HIPAA BUSINESS ASSOCIATE PRIVACY POLICY

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

This policy shall apply when CGI handles or comes in contact with Protected Health Information (PHI), a.k.a. Individually identifiable Health Information (IIHI) as defined by HIPAA, as either a Business Associate (to a Covered Entity) or a Business Associate (subcontractor) to other Business Associates.

All of the requirements in this policy are also flowed down to Business Associates/subcontractors to CGI.

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

This policy is provided to help you better understand how CGI uses, discloses, and protects PHI in accordance with the terms of Business Associate Agreements and/or HIPAA.

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.
- 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.
- Covered Entity: A health plan, healthcare provider, or healthcare clearinghouse that must comply with HIPAA.
- 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.
- Protected Health Information or PHI: PHI means 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.

Use and Disclosure of PHI

We may use PHI for 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 and Business Associates 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.

In the event that PHI must be disclosed to a subcontractor or agent, we will require the subcontractor or agent 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.

Anytime we use or disclose PHI, we will make reasonable efforts to limit the PHI disclosed 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.

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 electronic 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 assure 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.

Mitigation of Harm

In the event of an unauthorized use or disclosure of PHI due to CGI's violation of the requirements of the BA Agreement, CGI will mitigate, to the extent practicable, any harmful effect resulting from the use or disclosure. Such mitigation will include:

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

Access to PHI

As provided in the 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 regulations.

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 regulations.

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

Modification of Records

CGI is not the owner of the records as the Business Associate, therefore, CGI is not responsible for making any record modifications. Should any individual contact CGI for such corrections, the request will be submitted by CGI to the applicable Covered Entity or Business Associate.

Privacy and Security Officers

HIPAA requires 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.

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

Additional CGI Privacy Policies and Notices
CGI Privacy Policy
Binding Corporate Rules
Web Privacy Notice
California Notice