UNCG HIPAA PROCEDURES
SECURITY MANAGEMENT, PRIVACY, AND BREACH NOTIFICATION

TERMS AND DEFINITIONS

"A qualified protective order" restricting the use of PHI means, with respect to PHI requested under this section, an order of a court or a stipulation by the parties to the litigation or administrative proceeding that:

- Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
- Requires the return to UNCG or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

"Authorization" at the University of North Carolina at Greensboro (UNCG) allows for the use and disclosure of PHI for purposes other than treatment, payment, and health care operations (TPO).

"Availability" means that PHI data or information is accessible and useable upon demand by an authorized person such as UNCG staff members.

"**Breach**" generally is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment.

"**Breach Notification**" refers to the notification process following a breach of unsecured protected health information that must be provided to affected individuals, the Secretary of Health and Human Services, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Business Associate: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

"Confidentiality" means that PHI data or information is not made available or disclosed to unauthorized persons or processes.

"Data custodian" refers to the designated Information Technology Services Department employee who is responsible for providing a secure infrastructure to conduct data processing services for the University's software applications, data, networks, and operating systems (see the University Data Classification Policy).

"Data stewards" refers to the University employees responsible for direct operational level information management, including assignment of data access permissions to users.

TERMS AND DEFINITIONS

"Designated Record Set" is a group of records maintained by or for UNCG that are the medical records and billing records about patients that are maintained by or for UNCG and are the enrollment, payments, claims adjudication, and case or medical management record systems maintained by or for a health plan, or used, in whole or part, by or for UNCG to make decisions about patients.

"Disclosure" at UNCG means the release, transfer, provision of access to, or divulgence in any other manner, of information to any organization external to UNCG.

"Electronic Media" means:

- Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, digital memory card, or videotapes; or
- Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

"Electronic Protected Health Information" or **"EPHI"** means individually identifiable health information that is:

- Transmitted by electronic media to secure websites.
- Maintained in electronic media such as being stored on the secure HIPAA drive. EPHI is not to be stored on computer hard drives, laptops, PDAs, floppy disks, rewritable devices, flash memory devices, or USB memory devices.

"Health Information Manger HIM Custodian" is the person or department responsible for the maintenance, retention, access, data integrity, and data quality of PHI, including protecting patient privacy and providing information security, analyzing clinical data for research and public policy, preparing PHI for accreditation surveys, and complying with standards and regulations regarding PHI.

"HIPAA Compliance Officer" refers to the individual within each Covered Entity tasked with overall responsibility for HIPAA privacy and security compliance.

"Information Systems" means the workstations used within UNCG to connect to the network and to access, store, and manipulate EPHI.

TERMS AND DEFINITIONS

"Integrity" means that PHI data or information have not been altered or destroyed in an unauthorized manner.

"Medical Record" is the UNCG medical record maintained by each HIPAA Covered Entity that is designed to contain a composite of all clinical information gathered on a given patient. The medical record has been maintained in an electronic state since 2007. The medical record has a retention schedule based on NC General Statutes.

"Referring Physician" is the source behind a particular episode of health care. The referring physician may be the primary care physician, a facility, and/or a consulting physician to whom the primary care physician referred the patient.

"Right to Amend" is where an individual has the right to have a covered entity amend protected health information or record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

"Risk" means the likelihood that a specific threat will exploit certain vulnerabilities and the resulting impact of that event.

"Security Measures" means security policies, procedures, standards, and controls regarding EPHI.

"Staff Member" means employees, UNCG students, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the covered entity.

"UNCG HIPAA Privacy Officer" refers to the individual with overall responsibility for HIPAA privacy compliance for UNCG. Other responsibilities include HIPAA training and the UNCG HIPAA Committee.

"UNCG HIPAA Security Officer" refers to the individual within UNCG Information Technology Services responsible for UNCG HIPAA electronic security compliance.

"Use" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within UNCG.

"Workstation" includes the hardware, software, and other applications used to access EPHI stored on the network.