THE UNIVERSITY SYSTEM OFFICE
of the
BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA

POLICIES AND PROCEDURES FOR HIPPA COMPLIANCE

THE UNIVERSITY SYSTEM OFFICE
of the
BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA

POLICIES AND PROCESURES FOR HIPPA COMPLIANCE

I. GENERAL

As part of its broader mission and in support of the health and safety of the citizens of Georgia, the Board of Regents of the University System of Georgia (the Board) maintains personal healthcare information about its students, employees, patients, and others. The Board, its officers, and its employees are committed to protecting the privacy and confidentiality of this information. The Board fully supports and complies with all federal and state statutes and rules regulating the use, maintenance, transfer, and disposition of healthcare records and information.

The Board's University System Office (the USO) is committed to full compliance with all other rules, regulations, statutes, and policies governing the maintenance and disposition of health care records, including each provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These policies and procedures are designed to assist all responsible parties with this commitment.

II. MAINTENANCE AND REVIEW OF HEALTH CARE RECORDS

Except as noted below, it is the policy of the USO to allow individuals to inspect and obtain copies of their own health information and to request the amendment of their health information which is maintained by or at the USO. Additionally, the USO allows individuals to request information regarding disclosures of their health information made by the USO to third parties.

For purposes of these policies and procedures, employee records and student records subject to the Family Educational Rights and Privacy Act are specifically excluded from the definition of "health record".

Individuals will typically be denied access to information contained in psychotherapy notes, or to information that was obtained from a non-USO source under an agreement of confidentiality. The USO may otherwise choose to deny access to certain health information contained in the health record if, in the judgment of a licensed health care professional, such access could cause harm to the individual or to another person.

The USO will allow an individual to amend information in their health record where the information in question was created by the USO and is inaccurate or incomplete. Otherwise, the USO may allow an individual to request an amendment of their health record, which may be reviewed by a licensed health care professional at the

requestor's expense. Amendment requests should be directed to the USO's Director of Human Resources, who will, after appropriate consultations and investigation, make a recommendation to the Senior Vice Chancellor for Support Services regarding the requested amendment. The Senior Vice Chancellor shall, after receiving the recommendation and within a reasonable time, determine whether to grant the amendment request. If the request is denied, the USO will provide the individual a written explanation and allow the individual to submit a statement of disagreement to become a part of their health record. The Senior Vice Chancellor's decision may be appealed to the Chancellor of the University System, whose decision shall be final.

Except for health care information released pursuant to a signed authorization or otherwise exempted by statute, the USO will, upon request, provide an individual with information regarding the release of their identifiable health information to third parties that was made for purposes other than treatment, payment, and healthcare operations (as defined in HIPAA). Reasonable attempts will be made to provide this information in a format requested by the individual. Otherwise, it may be provided in any format mutually agreed upon.

Requests for access to health information, requests to amend health information, or requests for an accounting of disclosure of health information shall be in writing and shall be made to the USO's Director of Human Resources. Initial responses to such requests typically will occur within thirty days of an access request or sixty days in the case of request for amendment or for an accounting of disclosure. In the event of denial, the response will include an explanation of the denial and will inform the individual of their right to and the process for appeal. The USO may, at it's discretion, charge a requestor a fee not to exceed the actual cost of compiling, copying, and mailing requested information.

III. Physical Security

Each healthcare record maintained by the USO in physical form will be kept appropriately secured in a locked location. Each electronic healthcare record maintained by the USO shall be kept in a secure environment and protected by appropriate electronic safeguards. Protected health information stored in computers is to be password protected. Passwords are individual specific and are not to be shared by or accessible to more than one individual.

Electronic transmission devices, including computers, telefax machines, and other electronic equipment over which protected health information may be received or transmitted are to be maintained in secure sites and/or away from public access. Computer screens containing protected health information are to be inaccessible to public view. Computers that store protected health information are to be secured before being left unattended.

Health information may only be accessed by authorized personnel. With the exception of the use and disclosure of health information directly related to treatment and to the extent practicable, access to health information by USO employees or other authorized personnel is restricted to the minimum necessary to execute their job responsibilities. It is the responsibility of each USO department, division or unit to identify those persons or classes of persons who are authorized to access, use or disclose health information and specifically to identify to what health information to which they may have access.

Physical access to controlled areas and user accounts that provide access to protected health information are to be revoked upon the termination of an employee, student, or trainee or when others, such as contractors and vendors, no longer require access.

The unauthorized access to or unauthorized use or disclosure of health information that exists in any USO health record may subject the responsible employee, student, or trainee to disciplinary action up to and including termination of employment or suspension or expulsion from a student or trainee program. This extends to the unauthorized use or disclosure of health information that is overheard during the course of business or health information that is otherwise learned or secured by any USO employee, student or trainee by virtue of their employment or academic or training association with the University System.

USO departments that become aware of the unauthorized use or disclosure of protected health information that causes or reasonably could cause harm should immediately report the incident to the USO Privacy Officer, the Senior Vice Chancellor for Support Services, the Director of Human Resources, or any attorney in the USO's Office of Legal Affairs. To the extent practicable, the USO will attempt to minimize the known harmful effects and/or correct known instances of harm.

All USO employees, students, or trainees who may use, disclose, or have access to identifiable health information contained in any health record must, as a condition of continued employment or training, complete a training program that outlines employee responsibility and patient rights under the statutory privacy regulations contained in HIPAA.

IV. Use and Disclosure of Health Information

It is the policy of the USO that an individual's identifiable health information may only be used within the USO or disclosed to entities outside the USO after notification to and/or with the expressed permission of the individual, except in cases of emergency or where specifically permitted or required by law. Access to health information maintained by the USO is limited to those who have a valid business or medical need for the information or otherwise have a right to know the information. With the exception of purposes related to treatment, access to an individual's health information or the use or disclosure of an individual's health information must, to the extent practicable, be limited

to only that necessary to accomplish the intended purpose of the approved use, disclosure or request.

Information maintained by the USO for purposes related to the administration of a University System health plan will not be used for employment related purposes, including but not limited to, annual evaluations, employee discipline, promotion, retention or termination. The USO strictly segregates functions related to health plan administration from employment decisions.

An individual's health information may be used by the USO for treatment, payment, and healthcare operations (as defined by HIPAA) after the USO has provided to the individual a copy of these policies and procedures and has made a good faith effort to obtain an acknowledgment of its receipt. Additionally, the USO may use an individual's health information for other purposes or may disclose an individual's health information to external entities for other purposes upon obtaining a valid authorization from the individual giving permission for that stated use or disclosure. Further, the USO may use and disclose an individual's health information without prior permission or authorization where the health information has been sufficiently "de-identified", so as to hide the identity of the individual(s), is part of a "limited data set", or for other uses where allowable by law.

Health information may be used or disclosed without a individual's acknowledgment of receipt of these policies and procedures in the event of an emergency or where a communications barrier makes prior permission or notification impossible.

From time to time, the USO may disclose identifiable health information to other entities for use by the individual for treatment. Further, the USO may disclose identifiable health information to other entities to assist the individual in obtaining payment and, under limited circumstances, may disclose identifiable health information to other entities for purposes associated with healthcare operations.

V. Communication of Health Information

It is the policy of the USO to inform individuals about the USO's privacy practices as they relate to health information that may be maintained by the USO in order to safeguard health information in the USO's possession, and, to the extent practicable, to protect the communication of health information, including oral information, from intentional or unintentional use or disclosure. It is further the USO's policy to accommodate, to the extent practicable, the requests of individuals regarding the place, time, and method of communicating to them their own health information.

The USO will publicly disseminate these policies and procedures and make a good faith effort to receive an acknowledgment of such receipt prior to the first date of employment or student training. The USO will not knowingly use or disclose health information in a manner inconsistent with these policies and procedures, except to the extent that emergency patient care would be compromised. The USO reserves the right to

amend these policies and procedures as deemed necessary or advisable and, to the extent and in a manner practicable, will inform individuals of material changes to these policies and procedures. These policies and procedures constitute an official policy statement and may not be amended, or otherwise altered, by any area of the USO without the approval of an authorized USO official.

Health information that is communicated in any form is to be treated as confidential and in a manner that reasonably protects the communication from being intentionally or unintentionally overheard or intercepted by those who do not have a need or right to know the information. It is the responsibility of each USO department, division or unit to implement practices that protect the confidentiality of oral, written and electronic communications.

To the extent practicable, the USO will accommodate the written request of an individual to have their health information communicated to them at a time, place, and in a manner of their choosing. If the request is impractical or impossible for the USO to accommodate, this will be clearly communicated to the individual requesting the accommodation.

The USO will recognize personal representatives authorized by individuals, the courts, or by state law for purposes of communicating health information. Personal representatives may be parents or legal guardians of minor children or persons who are legally authorized or specifically identified by individuals, such as a close friend or family member, to act on behalf of the individual. The USO may, without prior authorization of an individual, and where necessary due to emergency or other professionally sound reason, communicate health information with persons directly involved in the care of the individual. The USO may refuse to provide information to personal representatives, or to the individuals themselves, where it is determined that access to the information may be detrimental to or otherwise not in the best interest of the individual, may endanger or breach the confidentiality of a third party or is precluded by statute.

Violation of this policy or negligence on behalf of any USO employee or student or trainee resulting in or having the potential to result in the unauthorized release of identifiable health information may result in disciplinary action up to and including termination of employment or suspension or expulsion from a student or trainee program.

VI. Marketing and Public Relations

It is the policy of the USO not to use or disclose identifiable health information for marketing or public relations purposes without the authorization of the individuals to whom the health information relates. It is further the policy of the USO to allow individuals to choose not to have their identifiable health information used for such purposes.

VII. NOTIFICATION AND AUTHORIZATION

It is the policy of the USO that an individual's identifiable health information may typically only be used or disclosed pursuant to notification to and/or permissions granted by the individual, unless otherwise permitted or required by statute.

The USO will provide individuals with a copy of these policies and procedures prior to the commencement of employment or training, unless an emergency or a communications barrier makes providing or obtaining these policies and procedures impossible or impracticable, and will make a good faith effort to obtain acknowledgment of its receipt.

Except in emergency situations where patient care might be compromised, the USO will not use or disclose identifiable health information in a manner inconsistent with these policies and procedures.

Only approved forms may be used for providing notification and no additions, deletions, or modifications may be made to the forms without the approval of an authorized USO official.

The USO allows individuals to request restrictions on the use and disclosure of their health information for treatment, payment, and healthcare operations. Following review by authorized USO personnel, the USO may choose not to agree to the requested restrictions. The USO will adhere, however, to any restrictions to which it agrees.

Acknowledgments of receipt of these policies and procedures will be retained by the USO for a minimum of six years. Any agreed upon restrictions arising out of a notification will remain in effect until revoked by the individual or until the individual is notified by the USO that the USO will no longer honor the agreed upon restrictions.

In the event the USO receives more than one authorization or permission from an individual that appear to be in conflict with each other, the USO will abide by the more restrictive patient permission, until the conflict is resolved. The USO will attempt to determine the true intentions the affected individual and thus resolve the conflicting permissions as soon as is practicable.

An individual's health information may be used or disclosed by the USO for purposes other than treatment, payment, and health care operations, such as for research. Use and disclosure for such purposes requires a valid, signed authorization specifically detailing what information will be used or disclosed, how and by whom the information will be used or disclosed, and during what time period the information will be needed or a statement indicating there is no defined duration.

Authorizations are valid only for the conditions outlined in the document and may not be used for any purpose or purposes not specifically stated and agreed to by the signing individual. The USO will allow an individual to revoke his or her authorization at

any time by submitting a written request. However, any such revocation shall not be retroactive to the extent that the USO has already relied and acted on a prior authorization.

VIII. Business Associates

The USO discloses identifiable health information to other public or private entities with which the USO or the University System has contracted to provide services to the USO, the University System or a health plan of the University System. Health information provided to such a business associate must be pursuant to an assurance that the business associate, and its sub-contractors, will use the information only for the purpose(s) intended, will restrict access to the information on a "need to know" basis only, and will otherwise take appropriate measures to safeguard the information in its possession. There must be a valid, signed business associate agreement in place before identifiable health information may be provided.

Except to the extent that patient care might be compromised, the use or disclosure of health information by a business associate must comply with these policies and procedures. In addition, except to the extent that patient care might be compromised, the use and disclosure of an individual's health information by a business associate must comply with any restrictions beyond the scope of these policies and procedures which are requested and subsequently agreed to by the USO.

Business associate agreements must be in writing and must contain USO-approved HIPAA compliant language and authorized signatures.

At any time the USO determines that a business associate has violated a material term or obligation under the agreement relating to HIPAA compliance, the USO shall seek to immediately remedy the breach or, if that is not possible, to alter or terminate the agreement. Violations may also be reported by the USO to the Secretary of the Department of Health and Human Services.

It is the responsibility of each USO department, division, or operating unit contracting for services with third parties with whom identifiable health information will be shared to assure that valid business associate agreements are executed.

IX. Electronic Data Interchange (EDI)

It is the policy of the USO to timely install and utilize the standards promulgated under HIPAA for transactions and code sets as each standard or code set is updated.

The HIPAA EDI transaction standards facilitate the communication between providers and health plans. These transaction standards improve efficiency by eliminating duplication and waste thus reducing the costs associated with efficient delivery of healthcare services and supplies. Code sets are used to facilitate the consistent and comprehensive view of complex information related to diagnoses and medical

procedures. By using a standard code set, all data is represented universally, and understood by all parties.

A. Transactions

Transaction sets are the common exchanges of information between health care providers and insurers. HIPAA requires electronic transactions adherence to a common format that all parties can interpret.

Batch transactions are those types of transactions that occur multiple times, and do not require immediate response. For example, a claim is a batch transaction. A doctor typically sees several patients each day. At the end of the week or other predetermined period, claims to the insurance company may be sent in one group, or batch. Each individual claim does not need to be processed – or even acknowledged – immediately. Once the entire batch of claims is received, the transaction is acknowledged and the claims are processed.

Current HIPAA standard transaction sets for batch transactions:

Premium Payment ASC X12N 820 (004010X061)
Eligibility ASC X12N 834 (004010X095)
Payment Remittance Advice ASC X12N 835 (004010X091)
Institutional Claims ASC X12N 837 (004010X096)
Professional Claims ASC X12N 837 (004010X097)
Dental Claims ASC X12N 837 (004010X098)

On-line transactions are those types of transactions that require an individual response. For example, a specialist referral request is an on-line transaction. A doctor typically refers patients to a specialist while the patient is in the doctor's office. The doctor sends a request to the insurance company for a referral and waits until he receives a response either approving or denying the referral request.

Current HIPAA standard transaction sets for on-line transactions:

Eligibility Inquiry ASC X12N 270/271 (004010X092)
Additional Claim Information ASC X12N 275 (004010X107)
Claims Status Inquiry ASC X12N 276 (004010X093)
Request for Additional Information ASC X12N 277 (004010X104)
Utilization Review Inquiry ASC X12N 278/279 (004010X094)

B. Standard Code Sets

By using a standard code set, all data is represented universally, and understood by all parties.

Current HIPAA standard code sets:

Logical Observation Identifier Names and Codes (LOINC)
Health Care Financing Administration Common Procedural Coding System (HCPCS)
Home Infusion EDI Coalition (HEIC) Product Codes
National Drug Code (NDC)
National Council for Prescription Drug Programs (NCPDP)
International Classification of Diseases (ICD-9)
American Dental Association Current Dental Terminology (CDT-4)
Diagnosis Related Group Number (DRG)
Claim Adjustment Reason Codes
Remittance Remarks Codes

X. ELECTRONIC SECURITY

[to be completed]