# HIPAA PRIVACY POLICY

As a global IT and business consulting services organization, CGI is committed to maintaining levels of protection of personal data aligned to best practices in the industry which, at a minimum, comply with the requirements of the applicable data protection legislation, as defined below, and CGI's contractual obligations.

This HIPAA Privacy Policy is an extension of CGI's Data Privacy Policy and is applicable when CGI processes Protected Health Information (PHI), a.k.a. individually identifiable Health Information (IIHI) as a Business Associate (to a Covered Entity) or a Business Associate (subcontractor) to other Business Associates.

CGI may become a Business Associate when it receives PHI from a Covered Entity or another Business Associate. Business Associate relationships should, but may not always, be documented with a Business Associate Agreement. This policy will apply whether or not a formal Business Associate Agreement exists.

This policy explains CGI's responsibilities with regard to the use, disclosure, and protection of PHI in accordance with the terms of Business Associate Agreements and HIPAA and is binding upon all Members of CGI Legal Entities that process PHI, regardless of their location and their relationship to a BU, SBU, or Corporate Functions.

## Key Definitions

- **Business Associate**: A person or entity that creates, receives, maintains or transmits protected health information on behalf of a Covered Entity or other Business Associate. Defined in 45 CFR 160.103.
- **Business Associate Agreement or BA Agreement**: A formal written contract between CGI and a Covered Entity or between CGI and another Business Associate that requires both parties to comply with specific requirements related to PHI. Business Associate Agreements may have requirements beyond those imposed by statute or regulation.
- **CGI Legal Entities**: All legal entities controlled directly or indirectly by CGI Inc., excluding any legal entities that are within the operational scope of CGI Federal.
- **Covered Entity**: A health plan, healthcare provider, or healthcare clearinghouse that must comply with HIPAA. Defined in 45 CFR 160.103.
- **Designated Record Set**:

(1) 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.

(2) For purposes of this paragraph, 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.

Defined in 45 CFR 164.501.

- **HIPAA**: Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including the Standards for the Privacy of Individually Identifiable Health Information, at 45 CFR Parts 160 and 164 ("Privacy Rule"), and the Security Standards, at 45 CFR Parts 160 and 164 ("Security Rule"), as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH), and any applicable associated federal rules and regulations.

- **Process, Processing, Processed**: Any exposure to, contact with, operation performed on, or set of operations performed on PHI whether or not by automated means, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting (including via remote access), using, disclosing, disseminating or otherwise making available, aligning, combining, restricting, erasing, destroying, or otherwise handling.

- **Protected Health Information or PHI**: All "individually identifiable health information" (as defined in this paragraph) about an individual's past, present or future physical or mental health, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual. Health information is deemed to be individually identifiable health information under HIPAA if it contains any of the following Individual Identifiers: name, date of birth, address, zip code, telephone number, diagnosis codes, dates of service, admission date, discharge date, date of death, age, member/patient numbers, social security numbers, certificate/license numbers, emails, URLs IP address numbers, images, finger prints, or other biometric markers. Defined in 45 CFR 164.103.

- **Electronic Protected Health Information (ePHI)**: Protected health information (PHI) that is produced, saved, transferred or received in an electronic form. Defined in 45 CFR 160.103.

- **Reproductive Healthcare**: Healthcare that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes.

- **Security Incident**: An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Defined in 45 CFR 164.304.

- **Substance Abuse Records**: Substance Abuse Records Defined in 42 CFR part 2, updated and effective April 16, 2024.

- **Unsecured Protected Health Information**: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. Defined in 45 CFR 164.402.

## HIPAA Privacy Rule

The Privacy Rule establishes national protection for the privacy of protected health information (“PHI”), and applies to three types organizations, known as Covered Entities: health plans, health care clearinghouses, and health care providers. The Privacy Rule requires that Covered Entities and Business Associates (CGI), as defined above, implement policies and procedures to protect and guard against the misuse of PHI. This policy reflects our commitment to compliance with the Privacy Rule.

## HIPAA Security Rule

The Security Rule establishes national standards for securing patient data that is stored or transferred electronically.

The rule requires the implementation of safeguards, both physical and electronic, to ensure the secure passage, maintenance and reception of ePHI.

Enforced by the Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS), the Security Rule aims to protect patient security while still allowing the health care industry to advance technologically.

## Use and Disclosure of PHI

We may use PHI to meet our management, administration, data aggregation and legal obligations to the extent such use of PHI is permitted or required by the BA Agreement and not prohibited by law. We may use or disclose PHI on behalf of, or to provide services to, Covered Entities for purposes of fulfilling our service obligations to them, if such use or disclosure of PHI is permitted or required by the BA Agreement and would not violate HIPAA. The specific BA Agreement for any given Covered Entity should be consulted and reviewed by everyone working for that Covered Entity to ensure compliance.

In the event that PHI must be disclosed to a subcontractor or agent, we will ensure that the subcontractor or agent agrees to abide by the same restrictions and conditions that apply to us under the BA Agreement with respect to PHI, including the implementation of reasonable and appropriate safeguards, prior to disclosure.

Anytime we process, including use or disclose, PHI, we should make reasonable efforts to limit the PHI processed to only the minimum information necessary for the purposes at issue.

We may also use PHI to report violations of law to appropriate federal and state authorities.

Potential for information permissibly disclosed to be redisclosed and no longer protected by HIPAA.

## Safeguards

We use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for in the BA Agreement. We have implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that we create, receive, maintain, or transmit on behalf of a Covered Entity. Such safeguards include but are not limited to:

- Maintaining appropriate clearance procedures and providing supervision to assure that our workforce follows appropriate security procedures;
- Providing appropriate training for our staff to ensure that our staff complies with our security policies;
- Limiting internal disclosures of PHI to only those members of our staff that need to access the PHI to perform their job duties;
- Making use of appropriate encryption when transmitting PHI over the Internet;
- Utilizing appropriate storage, backup, disposal and reuse procedures to protect PHI;
- Utilizing appropriate authentication and access controls to safeguard PHI;
- Utilizing appropriate security incident procedures and providing training to our staff sufficient to detect and analyze security incidents; and
- Maintaining a current contingency plan and emergency access plan in case of an emergency to assure that the PHI we hold on behalf of a Covered Entity is available when needed.

## Retention, Disposal and Storage

The following guidance should be utilized when working with and at the direction of the Covered Entity to ensure appropriate retention of PHI:

- PHI contained in the Designated Record Set (to be defined by the Covered Entity or Business Associate) will be retained according to the longer of state and federal regulations.
- PHI, including medical and financial records contained in the Designated Record Set, will be retained for a minimum of six years, as required by the Privacy Rule.
- In the absence of state law specifying a greater retention period, medical records must be retained for at least six years.
- For minor residents (persons who have not reached full legal age), medical records must be retained for three years after the minor reaches legal age under state law or six years from the date of discharge, whichever is longer.
- Medical records in connection with which there may be pending litigation may be exempt from scheduled destruction at the discretion of Covered Entity.
- If state laws and regulations require a greater retention time period, the greater will be followed.

## HIPAA Data Breach

In the event of a breach, please follow CGI's Security Monitoring and Response Standard. A privacy or security breach occurs when there has been an acquisition, access, use, or disclosure of unsecured PHI that compromises the security or privacy of the information.

Under HIPAA and for purposes of this Policy, a breach does not include:

- An unintentional acquisition, access, or use of PHI by a workforce member or other person acting under the authority of a Covered Entity (Client) or Business Associate, if the acquisition, access, or use was made in good faith and within the scope of the workforce member's authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.

- An inadvertent disclosure by a person who is authorized to access PHI (at a Covered Entity or Covered Entity's Business Associate to another person authorized to access PHI at Covered Entity or Covered Entity's Business Associate, or organized healthcare arrangement in which Covered Entity participates), and information received as a result of such a disclosure is not further used or disclosed in a manner not permitted by the privacy rule.

- Disclosure of PHI where the Covered Entity or the Covered Entity's Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

A breach is presumed to have occurred if there is an unauthorized access, acquisition, use, or disclosure of unsecured PHI, unless the Covered Entity can demonstrate a low probability that the information was compromised.

In the event a breach has occurred, the Covered Entity or at the direction of the Covered Entity (Client), CGI must notify the individuals whose information was breached and the Secretary of the U.S. Department of Health and Human Services, in accordance with the HIPAA breach notification rules and this Policy. In some cases, Covered Entity may be required to notify the news media.

CGI seeks to maintain strong relationships with data protection authorities. As such, CGI will cooperate with data protection authorities that have jurisdiction over the relevant PHI in relation to HIPAA related requests.

If you suspect a breach, follow CGI's Incident reporting process and identify the details related to the potential HIPAA breach. The US CSG Privacy team will ensure the correct review, process, and notification requirements are followed.

## Mitigation of Harm

In the event of unauthorized use or disclosure of PHI, i.e., use or disclosure that is not authorized in the BA Agreement, we must mitigate, to the extent practicable, any harmful effect resulting from the disclosure. Such mitigation should include:

- Reporting any use or disclosure of PHI not provided for by the BA Agreement and any security incident of which we become aware to the Covered Entity; and
- Documenting such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosure of PHI in accordance with HIPAA.

## Access to PHI

As should be noted in each BA Agreement, we will make available to Covered Entities, information necessary for the Covered Entity to give individuals their rights of access, amendment, and accounting in accordance with HIPAA.

Upon request, we will make our internal practices, books, and records including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of a Covered Entity available to the Covered Entity or the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the terms of the BA Agreement and HIPAA.

CGI will also make available to the Covered Entity information required for the Covered Entity to provide an accounting of disclosures.

## Reproductive Health Care

CGI complies with the HIPAA Privacy Rule to Support Reproductive Health Care Privacy and will follow the heightened privacy protections for protected health information involving reproductive healthcare. The Final Rule establishes a ban on the use or disclosure of PHI by a HIPAA covered entity (i.e., healthcare provider, health plan, healthcare clearinghouse) or their business associates (BAs) for any of the following:

- Investigations. Criminal, civil, or administrative investigations into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare.
- Imposing liability. Imposing criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare.
- Identification. Identifying any person for any purpose described above.

The prohibition applies only when a covered entity or BA has reasonably determined that one or more of the following conditions exist:

- The reproductive healthcare is lawful in the state in which it is provided. For example, the prohibition will apply if a resident of one state traveled to another state for an abortion that is lawful in the state where the healthcare was provided.
- The reproductive healthcare is protected, required, or authorized by federal law, including the US Constitution, regardless of the state in which it is provided. For example, the prohibition applies to PHI that relates to contraception, which is protected by the Constitution.
- The presumption described below applies.

The prohibition doesn't apply to the use or disclosure of PHI for purposes otherwise permitted under the HIPAA privacy rule, although an attestation may be required. In the preamble, HHS provides examples of other purposes to which the prohibition doesn't apply, such as for:

- Public health activities, investigations into sexual assault, human and sex trafficking, or child abuse, or professional misconduct or licensing inquiries when required by law
- Investigations of alleged violations of federal nondiscrimination laws or abusive conduct in connection with reproductive healthcare (for example, sexual assault allegations against a provider)

The Final Rule defines reproductive healthcare for purposes of the HIPAA privacy rule as healthcare that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes.

## ATTESTATION

A covered entity or BA must obtain a written attestation that the information is not for a prohibited purpose before PHI potentially related to reproductive healthcare can be used or disclosed in the following circumstances:

- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Disclosures to coroners and medical examiners to identify a deceased person, determine cause of death, or other duties as authorized by law

Disclosure for these purposes is permissive, not mandatory under HIPAA, except in instances where HHS requests information as part of a compliance investigation.

A valid attestation must contain the following:

- A description of the information requested, including the name of any individual(s) whose PHI is sought, or, if that's not practicable, a description of the class of individuals whose PHI is sought.
- The name of the person who has been asked to make the PHI use or disclosure and the name of the person to whom it should be made.
- A statement that obtaining, using or disclosing individually identifiably health information in violation of HIPAA may be subject to criminal penalties.

In addition, the attestation must be in plain language, signed by the requester, and must clearly state that the PHI is not for "criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive healthcare." It may be completed electronically.

## Substance Abuse Records (SUD)

CGI complies with the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations ("Part 2 rules") final rule published in 2024. SUD treatment records, or testimony relaying the content of such records, will not be used or disclosed in civil, criminal, administrative or legislative proceedings against the individual absent patient consent or a court order.

## Modification of Records

CGI is not the owner of the records provided to the Covered Entity; as such, CGI is not responsible for making any record modifications. Should any individual contact CGI for such corrections, the request should be submitted to the required Covered Entity with copy to the US CSG Privacy team.

## Privacy and Security Officers

Under HIPAA both the Privacy Rule and the Security Rule require that we designate a person or persons who will serve as our "Privacy Officer" and "Security Officer" who is responsible for the development and implementation of our privacy policies and procedures. The US CSG Privacy team will serve as the designate for these roles as it relates to HIPAA policies and procedures.

Questions regarding HIPAA may be submitted to privacy.uscsg@cgi.com

## Reporting and Sanctions

Any member who suspects or identifies potential or actual non-compliance with this policy should report the relevant information to the HIPAA Privacy Officer. No adverse action will be taken against any attorney or staff person for making such a report. Such reports should be submitted to privacy.uscsg@cgi.com.

To the extent permitted by law, any violation of this HIPAA Privacy Policy may result in administrative and/or disciplinary action by CGI (including monetary penalties, suspension or termination).

## Training

All members and contractors who may come in contact with PHI on behalf of a client (Covered Entity) or Business Associate (where CGI is a subcontractor/Business Associate) are required to take either the client's,

other Business Associate's (if CGI is subcontractor) or CGI's specific HIPAA Training. Records must be kept of training completion if done using CGI's HIPAA Training. Members and contractors are made aware of their responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the reviewing process detect a Member's or contractor's failure to comply with organizational policies.

HIPAA requires training for individuals as per 45 CFR §164.530 and 45 CFR §164.308.

PROCEDURE

- A Project Manager monitors their team's training history and submits member names to the BU Operations.
- Operations submits the individual's name, email address, and employee ID via an HR Service Request.
- Members identified via an HR Service Request are assigned the appropriate Learning Program.
- CGI's HIPAA training is delivered through CGI Academia on an annual basis.
- CGI's HIPAA Privacy Officer will complete review of the HIPAA training file in Academia, no less than once every 12 months to ensure all submitted members have completed training as assigned.

## Policy Owner

US HIPAA Privacy Officer

## Effective Date

February 23, 2023

## Revision History

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 2022-11-10 | Data Privacy | Initial US CSG HIPAA Privacy Policy - Internal |
| 1.1 | 2023-02-23 | Data Privacy/Legal | Review updates provided by legal and finalize for publication. |
| 1.2 | 2024-06-24 | Data Privacy/Security | Annual review US CSG Privacy and Security. Combined Public and Internal policy into a single public facing HIPAA privacy policy. |
| 1.3 | 2024-10-03 | Data Privacy/ Benefits | Updates related to HIPAA Final Rule changes for SUD and Reproductive Health care. |