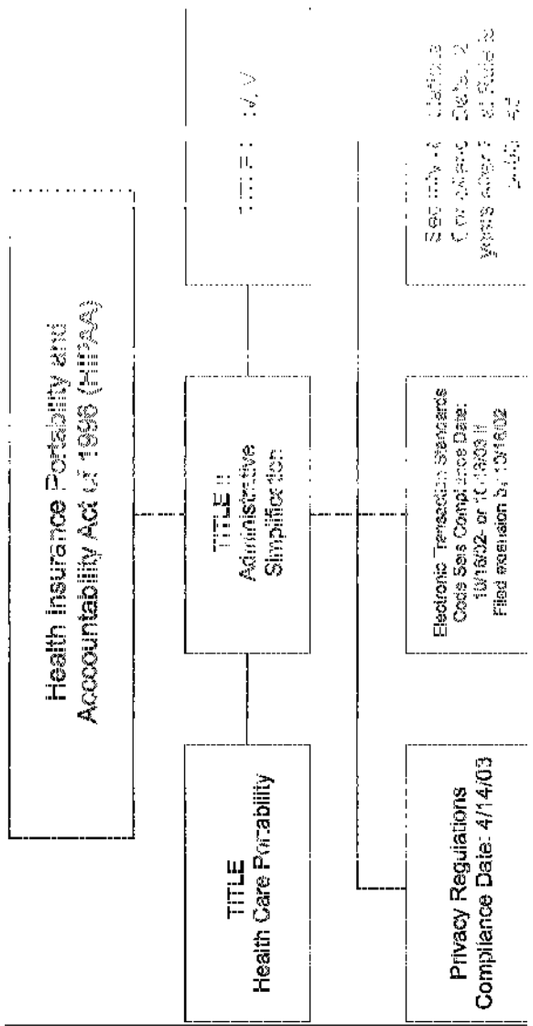
What does this mean to you as medical staff / allied health professionals? You are required to be knowledgeable of and to comply with the hospitals' policies and regulations.

Here are some examples of things you should do to protect patients' privacy and the security of their information:

- Treat all patient information, whether verbal, written or otherwise, as if it were your own.
- Take reasonable precautions when discussing private information within earshot of other patients.
- Share patient information only with colleagues or employees who have a need to know in the performance of their job duties.
- Follow hospital policies regarding release of patient records.
- Do not discuss confidential information in hallways, elevators or other high-traffic areas.
- Utilize patient conference rooms to discuss patient updates with family.
- Do not use the hospital computer systems to access patient information unless you need it to provide care.
- Do not share your password (PIN) with anyone.
- Use designated bins to dispose of confidential materials.

If you have questions about your responsibilities for maintaining compliance with HIPAA, or would like more information, please contact any one of the persons listed on the back of this brochure.



HIPAA Resources

Kerry Wolford
Director-Record Compliance & Privacy Officer
(920) 433-8513
Kerry.Wolford@hshs.org

Adam Nichol
Information Security Officer
(920) 431-3034
Adam.Nichol@hshs.org

Rachael Cochart
Responsibility Officer
(920) 884-4016
Rachael.Cochart@hshs.org

HIPAA

Health Insurance Portability and Accountability Act

Implications for Medical Staff / Allied Health Professionals

HSHS St. Vincent St. Mary's St. Nicholas St. Clare

Libertas
AN AFFILIATE OF HOSPITAL SISTERS HEALTH SYSTEM

Introduction

St. Vincent Hospital, St. Mary's Hospital Medical Center, St. Nicholas Hospital, St. Clare Memorial Hospital and Libertas Treatment Center are considered covered entities under the Health Insurance Portability and Accountability Act (HIPAA). As a provider, you may or may not be considered a covered entity; however, as a Medical Staff / Allied Health Professional, you have certain responsibilities to ensure HIPAA compliance at the hospitals. The brochure will highlight those key expectations.

St. Vincent Hospital, St. Mary's Hospital Medical Center, St. Nicholas Hospital, St. Clare Memorial Hospital and Libertas Treatment Center each will participate in an Organized Health Care Arrangement (OHCA) with credentialed providers on their medical staff. An Organized Health Care Arrangement exists when two or more providers present themselves to the public as participating in a joint arrangement, and participate in certain shared functions such as Medical Staff Committees.

Members of an OHCA may use and disclose protected health information with each other to carry out the health care operations of the OHCA.

This relationship also has another advantage. When a patient is admitted to the hospital, the physician seeing the patient does not have to provide his/her own Notice of Privacy Practices. The hospital Notice of Privacy Practices will suffice for the physicians as well as the hospital. However, this does not negate the responsibility of the clinic/physician office from publishing and distributing its own Notice of Privacy Practices to patients on their first clinic/office visit after April 13, 2003.

Privacy Regulation

The official title of the Privacy Regulation is Standards for Privacy of Individually Identifiable Health Information. The Privacy Regulation gives patients rights as to how their health information is used and disclosed. Patient rights identified by the Privacy Regulation include:

- Notice—To receive written notice describing the uses and disclosures of health information.
- Access—To inspect and receive copies of one's health information.
- Accounting—To receive a list of parties to whom one's health information has been disclosed.
- Request an Amendment— To request to change what the patient believes is in error.
- Restriction—To request a restriction on access and use of health information
- Complaint Process—To file a complaint with the provider and/or with the Federal Department of Health and Human Services (DHHS).

Protected Health Information (PHI)

All individually identifiable information that is transmitted or maintained in any form or medium. This relates to past present and future physical and mental health; the provision of health care to the patient; and payment for the patient's health care. It includes any information that can identify the patient or provides a reasonable basis to identify the patient including demographic information. Examples of PHI beyond the medical record include, but are not limited to: rounds reports, patient lists on personal digital assistants (PDAs), electronic medical record (EMR) access through smartphones, tablets or mobile devices, dictation recordings, raw diagnostic data on CD or flash drive.

Security Regulation

The Security Regulation identifies the technical, physical and administrative safeguards that must be in place to protect health information. This includes such things as disaster recovery and backup plans for computer systems, termination policies for employees and e-mail encryption.

Transactions and Code Sets (TCS)

The TCS rule adopts standards for electronic transactions and requires standardized code sets to be used in those transactions. These electronic transactions currently include:

- Health claims – submission of claims
- Health care payment and remittance advice – payments or explanation of benefits
- Coordination of benefits – claims and payment information between payers
- Health claim status - inquiries on claims
- Enrollment and disenrollment in a health plan – between plan sponsors and health plans
- Eligibility for a health plan verification – inquiries about eligibility, coverage, benefits
- Health plan premium payments – payments by employers, employees, etc., to health plans
- Referral certification and authorization – between health care providers and health plans
- First report of injury – reporting information related to injuries
- Health claims attachments for requests for review, certification, notification, etc.

Penalties for Non-Compliance

The Department of Health and Human Services (HHS) confers its primary enforcement responsibilities to the Centers for Medicare and Medicaid Services (CMS) for the Transactions and Codes Sets regulation and to the Office for Civil Rights (OCR) for Privacy and Security Regulations. The OCR is charged with:

- Investigating all complaints;
- Conducting compliance reviews;
- Obtaining monetary penalties; and
- Referring parties for criminal prosecution.

All medical staff / allied health professionals are required to comply with the hospitals' policies and regulations. Failure to comply with the HIPAA regulations can result in the following penalties levied against the hospital including its colleagues and medical staff appointees:

Civil Penalties—which can be levied against the covered entity. For example, not having policies and procedures in place, not having staff trained on requirements, not implementing regulations.

- $100 -$50,000 per violation, up to a yearly total of $1,500,000.

Criminal Penalties – these penalties can be assessed against individuals.

- Up to $50,000, 1 year in prison, or both for inappropriate use of protected health information. For example, disclosing records when an authorization or business associate contract was required.
- Up to $100,000, 5 years in prison, or both for using PHI under false pretenses. For example, accessing a record under pretenses of treatment when there is no treatment relationship and using that information in some manner, such as divulging it to a third party.
- Up to $250,000, 10 years in prison or both, for the intent to sell or use PHI for commercial advantage, personal gain, or malicious harm. For example, selling lists of patients with elevated cholesterol levels to a pharmaceutical company for their direct marketing purposes.