

Excerpts from:

**Summary Plan Description  
Sarasota Memorial Health Care System  
Health and Wellness Plan  
October 1, 2012**

**HIPAA PRIVACY INFORMATION  
(pages 69-71)**

**Compliance with HIPAA Privacy Standards**

Certain members of the Employer's workforce perform services in connection with administration of the Plan. In order to perform these services, it is necessary for these employees from time to time to have access to Protected Health Information (as defined below).

Under the Standards for Privacy of Individually Identifiable Health Information (45 CFR Part 164, the "Privacy Standards"), these employees are permitted to have such access subject to the following:

- (1) **General.** The Plan shall not disclose Protected Health Information to any member of the Employer's workforce unless each of the conditions set out in this HIPAA Privacy section is met. "Protected Health Information" shall have the same definition as set out in the Privacy Standards but generally shall mean individually identifiable health information about the past, present or future physical or mental health or condition of an individual, including information about treatment or payment for treatment.
- (2) **Permitted Uses and Disclosures.** Protected Health Information disclosed to members of the Employer's workforce shall be used or disclosed by them only for purposes of Plan administrative functions. The Plan's administrative functions shall include all Plan payment and health care operations. The terms "payment" and "health care operations" shall have the same definitions as set out in the Privacy Standards, but the term "payment" generally shall mean activities taken with respect to payment of premiums or contributions, or to determine or fulfill Plan responsibilities with respect to coverage, provision of benefits, or reimbursement for health care. "Health care operations" generally shall mean activities on behalf of the Plan that are related to quality assessment; evaluation, training or accreditation of health care providers; underwriting, premium rating and other functions related to obtaining or renewing an insurance contract, including stop-loss insurance; medical review; legal services or auditing functions; or business planning, management and general administrative activities.
- (3) **Authorized Employees.** The Plan shall disclose Protected Health Information only to members of the Employer's workforce who are designated and are authorized to receive such Protected Health Information, and only to the extent and in the minimum amount necessary for these persons to perform duties with respect to the Plan. For purposes of this HIPAA Privacy section, "members of the Employer's workforce" shall refer to all employees and other persons under the control of the Employer.
  - (a) **Updates Required.** The Employer shall amend the Plan promptly with respect to any changes in the members of its workforce who are authorized to receive Protected Health Information.

- (b) **Use and Disclosure Restricted.** An authorized member of the Employer's workforce who receives Protected Health Information shall use or disclose the Protected Health Information only to the extent necessary to perform his or her duties with respect to the Plan.
- (c) **Resolution of Issues of Noncompliance.** In the event that any member of the Employer's workforce uses or discloses Protected Health Information other than as permitted by the Privacy Standards, the incident shall be reported to the privacy official. The privacy official shall take appropriate action, including:

  - (i) Investigation of the incident to determine whether the breach occurred inadvertently, through negligence, or deliberately; whether there is a pattern of breaches; and the degree of harm caused by the breach;
  - (ii) Applying appropriate sanctions against the persons causing the breach, which, depending upon the nature of the breach, may include, oral or written reprimand, additional training, or termination of employment;
  - (iii) Mitigating any harm caused by the breach, to the extent practicable; and
  - (iv) Documentation of the incident and all actions taken to resolve the issue and mitigate any damages.
- (4) **Certification of Employer.** The Employer must provide certification to the Plan that it agrees to:

  - (a) Not use or further disclose the Protected Health Information other than as permitted or required by the Plan Documents or as required by law;
  - (b) Ensure that any agent or subcontractor, to whom it provides Protected Health Information received from the Plan, agrees to the same restrictions and conditions that apply to the Employer with respect to such information;
  - (c) Not use or disclose Protected Health Information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Employer;
  - (d) Report to the Plan any use or disclosure of the Protected Health Information of which it becomes aware that is inconsistent with the uses or disclosures hereunder, or required by law;
  - (e) Make available Protected Health Information to individual Plan Members in accordance with Section 164.524 of the Privacy Standards;

- (f) Make available Protected Health Information for amendment by individual Plan Members and incorporate any amendments to Protected Health Information in accordance with Section 164.526 of the Privacy Standards;
- (g) Make available the Protected Health Information required to provide any accounting of disclosures to individual Plan Members in accordance with Section 164.528 of the Privacy Standards;
- (h) Make its internal practices, books and records relating to the use and disclosure of Protected Health Information received from the Plan available to the Department of Health and Human Services for purposes of determining compliance by the Plan with the Privacy Standards;
- (i) If feasible, return or destroy all Protected Health Information received from the Plan that the Employer still maintains in any form, and retain no copies of such information when no longer needed for the purpose of which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information unfeasible; and
- (j) Ensure the adequate separation between the Plan and member of the Employer's workforce, as required by Section 164.504(f)(2)(iii) of the Privacy Standards.

Please refer to SMHCS policies referring HIPAA privacy for information on the personnel authorized to access Protected Health Information.

### **Compliance with HIPAA Electronic Security Standards**

Under the Security Standards for the Protection of Electronic Protected Health Information (45 CFR Part 164.300 et. seq., the "Security Standards"), the Employer agrees to the following:

- (1) The Employer agrees to implement reasonable and appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of Electronic Protected Health Information that the Employer creates, maintains or transmits on behalf of the Plan. "Electronic Protected Health Information" shall have the same definition as set out in the Security Standards, but generally shall mean Protected Health Information that is transmitted by or maintained in electronic media.
- (2) The Employer shall ensure that any agent or subcontractor to whom it provides Electronic Protected Health Information shall agree, in writing, to implement reasonable and appropriate security measures to protect the Electronic Protected Health Information.
- (3) The Employer shall ensure that reasonable and appropriate security measures are implemented to comply with the conditions and requirements set forth in Compliance With HIPAA Privacy Standards provisions (3) Authorized Employees and (4) Certification of Employers described above.

## **Privacy Statement (pages 81-82)**

Sarasota Memorial Health Care System (SMHCS) is committed to safeguarding the confidential information of your nonpublic information. Because SMHCS respects the individual's right to privacy, a high priority has always been placed on the personal information you provide. All personal information provided to Sarasota Memorial Health Care System is held in the strictest confidence. Information is never disclosed to non-affiliated third parties, except as required by law, and there is no anticipation of doing so in the future. Health and financial information that you provide is used to meet your personal financial goals and to administer health benefits while guarding against any real or perceived infringements on your rights of privacy. SMHCS's policy with respect to personal information about you is listed below.

Employee and third party access to information is limited to only those who have a business or professional reason for access. For example, the minimum necessary information may be shared with insurance carriers and other third parties in order to obtain proposals on your behalf and to administer your health benefits.

A secure office and computer environment is maintained to ensure that your information is not placed at unreasonable risk. There are policies that provide for:

- Password protection on database access for employees and clients,
- Monitoring of our computer networks and testing of the strength of our security in order to help us ensure the safety of client information,
- Backup and recovery procedures.

The categories of nonpublic personal information that are collected from a third party depends on the scope of the third party engagement. It will include information about your health to the extent that it is needed for the underwriting process, information about your transactions between you and health care providers and other third parties, and information from consumer reporting agencies.

For unaffiliated third parties that require access to your personal information, including financial service companies, consultants, and other professionals, information is provided only with your approval and requires strict confidentiality in our agreements with them. Federal and state regulations may also review SMHCS's records as permitted under law.

Your personal identifying information is not provided to mailing list vendors or solicitors for any purpose, at any time, under any circumstances.

Personally identifying information about you will be confidentially maintained during and after your employment with Sarasota Memorial Health Care System for the required time thereafter that such records are required to be maintained by federal and state securities

laws, the Internal Revenue Service, any applicable state department of insurance and consistent with sound business practices.

If you would like to discuss the confidentiality and privacy of your nonpublic personal information in detail, or if you ever have concerns, please feel free to contact the Human Resources Department.