COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA") AT ONSLOW MEMORIAL HOSPITAL

What is HIPAA?

As part of its regulatory compliance efforts, Onslow Memorial Hospital ("Hospital") is committed to fulfilling the requirements of The Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

HIPAA is a federal law that includes requirements relating to the following areas:

1. It provides for "portability" of health care coverage so that individuals can transfer from one health plan to another without exclusions and limitations relating to preexisting conditions;

2. It prohibits discrimination relating to health plan eligibility and premiums;

3. It establishes increased surveillance and penalties relating to fraud and abuse; and

4. It includes administrative simplification provisions that establish standards for electronic transmission of certain health information.

The administrative simplification provisions of HIPAA relate to maintaining privacy and security of individually identifiable health information (also referred to as protected health information or "PHI") by prescribing how such information is to be shared, transferred, and stored. These provisions will have a significant impact on how PHI is managed and disclosed by the Hospital and other health care providers. The provisions will also affect how information is shared relating to the group health plan that covers Hospital employees.

The HIPAA administrative simplification requirements specify national standards relating to handling of PHI in the following areas:

• **Electronic Transactions and Code Sets**: These provisions automate business processes relating to administration and payment of health care claims.

• **Data Security**: These provisions ensure confidentiality and integrity of PHI that is transmitted electronically.

• **Unique Health Identifiers**: These provisions establish a system for identifying individuals, health plans, employers, and health care providers for use in data transmissions.

• **Privacy**: These provisions ensure that patients have control over and can obtain specific information about how their PHI is disclosed to others, limit release of PHI to the minimum reasonably necessary for the particular need or transaction, and give patients an opportunity to inspect, obtain copies of, and request amendment of their PHI. The privacy protections also apply to PHI relating to Hospital employees who receive services through the Hospital's Employee Health Services, who are enrolled in the Hospital's group health, dental, and disability insurance plans, or who sustain on-the-job injuries.

How is HIPAA Enforced?

HIPAA privacy provisions will be enforced through complaints made by individuals or their attorneys to the U. S. Office of Civil Rights ("OCR"). Enforcement of HIPAA security and other provisions will be handled by the Center for Medicare and Medicaid Services ("CMS"). Punishments for violation of HIPAA can include being excluded from Medicare and Medicaid. In addition, monetary penalties and prison terms can apply as follows:

Offense	Monetary Penalty	Imprisonment
One violation of a provision	up to $100	N/A
Multiple violations of a provision	up to $25,000	N/A
Wrongful disclosure of PHI	up to $50,000	up to 1 year
Wrongful disclosure of PHI under false pretenses	up to $100,000	up to 5 years
Wrongful disclosure of PHI under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm	up to $250,000	up to 10 years

Who is Involved in Implementing HIPAA?

Achieving HJPAA compliance at the Hospital will involve all employees, medical staff members, volunteers, contractors, vendors, and others who receive or are exposed to PHI or who use PHI in connection with performing services for the Hospital. Everyone who works for the Hospital or within the Hospital environment will be required to comply with the Hospital's policies and procedures relating to preserving and protecting the integrity of PHI and maintaining a "culture of confidentiality" relating to use of such information.

Special efforts are being made by the Hospital Administration and Information Systems to implement procedures to ensure that HIPAA security requirements will be satisfied in connection with electronic exchanges of PHI relating to billing, insurance, and performance of other functions. These procedures will include providing for protection of PHI stored or transmitted in electronic form and internal tracking methods for conducting periodic audits to confirm that only authorized persons access or use PHI and that such access and use are restricted to the nature and amount of PHI required for the particular

task or function being performed. Health Information Services has established procedures relating to accessing and disclosing PHI and responding to patient requests for amendment of PHI and accounting of disclosures of PHI.

Several individuals have been designated to perform particular responsibilities relating to implementation of HIPAA at the Hospital. These include a Privacy Officer and Security Officer as required by HIPAA as well as persons who are involved handling patient concerns and corporate compliance for the Hospital. Please contact these individuals if you have questions or concerns relating to implementation of HIPAA at the Hospital.

HIPAA Terms and What They Mean

Some important HIPAA terms and concepts include the following:

• **Acknowledgment**: A document signed by a patient to confirm that the patient has been provided with the Hospital's Notice of Privacy Practices;

• **Authorization**: A specific grant of authority for a specific period of time given by an individual to the Hospital or another covered entity under HIPAA that allows for use or disclosure of PHI for a specific purpose. An authorization is similar to a consent but is more specific as to time and purpose. If a particular use or disclosure of PHI is not covered by the Hospital's Notice of Privacy Practices, it must be covered by an authorization signed by the person to whom the PHI relates.

• **Business Associate Agreement ("BAA")**: This is a formal written agreement between the Hospital and another person or organization, referred to as a "Business Associate", that performs particular functions on behalf of the Hospital and involving PHI. The agreement commits the Business Associate to comply with HIPAA requirements relating to handling and safeguarding PHI. The Hospital will have BAAs with various persons and entities that perform services involving use or exposure to PHI. Examples include persons and entities that provide transcription services, clinical management services, legal services, software maintenance services, consultant services, as well as educational institutions whose students have clinical education experiences at the Hospital, etc. We will also have BAAs with certain members of the medical staff who perform medical director services and certain other administrative functions for the Hospital.

• **Covered Entity**: Entities that are covered by and must comply with HIPAA. These include health plans, health care clearinghouses, and health care providers, like the Hospital, who conduct standard health care transactions electronically.

• **Health Plan**: An individual or group plan that provides or pays the cost of medical care. Hospital employees are covered by a group health plan. The Hospital will work with the group health insurer to satisfy HIPAA requirements relating to sharing of PHI relating to employees covered by the plan.

• **Minimum Necessary Standard**: As part of protecting PHI, HIPAA requires that, except where disclosure is necessary for treatment purposes, only the minimum necessary amount of PHI needed to handle the particular job or function should be disclosed or used. In making minimum necessary determinations, it is important to evaluate: (i) who wishes to obtain or access the PHI, (ii) the purpose for which such PHI is needed, (iii) the nature and amount of PHI that will satisfy the need, (iv) the particular person or persons who need the PHI, and (v) how the PHI can be provided so that amount revealed and the number of persons who receive it are as limited as possible. For example, if a question arises relating to payment for a particular procedure, it may not be necessary to look at the patient's entire medical record in order to evaluate such matter. Under these circumstances, the person accessing the record or providing the information to the insurance company or other payor should access and disclose only that portion of the PHI that is relevant to the payment issue.

• **Notice of Privacy Practices**: A formal document that is given to Hospital patients at the time of registration, admission, or other point of contact and that outlines the Hospital's general policies and practices relating to complying with the HIPAA privacy requirements. This document is also posted in the Hospital and ancillary facilities and also appears on the Hospital website. Patients will be asked to sign an acknowledgment form to confirm that they have received the Hospital's Notice of Privacy Practices. The document will be kept on file and will apply to future registrations, admissions, and other contacts between the patient and the Hospital.

• **Protected Health Information ("PHI")**: Individually identifiable health information, i.e., information that identifies an individual or provides a reasonable basis for believing that it would identify an individual that is maintained or transmitted electronically or in any other form. It can include personal medical information as well as demographic information (e.g. address, telephone and fax numbers, Social Security numbers, medical record numbers, patient account numbers, etc.) used for treatment or payment. The Hospital has policies and procedures and uses specific forms in order to comply with HIPAA requirements relating to handling and release of PHI.

• **Transaction**: A transmission or exchange of information between two parties or entities for the purpose of handling financial or administrative activities relating to health care. The Hospital is involved in many different types of transactions that are or will be subject to HIPAA requirements. The Hospital will follow policies and procedures with regard to handling internal administrative functions and relationships with other involved parties in order to achieve HIPAA compliance with regard to various transactions.

HIPAA AND NORTH CAROLINA LAW

North Carolina has certain laws that relate to patient consent, confidentiality of patient information, and release of health information. Some of these laws are more restrictive or provide for greater protection of persons or PHI than the requirements of HIPAA. Where state law is stricter or more stringent than HIPAA, the state law preempts HIPAA and state law must be followed. Examples include, but are not limited to: (i) laws that require health care providers to report to appropriate governmental agencies PHI relating to suspected abuse, communicable diseases, and other matters; and (ii) laws that grant minors the right to consent to and to have confidentiality maintained with regard to certain types of care. The Hospital's policies and procedures relating to implementation of HIPAA will satisfy state law requirements in those instances where state law preemption applies.

HIPAA Dos and Don'ts

DO:

• Attend one or more training programs relating to HIPAA compliance;

• Review and understand policies and procedures relating to implementation of HIPAA at the Hospital;

• Know how to access and use HIPAA forms;

• Use or share PHI in accordance with HLPAA policies and procedures;

• Except for patient treatment situations, access, use, or share only the portion of PHI that is minimally necessary to address a particular need or circumstance;

• Confirm that every patient who has contact with the Hospital or receives Hospital services is provided with or has a written acknowledgement on file indicating that he/she has previously received a copy of the Hospital's Notice of Privacy Practices;

• Take precautions to avoid incidental disclosure of PHI to persons other than the patient or those who are involved in the patient's treatment or payment and other operational activities relating to the patient's treatment. Consider taking some of the following general precautions:

- Avoid discussing patients in hallways, elevators, the cafeteria, etc.;

- Avoid leaving messages on answering machines about patient conditions, scheduling of particular procedures, or test results;

- Avoid leaving PHI on computer screens or on desks, counters, fax machines, or in wastebaskets where it may be seen by persons other than the patient or those who are providing care or performing other services relating to the patient; when faxing information containing PHI, confirm that the fax machine to which the transmittal is being made is attended or that it is in a secure location or has a locked receiving box;

- Avoid sending e-mail messages that contain patient names, demographic information, or other PHI unless the information is encoded; double check to be sure that the correct addressee is used in an e-mail message before sending the message; never share with another person password information that can be used to access PHI;

- Avoid paging patients in a manner that could indicate their health conditions — i.e. by using the name of their physician, identifying a particular unit, or referring to a particular procedure;

- Avoid incidental disclosures of patient information by closing doors, speaking softly, and being careful about telephone conversations;

• Check with the Privacy Officer or Compliance Counsel if you have questions, concerns, or need clarification before you use or release PHI.

DON'T:

• Believe that HIPAA is too complex to understand and implement;

• Assume that HIPAA doesn't apply to you or that you won't get caught if you don't follow proper procedures;

• Think that things haven't changed and that you can do what you've been used to doing with regard to accessing, using, and releasing patient information;

• Act first and ask questions later. Once an improper use or disclosure occurs or there is a breach of security relating to PHI, the harm is done.

HIPAA Information and Training Resources

The Hospital will provide education relating to HIPAA implementation at the Hospital through distribution of this brochure, informational overviews for the Board of Directors, Medical Staff, and Senior Management Staff, and training programs for employees, volunteers, and on-site vendors and other service providers. HIPAA information will also be included as part of the orientation process for new employees and the periodic re-orientation process for existing employees. The Education Department of the Hospital

will have and maintain various films, PowerPoint programs, and other resource information relating to HIPAA compliance. These resources will be available for use at staff meetings and in other settings within the Hospital to reinforce basic HIPAA concepts and to provide updated information relating to continued compliance with HIPAA requirements.

Commitment to HIPAA Compliance

The Hospital is committed to implementation of HIPAA requirements and expects that all persons associated with the Hospital will make a formal commitment to this endeavor. Your cooperation and prompt response are greatly appreciated.