

PRIVACY POLICY

I. Policy

It is the **policy** of Cardiac Surgical Associates of Western Mass, P.C. (“CSWM”) to safeguard confidential business information and to protect the **privacy** of our patients and their protected health information (“PHI”). CSWM considers any inappropriate use or disclosure of PHI or business information a violation of trust that jeopardizes the mission and survival of the organization. Events and information relating to services provided to patients are confidential.

II. Purpose

The purpose of this **policy** is: to comply with Section 164.502(b) of the Health Insurance Portability and Accountability Act of 1996; to protect CSWM and its patients from inappropriate use or disclosure of protected health information and business information; to limit access to such information to only those who have a legitimate need to know; and to ensure that reasonable efforts are made to limit the use and disclosure of PHI to the minimum necessary needed to accomplish the intended purpose of the use, disclosure or request.

Scope

This **policy** shall apply to all employees, medical staff, students, volunteers, and trustees of CSWM.

Procedure

- A. Individuals covered within the scope of this **policy** are expected to:
1. Use good judgment when using, disclosing or requesting PHI and related business
 2. Protect PHI and business information to which they have access and limit dissemination to appropriate individuals at appropriate times and to the appropriate extent;
 3. Maintain an environment that fosters strict adherence to confidentiality of PHI and business information;
 4. Only seek access to, use or disclose business information or PHI, including their own or a family member’s PHI, for which they have a legitimate business need and right to know to perform their direct responsibilities. Persons seeking access to their own PHI shall follow the procedures outlined in the appropriate Medical Records **Policy**.
- B. Individuals involved in patient care and treatment will only seek access to the medical records of those patients for whom the employee is responsible (e.g., only those patients on a nurse's floor.)

C. All Vice Presidents will be responsible for:

1. Identifying the classes of persons within their departments who need access to PHI to carry out their job duties;
2. Identifying the categories or types of PHI needed;
3. Identifying the conditions appropriate to such access;
4. Identifying routine and recurring disclosures of and requests for PHI within their department and document with the appropriate and defined amounts of disclosed PHI (See Appendix B); and
5. Monitoring and revising these standards as the roles within the department or needs of the department change.

D. All Managers will be responsible for:

1. Only authorizing access to those systems and/or databases that contain PHI to those employees that need access to carry out the requirements of their jobs.
2. Reviewing, revising (if necessary) and signing off on the access levels of each employee within their department as needed.
3. Educating all employees within their department on this **policy** and the department-specific standards to ensure that employees understand and agree to comply with both this **policy** and their department's access **policy**.
4. Reviewing all non-routine disclosures or requests against the Criteria for Non-Routine Disclosures contained in Section H of this **policy**. Each such non-routine disclosure needs to be reviewed and approved by the department manager prior to disclosure. The department manager shall consult with the CSWM **Privacy** Officer when appropriate.

E. Anyone who violates the terms of this **policy** will be disciplined up to and including termination of employment or of the business relationship. The degree to which the integrity of this **policy** is breached will determine the level of discipline.

F. Anyone who gains access to PHI inadvertently, either within the organization or outside it, has a responsibility to protect the confidentiality of the PHI and to take action to stop the further dissemination of the confidential information.

G. Anyone who learns of a breach of this **policy** has an obligation to report the breach to his or her manager or to the CSWM **Privacy** Officer.

H. Criteria for Non-Routine Disclosures

1. All non-routine requests for disclosure will be reviewed on an individual basis (See Appendix A) against the following designated criteria which have been designed to limit the PHI disclosed to that which is reasonably necessary to accomplish the purpose of the disclosure:

- The disclosure is not prohibited by any state or federal law
- The disclosure serves a legitimate business purpose
- The disclosure is sensible and reasonable
- The disclosure is consistent with the needs of CSWM
- The disclosure is limited to the minimum necessary needed to accomplish the purpose of the disclosure

Definitions

Disclosure: the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Personal Health Information (PHI): Information, including demographic information, that:

1. Is created or received by a health care provider, health plan, employer or health care clearinghouse and
2. Relates to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
3. Identifies the individual or can be used to identify an individual.

Use: the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information.