TEEMA

PRIVACY POLICY

Table of Contents

1.0 PURPOSE AND SCOPE. TEEMA has legal obligations under relevant regulations, acts, and other legislation and standards of practice, for the custody or control of Personal Health Information ("PHI"). The purpose of this Privacy Policy is to provide consistent standards to ensure that Members and Consultants of TEEMA are aware of and acknowledge these obligations to protect PHI and other confidential information under the custody and control of TEEMA or under the custody and control of any other associate, client or customer that TEEMA provides services to and to which TEEMA Members and/or Consultants have access to while performing their role.

This Policy applies to all TEEMA staff, personnel, Members, and Consultants, and all Personal and Confidential Information regardless of format or how it is stored or recorded. This Policy applies while in the course of working and conducting business for on behalf of TEEMA, including when off-duty, and extends beyond the completion of the employment or business relationship with TEEMA or a TEEMA associate, client or customer.

2.0 KEY DEFINITIONS.

Business Associate (BA): Under the HIPAA Privacy and Security Rules, a person (or entity) who is not a member of the covered entity's workforce and who performs any function or activity involving the use or disclosure of individually identifiable health information or who provides services to a covered entity that involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc.

Business Associate Agreement (BAA): Under the HIPAA Privacy and Security Rules, a legally binding agreement entered into by a covered entity and business associate that establishes permitted and required uses and disclosures of protected health information (PHI), provides obligations for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation. Refer to 45 CFR § 164.502(e)(1) to determine when the standard is not applicable.

Confidential Business Information: Any Corporate-related, financial or administrative information. This includes information stored on all forms of media including but not limited to, paper, electronic, magnetic, optical disc and microfiche. For purposes of this Policy, all Confidential Business Information is also contained within the definition of Protected Health Information.

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media. For purposes of this Policy, all ePHI is also contained within the definition of Protected Health Information.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Examples of PHI include, but are not limited to:

- An individual's name, address, telephone number, personal healthcare number;
- An individual's race, national or ethnic origin, color or religious beliefs or associations;
- An individual's age, sex, sexual orientation, marital or family status;
- An individual's fingerprints, blood type or inheritable characteristics;
- Information about the individual's health care history, including physical or mental disability;
- Information about an individual's education, financial, criminal or employment history; and
- Opinions about an Individual.

PHI can be recorded in any format, including books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means.
Relevant Laws: includes, but is not limited to, the laws, legislation, regulations and other legal obligations TEEMA must abide by when dealing with PHI (*See* Appendix II).
Staff: Includes but is not limited to: Members, Consultants, Business Associates, Employees, and Owners that are in a business or employment relationship with TEEMA.

3.0 POLICY

3.1 Accountabilities.

Governance: Accountability for TEEMA compliance with this Policy rests with the Compliance Team, although other Staff is responsible for day-to-day collection and processing of PHI. Members have a responsibility to oversee compliance with this Policy by Staff within their area(s) of responsibility.

All members of Staff have responsibility to ensure that appropriate steps are taken to protect PHI at all times. They must ensure that their practices in collecting, accessing, using or disclosing PHI comply with this Policy as well as with statutory requirements and their professional codes of practice. In addition, Staff are expected to report to the TEEMA Compliance Team any concerns with or recommended improvements to information privacy and security procedures, and any information to help resolve problems.

3.2 Acknowledgement of Confidentiality. TEEMA will make all Staff aware of the importance of maintaining the confidentiality of PHI. As a condition of employment or affiliation, all new Staff must read this Privacy Policy and sign an approved Confidentiality Acknowledgement (*see* Appendix I). In addition, PHI obtained in the course of one's employment or other affiliation with TEEMA must be held in confidence even after the affiliation comes to an end.

3.3 Failure to Comply. Failure to comply with this Policy may result in disciplinary action including, but not limited to, the termination of employment or relationship with TEEMA, prosecution and restitution for damages.

3.4 Business Associates & Business Associate Agreements. TEEMA's Compliance Team is responsible for facilitating the assessment of both existing and future vendor/business relationships to determine whether the relationship meets the criteria for a HIPAA Business Associate Agreement (BAA). When a Business Associate agreement exists, the Compliance Team shall contact the responsible individual/team to initiate a BAA document.

3.5 Collection of PHI. The collection of PHI is governed by Relevant Laws and must be limited to what is needed to fulfill the purposes identified.

3.6 Accuracy of PHI. Staff must take all reasonable steps to ensure the accuracy and completeness of any PHI they collect or record and be diligent to protect against making any errors due to carelessness or other oversights.

3.7 Access, Use, Disclosure or Sharing of PHI. Staff is only authorized to access, use, disclose or share PHI for legitimate purposes and only when necessary to perform their job functions and responsibilities. Where necessary, Staff shall disclose only the minimum PHI necessary to performing or fulfilling a specific required or permitted function.

3.8 Release of Information. No Staff may release PHI about an individual to any Party unless expressly authorized by the Relevant Laws.

3.9 Security of Information. TEEMA is committed to maintaining the security of PHI and other sensitive information, including appropriate physical security of records and security safeguards for computer and network systems. Staff are expected to comply with TEEMA security requirements developed for use of such systems. All Staff have the responsibility to protect against unauthorized access and disclosure of PHI. This responsibility includes ensuring that access or disclosure is only made to or by authorized individuals and reasonable measures are taken to prevent any unauthorized access, disclosure, loss or theft of information.

3.10 Retention and Destruction of PHI. Records will be retained in accordance with all Relevant Laws, as well as with any TEEMA record retention policies. Staff holding records containing PHI are expected to identify retention times and then follow the TEEMA guidelines and procedures for the secure destruction of PHI that is no longer required to ensure the information is destroyed, erased or made anonymous.

3.11 Compliance Monitoring. Access, use, disclosure and sharing of PHI will be monitored and all suspected breaches of this Policy will be investigated by the Compliance Team. This includes any software, applications, or systems designed to monitor remote device encryption and activity. Any disciplinary actions to be taken will be determined by the Compliance Team and/or Managing Partners according to the nature of the breach and parties involved. TEEMA operational areas and programs must conduct appropriate reviews and audits of their systems and processes to ensure compliance with TEEMA policies and standards.

3.12 Breach of Policy. Staff are expected to report any real or suspected breaches of this Policy within two (2) days of discovery. All reports must be made to the Compliance Team at compliance@teemagroup.com. Staff may report real or suspected breaches without any fear of reprisal. All incidents involving theft or loss of PHI will be promptly addressed for containment, investigation, reporting, remote destruction and remedial actions.

4.0 PROCEDURES

4.1 General Inquiries. Questions or concerns about collection, access, use or disclosure of PHI, reports of privacy breaches or loss of information should be directed to the Compliance Team.

4.2 Confidentiality Acknowledgments. The Compliance Team is responsible for obtaining and holding Confidentiality Acknowledgements for all Staff.

5.0 APPENDICES

5.1 Appendix I: Confidentiality Acknowledgement

5.2 Appendix II: Relevant Laws

APPENDIX I
CONFIDENTIALITY ACKNOWLEDGEMENT

In consideration of my relationship with TEEMA, I acknowledge and agree as follows:

1. I have read, understand and will adhere to this Privacy Policy and related policies as amended from time to time, concerning the collection, use and disclosure of PHI, as defined herein and in the Relevant Laws, obtained in the course of my relationship with or provision of services to TEEMA;
2. I understand that all PHI is confidential and may not be communicated to anyone in any manner, except as authorized by TEEMA, or Relevant Laws;
3. I understand and acknowledge that all information regarding TEEMA, including corporate, financial and administrative records, is confidential and may not be communicated or released to anyone in any manner except as authorized by TEEMA, or applicable policies;
4. I understand I must protect all PHI in my possession from theft or loss. This includes but is not limited to, keeping the information with me at all times, storing it in a locked and secured area when unattended, and encrypting and password protecting it when stored on electronic mobile devices (e.g. USB drives, laptops, etc.);
5. I will not copy, alter, interfere with, destroy or remove any confidential information or records except as authorized by TEEMA in accordance with established policies;
6. I understand that access to PHI is only for the purpose of and limited to what is required to perform my role. I will not access my record or those of family, friends or others, unless I am directly involved in providing care or other services to the individual the information is about;
7. I will immediately report to the Compliance Team the potential or actual unauthorized disclosure or loss of any PHI;
8. I understand that compliance with this Policy is a condition of my relationship, employment or service contract with TEEMA and that failure to comply may result in immediate termination of my employment or services, in addition to legal action by TEEMA and/or others.

By accepting these terms, I am confirming that I acknowledge, understand and agree to the above.

_____
Signature

_____
Name

_____
Date

APPENDIX II
RELEVANT LAWS: Excerpts & Links

The following is a non-exclusive list of relevant laws, regulations, etc. that TEEMA is legally or contractually bound to abide by when handling PHI. This list is merely for reference and may change from time to time.

EU-U.S. Privacy Shield Frameworks: The EU-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

> *Onward Data Transfer Agreement – The Framework requires in Principle 3 b that in order to transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.*

Link: https://www.privacyshield.gov/welcome

Freedom of Information and Protection of Privacy Act ("FIPPA"): An information rights law that gives an individual a legal right of access to records held by relevant Canadian public bodies, subject to specific and limited exceptions.
Links: http://www.bclaws.ca/civix/document/id/consol26/consol26/96165_00; http://www.gov.mb.ca/chc/fippa/index.html; https://www.ontario.ca/laws/statute/90f31; http://www.servicealberta.ca/foip/; https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Health Insurance Portability and Accountability Act ("HIPAA"): National standard in the United States to protect individual medical records and other personal health information and applies to health plans, healthcare clearing houses, and those health care providers that conduct certain healthcare transactions electronically. TEEMA is contractually bound to be HIPAA Compliant as a Business Associate.
Link: https://www.hhs.gov/hipaa/for-professionals/index.html

Health Information Technology for Economic and Clinical Health ("HITECH"): National act enacted to promote the adoption and meaningful use of health information technology. Often lumped into the definition and regulations of HIPAA. TEEMA is contractually bound to abide by HITECH standards as a Business Associate in the same manner as HIPAA.
Link: https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/

Personal Information Protection and Electronic Documents Act ("PIPEDA"): Federal privacy law in Canada for private-sector organizations that sets out the ground rules for how businesses must handle personal information in the course of commercial activity.
Link: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/