HIPAA because their clients are not just employers who must comply with HIPAA if they offer a medical plan - their clients may actually be in the health care industry. There is where you come in if and when you may be working on a project for IBM's end client who may be an insurance carrier or a health care provider such as a hospital group.

These rules apply to "covered entities" as defined by HIPAA and the HHS.

Covered entities include health plans, health care clearinghouses, such as billing services and community health information systems, and health care providers that transmit health care data in a way that is regulated by HIPAA.

Five rules regarding AS:

1. the Privacy Rule,
2. the Transactions and Code Sets Rule,
3. the Security Rule,
4. the Unique Identifiers Rule, and
5. the Enforcement Rule.

## 1. The Privacy Rule

What is PHI?

PHI = Protected Health Information

PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of an individual's medical record or payment history.

## 2. Transaction and Code Sets Rule

HIPAA-covered health plans are now required to use standardized electronic

transactions:

- used to submit health care claim billing information,
- used to submit retail pharmacy claims to payers by health care professionals who dispense medications, either directly or via intermediary billers and claims clearinghouses,
- used to make a payment, send an Explanation of Benefits (EOB),
- send an Explanation of Payments (EOP) remittance advice, or make a payment and send an EOP remittance advice only from a health insurer to a health care provider either directly or via a financial institution,
- used to define the control structures for a set of acknowledgments to indicate the results of the syntactical analysis of the electronically encoded documents.

The size of many fields {segment elements} will be expanded, causing a need for all IT providers to expand corresponding fields, element, files, GUI, paper media and databases.

## 3. The Security Rule

The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical.

- Administrative Safeguards — policies and procedures designed to clearly

show how the entity will comply with the act

    - Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
    - The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.

- Procedures should clearly identify consultants or classes of consultants who will have access to electronic protected health information (EPHI). Access to EPHI must be restricted to only those consultants who have a need for it to complete their job function.
- The procedures must address access authorization, establishment, modification, and termination.
- Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to consultants performing health plan administrative functions.
- Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
- A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

**Physical Safeguards — controlling physical access to protect against inappropriate access to protected data**

- Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
- Access to equipment containing health information should be carefully controlled and monitored.
- Access to hardware and software must be limited to properly authorized individuals.
- Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.

- Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

**Technical Safeguards** — controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

- Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
- Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems.
- Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
- In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
- Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

### 4. Unique Identifiers Rule (National Provider Identifier)

HIPAA covered entities such as providers completing electronic transactions, healthcare clearinghouses, and large health plans, must use only the National Provider Identifier (NPI) to identify covered healthcare providers in standard transactions. All covered entities using

electronic communications (e.g., physicians, hospitals, health insurance companies, and so forth) must use a single new NPI.

The NPI replaces all other identifiers used by health plans, Medicare, Medicaid, and other government programs. However, the NPI does not replace a provider's DEA number, state license number, or tax identification number. The NPI is unique and national, never re-used, and except for institutions, a provider usually can have only one. An institution may obtain multiple NPIs for different "subparts" such as a free-standing cancer center or rehab facility.

### 5. Enforcement Rule

This rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations.

### Your Responsibilities at Client or End Clients' Sites

Our consultants' responsibilities can vary greatly from client site to client site depending upon if the client or end client is a covered entity (e.g. insurance company) or not.

If a covered entity, great responsibility would be on the shoulders of the client management, their employees having access to PHI, their IT management, etc. However, being a technical consultant and having access to the client's h/w that stores the PHI or s/w that processes PHI is why you have a responsibility for HIPAA compliance. The following areas are where you may have a role in maintaining the security of PHI at a client site:

- Access to equipment containing health information should be carefully controlled and monitored.
- Access to hardware and software must be limited to properly authorized individuals.
- Workstations should be removed from high traffic areas, if possible, and monitor screens should not be in direct view of the public or to those not authorized to have access to PHI.
- Covered entities should train their contingent workforce (our consultants) on their physical access responsibilities. Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- Ensure that the data you are working with has not been changed or erased in an unauthorized manner.
- Ensure data integrity as appropriate - data corroboration, including the use of check sum, double-keying, message authentication, and digital signature.
- Covered entities, on whose projects you may be working, must also authenticate entities with which they communicate. Authentication consists of corroborating that

an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems.

- In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
- Take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

**Process for When a Breach of PHI is Suspected or Discovered**

A breach is defined as the "unauthorized acquisition, access, use, or disclosure" of PHI that can compromise the privacy and/or security of this information. If, however, the PHI is "unusable, unreadable, or indecipherable", no notification is required.

Should there be a breach of confidential employment or health plan participant data at a client or end client site, the consultant is to report it immediately (within no more than 1

hour of discovering the breach) to their client manager as well as to Collabera's Privacy Official at 973-889-5200 or to: hrusaoffice@collabera.com

Collabera's Privacy Official will in turn notify the Sales Head for that client. The Privacy Official will conduct an investigation with our Legal Department to determine:

- How the breach occurred
- The consultant(s) involved
- The number of records or files breached
- The nature of the exposure
- Work with client to attempt to retrieve the data breached from recipients
- Work with end client in the notification to those affected by the breach and
- Initiate corrective action against those responsible as appropriate.

**Sanction Policy for Breach**

Depending upon the seriousness of the breach and the consultant's role in that breach, the appropriate corrective action will be administered by the Corporate Human Resources Dept.

**Types of Offenses**

**Category A offenses - including, but not limited to**:

- accessing PHI that one does not need to have access to as part of their job function,
- divulging one's user name & password,

- leaving one's computer unattended while logged into a system displaying PHI data,
- sharing or discussing PHI with another individual without authorization and/or who does not have need-to-know access,
- copying PHI without requisite approval(s),
- editing or modifying PHI without requisite approval(s)
- discussing PHI in a public area where others could hear or ¢ failing to cooperate with an investigation for breach of PHI.

**Category B offenses - including, but not limited to:**

- includes a second offense of any Category A offense (does not have to be a repeat offense), * unauthorized use or disclosure of PHI,
- accessing another's computer, client's system or using another's user name & password) or
- failing to comply with an investigation's corrective action or recommendation.

**Category C offenses - including, but not limited to:**

- includes a third offense of any Category A offense (does not have to be a repeat offense),
- second offense of any Category B offense (does not have to be a repeat offense),
- obtaining PHI under false pretenses; or
- using or disclosing PHI for financial or material gain, personal use or other malevolent purpose.

**Types of Sanctions**

**Category A — including, but not limited to:**

- verbal warning,
- written warning,
- retraining on Collabera's HIPAA training,
- retraining on Collabera's Privacy Policy and how it impacts consumers, consultant, consultant's department, the Company and Company's clients; or
- retraining on the proper procedures for protecting PHI and other company confidential information and the use of any HIPAA required forms.

**Category B - including, but not limited to:**

- written warning, retraining on Collabera's HIPAA training,

- retraining on Collabera's Privacy Policy and how it impacts consumers, consultant, consultant's department, the Company and Company's clients,
- retraining on the proper procedures for protecting PHI and other company confidential information and the use of any HIPAA required forms; or
- suspension of minimum of one (1) day or a maximum of three (3) days.

**Category C - including but not limited to:**

- termination of employment, civil penalties as provided under HIPAA or other applicable local/state/federal law or criminal penalties as provided under HIPAA or other applicable local/state/federal law.
- Upon conclusion of the investigation regarding a breach, the consultant(s) involved will be contacted by Corporate Human Resources to learn of the corrective action to be taken.

HIPAA COMPLIANCE TRAINING ACKNOWLEDGEMENT

| acknowledge that | have received, read and understood this Collabera HIPAA Compliance Training. | agree to abide by the HIPAA regulation and its corresponding policy and processes as it relates to my job as a Consultant assigned to Collabera's client's or end client's project:

Consultant's Printed Name:-

Signature:-

Date:-