HSC Health Care System
Ethics, Research and Compliance

ET/22
Original: 03/18

HIPAA Privacy Policy

1. General.

1.1. General.

The Covered Entity components of The HSC Health Care System ("HSC") comply with the Administrative Simplification section of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), and regulations promulgated thereunder (collectively, "HIPAA"). The HIPAA regulations applicable to the Covered Entity components of HSC include the Standards for the Privacy of Individually Identifiable Health Information, the Security Standards for the Protection of Electronic Protected Health Information and the requirements for Notification of a Breach of Unsecured Protected Health Information.

HIPAA is not the only law governing HSC with respect to data privacy and security. HSC also complies with state laws and other federal laws governing privacy, to the extent those laws are not preempted by HIPAA and are applicable to HSC.

1.2. Scope.

This Policy governs the Covered Entity components of HSC. The Covered Entity Components of HSC include: The HSC Pediatric Center; HSC Home Care, LLC; and Health Services for Children with Special Needs, Inc., and applies to all patients and health plan members and beneficiaries of such Covered Entities.

No third-party rights are created by this Policy. HSC reserves the right to amend or change this Policy at any time without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, this Policy shall be aspirational and shall not be legally binding upon HSC, or give rise to a violation of the HIPAA Privacy Rule. Thus, individuals may not bring a private cause of action based on this Policy or HSC's obligations under HIPAA. This Policy applies to all members of HSC's Workforce with access to Protected Health Information.

2. Definitions.

All terms used, but not otherwise defined, in this Policy shall have the same meaning as those terms in HIPAA.

2.1. "Breach" is an unauthorized acquisition, access, use, or disclosure of Unsecured PHI which compromises the security or privacy of such information. Except as indicated below in subsections A. through C., an unauthorized acquisition, access,

use, or disclosure of Unsecured PHI is presumed to be a Breach unless, after conducting a risk assessment, HSC has demonstrated that there is a low probability that the PHI has been compromised. The term "Breach" does *not* include:

A. Any unintentional acquisition, access, or use of PHI by a Workforce member or individual acting under the authority of HSC if:

1. Such acquisition, access, or use was made in good faith and within the course and scope of their authority with HSC and

2. Such information is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule; or

B. Any inadvertent disclosure by a person who is authorized to access PHI at HSC or to another person authorized to access PHI at HSC and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule; or

C. A disclosure of PHI where HSC has a good-faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.2. "Business Associate" is an entity, acting other than in the capacity of a member of the HSC workforce, that creates, receives, maintains, or transmits PHI for or on behalf of HSC, or that provides services to or for HSC, where the provision of services involves the disclosure of HSC's PHI.

2.3. "Discovery of a Breach" occurs as of the first day on which the Breach is known to HSC or should have been known to HSC if it had exercised reasonable due diligence.

2.4. "Electronic PHI" or "EPHI" means Protected Health Information which is transmitted by electronic media or maintained in electronic media, limited to information that HSC creates, receives, maintains, or transmits.

2.5. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended and in effect.

2.6. "Mobile Device" means any electronic asset including, but not limited to, laptops, smartphone and tablet devices that support electronic assets, regardless of whether or not they contain Mobile Media.

2.7. "Mobile Media" means electronic storage material on which information is or may be recorded electronically including devices in computers and any removable or transportable digital memory medium (such as magnetic disks and digital memory cards).

2.8. "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. parts 160 and 164, Subparts A, D and E, as currently amended and in effect.

2.9. "Protected Health Information" or "PHI" is any oral, written, or electronic individually identifiable health information maintained or transmitted in any form or medium. Individually identifiable health information includes demographic information and any information that relates to a past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to any individual.

2.10. "Security Rule" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subpart C, as amended and in effect.

2.11. "Subcontractor" is an entity that creates, receives, maintains, or transmits PHI for or on behalf of Business Associates of HSC or that provides services to or for Business Associates of HSC where the provision of services involves the disclosure of HSC's PHI. Subcontractors are Business Associates under HIPAA.

2.12. "Unsecured Protected Health Information" or "Unsecured PHI" is PHI that is not encrypted and rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services ("HHS").

2.13. "Workforce" means all members of the HSC workforce who have access to PHI in order to perform their job functions of HSC. Workforce includes HSC's employees, volunteers, trainees, and other persons whose work performance is under the direct control of HSC, whether or not they are paid by HSC.

3. Privacy Policies.

3.1. Privacy Officer and Contact Person.

A. HSC designates a Privacy Officer. The Privacy Officer serves as the contact person who is responsible for receiving complaints and inquiries regarding HSC's compliance with the applicable provisions of HIPAA and this Policy. Wherever this Policy refers to the Privacy Officer, if applicable, such reference shall include any person delegated by the Privacy Officer, whether such delegation is oral or written.

B. The Privacy Officer may be reached by contacting the HSC Health Care System's Compliance Department at 202-441-6253.

3.2. Policy and Procedure Implementation.

A. HIPAA Privacy Policy. HSC will implement and update as needed this Policy, which is designed to comply with HIPAA, implementation specifications.

B. Changes to Policies. HSC will amend its other applicable policies and procedures as necessary and appropriate to comply with changes in HIPAA and this Policy.

3.3. Training of Workforce Members.

Workforce members will receive the training necessary and appropriate to permit them to carry out their functions for HSC, in accordance with this Policy.

A. Identification of Workforce. HSC will identify all employees and other personnel who are members of its Workforce.

B. Training. HSC will conduct a training session for all current members of its Workforce regarding the Privacy Rule, the Security Rule, the Breach Notification Rule, the Enforcement Rule, and this Policy. All individuals who join the Workforce after the initial or any subsequent training will be trained within a reasonable time after joining the Workforce. If this Policy is materially changed, the Privacy Officer will perform a new training session for Workforce members within a reasonable time after the new Policy takes effect as necessary. HSC is not required to train Business Associate personnel unless such personnel are designated as Workforce members of HSC.

C. Documentation. HSC will document the time, date, place, and content of each training session, as well as the Workforce members who attend each training session. The Privacy Officer will maintain such documentation in HSC's HIPAA compliance files for a period of at least six (6) years and will make it available for inspection by regulatory authorities, as appropriate.

4. Management and Administration of PHI.

4.1. Safeguarding PHI.

HSC will establish reasonable and appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of applicable Privacy Rule requirements, in compliance with the applicable provisions of the Security Rule.

A. Safeguarding – General.

1. HSC will implement administrative, technical, and physical safeguards to protect PHI that are reasonable and appropriate.

2. HSC will reasonably safeguard PHI to eliminate impermissible uses and disclosures and to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

3. HSC will periodically review the safeguards and will coordinate the safeguards with internal policies and procedures.

B. Safeguarding Uses of PHI.

1. Paper PHI. When appropriate, to the extent that cabinets and/or offices contain PHI, such cabinets and/or offices shall be locked after business hours or during extended absences. Access to such cabinets and offices will be limited to Workforce members who require access to perform their job duties. Where paper copies of PHI are outside of storage for use, they will be handled in a reasonable manner to prevent unintended access to such PHI.

2. EPHI. As applicable, technical safeguards shall be implemented, such as reasonable and appropriate firewalls, security software, and encryption programs as well as a requirement for unique usernames and passwords for access to computer files and Mobile Devices that contain PHI. Only members of the Workforce shall have such unique usernames and passwords. All EPHI maintained in e-mail, on a hard drive, or on a Mobile Device or Mobile Media, except EPHI maintained on a Personal Devices (as defined herein), shall necessitate the activation of HSC's encryption program/system functions to ensure the EPHI is secure.

3. Secure Premises. Workforce members will safeguard all electronic and paper copies of PHI by ensuring that access to HSC's premises and workstations is secure and by logging off when workstations are not in use.

4. Return or Destruction of PHI.

a. Paper copies of PHI will be properly disposed of by shredding, by placing in locked disposal containers, or in another reasonably safeguarded process.

b. EPHI will be deleted from electronic media in a commercially reasonable manner to ensure that the information is permanently unreadable prior to disposal.

4.2. Sanctions for Violations of Privacy.

Sanctions for using or disclosing PHI in violation of this Policy will be imposed in accordance with HSC's Human Resources Department's applicable Workforce policies, up to and including termination of employment.

A. Procedures.

During training, Workforce members shall be informed that sanctions may be imposed if this Policy is violated. Appropriate sanctions shall be determined on the basis of the nature of the violation, its severity, and whether it was intentional or unintentional. Such sanctions may include, without limitation, verbal warnings, written warnings, probationary periods, and termination of employment.

B. Safeguarding Disclosures of PHI.

1. Electronic Information. All Health Information pertaining to an individual that is electronically transmitted will be transmitted in accordance with the safeguard requirements of this Policy.

2. Internal Disclosures. Workforce members will use the minimum PHI necessary to accomplish the intended HSC function.

3. Disclosures to Third Parties. For any disclosure that is permitted or required of HSC in accordance with this Policy, Workforce members and agents will verify the identity, authority and location (e.g., fax number, mailing address) of the party or parties receiving the information and the scope of such requested information.

4. Reasonable Safeguards of Business Associates. When HSC engages Business Associates for services and Business Associates have access to PHI, HSC will require each Business Associate to agree, in writing, that it will reasonably safeguard PHI.

5. Permitted Uses and Disclosures of PHI.

HSC may use and disclose PHI as required by law or for a permissible purpose in accordance with applicable provisions of HIPAA.

5.1. Uses and Disclosures of PHI.

HSC may use and disclose PHI for treatment, payment, and health care operations, including performance of the following:

A. The provision, coordination or management of health care and related services by one or more health care providers, consultation between health care providers relating to a patient, health plan member or beneficiary or the referral of a patient, health plan member or beneficiary for health care from one health care provider to another.

B. Activities undertaken to obtain reimbursement for services individuals received from HSC or another entity involved in an individual's care. Payment activities include but are not limited to billing, claims management, collection activities and related health care data processing,

determinations of eligibility and coverage to obtain payment from an individual, an insurance company or another third party.

C. Conducting quality assessment and improvement activities; reviewing the competency of health care professionals; conducting or arranging for medical review, legal services and auditing functions; business planning and development; and business management and general administrative activities.

5.2. Disclosure of PHI to a Third Party for Management and Administration.

HSC may disclose PHI to third parties for its management and administration, in accordance with Section 6.

6. Contracting with Business Associates.

HSC may enter into Business Associate Agreements to establish how Business Associates may create, maintain, use, or transmit PHI on behalf of HSC. HSC may not enter into any Business Associate Agreements in which the terms would prevent HSC from complying with any applicable law or internal policy.

6.1. Form of Business Associate Agreement. HSC will ask Business Associates to agree to and sign HSC's form of Business Associate Agreement. If a Business Associate refuses to sign HSC's form because the Business Associate (1) requests modifications to certain terms of the agreement, or (2) requests HSC to use Business Associate's form, HSC will review each request on a case-by-case basis.

6.2. Non-Compliance with Business Associate Agreement by Business Associate. If a Workforce member knows of a pattern of activity or a practice of a Business Associate that constitutes a breach or other violation of a Business Associate Agreement, the Workforce member should promptly notify the Privacy Officer.

7. Use and Disclosure of PHI.

7.1. General.

HSC may use and disclose PHI as set forth in this Policy or upon obtaining an individual's authorization on an authorization form (an "Authorization") that complies with the requirements of the Privacy Rule and other applicable law prior to using or disclosing PHI for any purpose other than (A) treatment, payment or health care operations; (B) certain public policy purposes; or (C) other limited circumstances, as permitted under applicable HIPAA provisions.

A. Use or Disclosure With an Authorization. If HSC wishes or needs to use or disclose PHI for a purpose other than as set forth in this Policy, the Privacy Officer will determine whether it is permitted to do so, and if applicable, will determine whether HSC is permitted or required to obtain an Authorization from the applicable patient or health plan member or beneficiary. Authorizations require the following procedures:

1. The member of the Workforce receiving the request should follow the procedures set forth in Section 7.8.

2. All uses and disclosures made pursuant to an Authorization must be consistent with the terms and conditions of the Authorization.

3. Disclosures must be documented in accordance with this Policy's procedures under Article 10. A copy of the Authorization should also be made available to the authorizing individual.

B. Documentation Requirements. HSC will retain all documentation concerning a use or disclosure that is made in accordance with an Authorization for a minimum of six (6) years.

7.2. Uses and Disclosures for Public Policy Purposes.

Under certain circumstances, the Privacy Rule permits HSC to use and disclose PHI without first obtaining an Authorization, on the basis of the public policy considerations identified in HIPAA. For each potential public policy exception, HSC will consult the Privacy Officer, as necessary. Such exceptions include, but are not limited to the following:

A. Disclosures about victims of abuse, neglect or domestic violence may be made, in accordance with HIPAA.

B. Disclosures may be made for judicial and administrative proceedings, in response to an order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); or a subpoena, discovery request or other lawful process, not accompanied by a court order or administrative tribunal, upon receipt of assurances that the individual has been given notice of the request or that the party seeking the information has made reasonable efforts to receive a qualified protective order.

C. Disclosures may be made to a law enforcement official for law enforcement purposes.

D. Disclosures may be made to appropriate public health authorities for public health activities.

E. Disclosures may be made to a health oversight agency for health oversight activities, as authorized by law.

F. Disclosures may be made to a coroner or medical examiner about decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.

G. Disclosures may be made for certain limited research purposes.

H. Disclosures may be made to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.

I. Disclosures may be made upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.

J. Disclosures may be made for specialized government functions, including disclosures of an inmate's PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials for the conduct of national security activities.

K. Disclosures may be made for workers' compensation purposes to the extent necessary to comply with laws relating to workers' compensation or similar programs.

L. Any other permissible purpose, in accordance with HIPAA and applicable HSC policies.

7.3. Disclosures of PHI to Business Associates.

All uses by and disclosures to a Business Associate must be made in accordance with a valid written Business Associate agreement that complies with the requirements of HIPAA. Disclosures must comply with the "Minimum Necessary" Standard.

7.4. Marketing.

Except as set forth in A. and B. below, HSC may use and disclose PHI for marketing purposes only if it first obtains an Authorization from the individual who is the subject of the PHI. The Authorization must state that there will be or may be an exchange of financial remuneration if HSC receives or may receive financial remuneration from a third party in exchange for the marketing communication.

A. Permissible Marketing Communications

1. Refill Reminders. HSC may provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, provided that any financial remuneration received by HSC in exchange for making the communication is reasonably related to HSC's cost of making the communication.

2. Treatment and Healthcare Operations. Provided HSC does not receive financial remuneration in exchange for making the communications, it may use and disclose PHI to make communications for the following purposes without obtaining prior authorization:

a. Treatment of the individual by a health care provider, including for the individual's case management or care coordination or to direct or recommend to the individual alternative treatments, therapies, health providers, or care settings.

b. To describe a health-related product or service that HSC provides; or

c. For the individual's case management or care coordination or to direct or recommend to the individual alternative treatments and related functions to the extent these activities do not fall within the definition of treatment.

B. Exceptions to the Prohibition for Marketing

A marketing communication does not require an authorization if:

1. It is in the form of a face-to-face communication made by HSC to an individual; or

2. It is a promotional gift of nominal value provided by HSC to the individual.

7.5. Fundraising.

HSC may use, or may disclose to a Business Associate or to its Foundation, PHI that may include individual demographic information, dates of service, departments of service, treating physician, outcome, and health insurance status information, for the purpose of raising funds for HSC's benefit, without the individual's authorization, so long as the following conditions are met:

A. This information may be disclosed solely for the purpose of raising funds for the benefit of HSC.

B. HSC will clearly identify this use and disclosure of PHI for fundraising purposes in its "Notice of Privacy Practices."

C. Should HSC choose to use or disclose PHI for fundraising purposes, HSC will include in each fundraising communication a clear description of how the individual may opt out of receiving any further fundraising communications. The opt-out method may not cause the individual to incur an undue burden or more than a nominal cost.

D. HSC may not send further fundraising communications to any individual who has opted out of receiving such communications. HSC may, however, provide an individual who has elected not to receive further fundraising

communications with a method to opt back in to receive such communications.

E. HSC may not condition treatment or payment on the individual's continuing receipt of fundraising communications.

7.6. Prohibition on Sale of PHI.

HSC may not request, receive or pay any cash or other remuneration in exchange for PHI, except as permitted by the Privacy Rule.

7.7. Disclosures of De-Identified Health Information and Limited Data Sets.

HSC may use PHI to create de-identified PHI or a limited data set. If the specific identifiers are removed, HSC must also lack actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

A. Procedures for De-Identification of Health Information.

HSC may determine that data is de-identified only if HSC complies with one of the following de-identification procedures.

1. De-identified under statistical methods in accordance with HIPAA, or;

2. Removal of certain identifiers in accordance with HIPAA.

B. Procedures for Limited Data Sets.

1. Creation of a Limited Data Set. A limited data set is a collection of PHI and other data that excludes "direct identifiers" of individuals who are the subject of the PHI or are a relative, employer, or household member of the individual.

2. Use of a Limited Data Set by HSC. HSC may only use or disclose a limited data set upon entering into a Data Use Agreement that complies with HIPAA.

3. Valid Purpose. HSC may only use or disclose a limited data set for research, public health, health care operations purposes, or another purpose permitted by HIPAA.

7.8. Verification of Identity and Authority.

HSC verifies the identity of a person requesting PHI ("Requestor") and the authority of any Requestor to have access to PHI.

A. Verification of Identity. Prior to disclosing PHI to a Requestor, HSC will take reasonable steps to verify the identity of the Requestor and the

authority of the Requestor to have access to such PHI. Unless a Requestor is already known to HSC at the time of the request, HSC must request reasonable proof of a Requestor's identity, for example:

1. Valid driver's license, passport or other photo identification issued by a government agency;

2. If request is made over the telephone, the address, date of birth, phone number and/or last four digit of the individual's Social Security Number;

3. If the request is made by a public official, an agency identification badge or other proof of government status, or appropriate letterhead if request is in writing.

B. Documentation. When a disclosure is conditioned on the Requestor's production of particular documentation, statements, or representations (such as disclosures for health oversight activities, judicial and administrative proceedings, or law enforcement activities), HSC will require the Requestor to provide such documentation, statements, or representations. If such reliance is reasonable under the circumstances, HSC may rely on documentation, statements, or representations that, on their face, meet the applicable requirements.

7.9. Minimum Necessary Requirements.

A. Minimum Necessary Standard. HSC makes reasonable efforts to limit the use, disclosure or request of PHI to the minimum necessary to accomplish the intended permissible purpose of the use, disclosure, or request.

1. If PHI is requested by a member of the Workforce, a Business Associate, another covered entity or a public official, members of the Workforce may reasonably rely on the request as being compliant with the "Minimum Necessary" Standard.

2. For all other requests for disclosures of PHI, members of the Workforce must determine that the amount of information disclosed meets the "Minimum Necessary" Standard to accomplish the purpose of the disclosure.

3. If a member of the Workforce requests PHI from another covered entity, such request must meet the "Minimum Necessary" Standard for the requested purpose.

4. If a member of the Workforce has a question regarding whether a use or disclosure meets the "Minimum Necessary" Standard, he or she should consult with the Privacy Officer.

B. Applicability of Minimum Necessary Standard. Generally, the minimum necessary standard will apply to all services and activities of HSC involving PHI. However, the minimum necessary standard does not apply to the following:

1. For Treatment. Disclosures to or requests by a health care provider for treatment purposes.

2. To Patient or Health Plan Member or Beneficiary. Uses or disclosures made to the subject of the PHI.

3. Pursuant to an Authorization. Uses or disclosures pursuant to a valid Authorization, in which case the extent of the disclosure must be consistent with the limitation imposed by the Authorization.

4. Required by Law. Uses or disclosures required by law.

7.10. Mitigation of Unauthorized Uses and Disclosures.

HSC must mitigate, to the extent practicable, any harmful effect that is known to HSC to have occurred as a result of a use or disclosure of PHI in violation of the requirements of the applicable Privacy Rule, Security Rule, or Breach Notification Rule provisions of this Policy by HSC or by one of its Business Associates, including the effects of any Breach.

A. Reporting to Privacy Officer. Information regarding any unauthorized use or disclosure discovered by any Workforce member of HSC will be reported promptly and directly, or indirectly through an appropriate supervisor, to the Privacy Officer at 202-466-2145 or via the toll-free confidential compliance hotline at 1-844-556-9152, including any reports of a known or potential unauthorized use or disclosure that a Workforce member receives from outside individuals.

B. Mitigation Plan. The Mitigation Plan may include the following elements, as appropriate.

1. Identifying the source(s) of the unauthorized use or disclosure and taking appropriate corrective action;

2. Contacting the recipient of the information that was the subject of the disclosure and requesting that such recipient either destroy or return the information;

3. Instructing such recipient to make no further disclosures of such information; and

4. Reviewing, and correcting where appropriate, any policy or procedure of HSC that directly caused or contributed to the disclosure.

C. Notification to Patient or Health Plan Member or Beneficiary. The Privacy Officer will notify patients or health plan members or beneficiaries regarding an unauthorized use or disclosure in accordance with the applicable provisions of HIPAA and applicable terms of the Business Associate Agreement. In the event of a Breach of Unsecured PHI or suspected Breach of Unsecured PHI by HSC, it shall comply with its Breach Notification Policy.

7.11. Government Investigations.

HSC must cooperate with government investigations in an accurate and truthful manner, in accordance with this Policy. If a Workforce member is contacted by a governmental official, the Workforce member must Call for Assistance Immediately; DO NOT Automatically Authorize Access to Property.

A. If at any time a person contacts a Workforce member and claims that he or she represents a government agency, the Workforce member will call the Privacy Officer or appropriate executive leader for assistance. Workforce members will direct any person requesting documents, information, or access on behalf of a government agency to such administrator or Privacy Officer.

B. Workforce members should do nothing to obstruct or interfere with an ongoing search pursuant to a valid search warrant.

8. Individual Rights.

8.1. Special Communication Requirements.

HSC is required to accommodate an individual's reasonable request to receive communications of his or her PHI by alternative means or at alternative locations (e.g., at patient's or health plan member's or beneficiary's business address). The following procedures apply to requests for alternative communications:

A. All requests must be in writing.

B. The member of the Workforce receiving the request should follow the procedures set forth in Section 7.8.

C. The member of the Workforce should determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual. If the request contains a statement that the disclosure could endanger the individual, the request will be honored. If no such danger exists, HSC does not need to honor the request.

D. All confidential communication requests that are approved must be notated on the individual's file clearly so that all members of the Workforce who

have access to such individual's PHI are made aware of the communication instructions. Business Associates who communicate directly with the individual must be notified of such communication requirements, as necessary.

8.2. Access to and Amendment of PHI.

Individuals have the right to access and obtain copies of their PHI that HSC (or its Business Associates) maintains in a health record. The Privacy Rule also provides that individuals may request to have their PHI amended. HSC will only consider requests for access or amendment that are submitted in writing. HSC will respond to requests for access or amendment to certain PHI according to the following procedures:

A. Requests for Access to PHI.

1. Follow the procedures for verifying the identity of the individual set forth in Section 7.8.

2. Review the disclosure request to determine whether the PHI at issue is held in the individual's health record maintained by HSC. If so, provide access in accordance with this Section.

3. Review the disclosure request to determine whether an exception to the disclosure requirement might exist. See the Privacy Officer if there is any question about whether an exception applies.

4. Respond to the request by providing the information or denying the request within 30 days. If the requested PHI cannot be accessed within the 30-day period, the deadline may be extended for 30 days, in accordance with 45 C.F.R. § 164.524.

5. If HSC does not maintain the PHI to which the individual requests access, and HSC knows where the requested information is maintained, HSC must inform the individual where to direct the request for access.

6. Provide the requested PHI in the electronic form and format requested by the individual if the PHI is maintained in one or more health records electronically, and if not readily producible in the requested form or format, in a readable hard copy form. Individuals have the right to receive a copy by mail or by e-mail or can come in and pick up a copy.

7. Provide a copy of the requested PHI to another person designated by the individual, if the individual makes such a request in a signed writing that clearly identifies the designated person and where to send the copy of the PHI.

8. If desired by HSC, charge a reasonable cost-based fee for labor for copying, postage, supplies and preparing a summary. The fee for preparing a summary must be agreed to in advance by the individual.

9. Disclosures must be documented in accordance with this Policy's procedures under Section 10.

10. A written denial notice must contain in plain language (i) the basis for the denial; (ii) a statement of the individual's right to request a review of the denial, if applicable; and (iii) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Officer.

B. Requests for Amendment of PHI.

1. Follow the procedures for verifying the identity of the individual set forth in Section 7.8.

2. Review the request for amendment to determine whether the amendment is appropriate, as outlined by the Privacy Rule.

3. Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days, in accordance with 45 C.F.R. § 164.526.

4. When an amendment is accepted, make the change in the Designated Record Set and provide appropriate notice to the individual. HSC must also make reasonable efforts to provide appropriate notice to all persons or entities listed on the individual's amendment request, if any, and also provide notice of the amendment to any persons/entities that are known to have a copy of the particular record (*e.g.* Business Associates).

5. When an amendment request is denied, the denial notice must contain (i) the basis for the denial; (ii) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (iii) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (iv) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Officer.

8.3. Accounting of Disclosures of PHI.

HSC is required to provide its patients and health plan members and beneficiaries with a list (called an accounting) of Accountable Disclosures, as set forth in HIPAA, of PHI made by HSC or its Business Associates.

A. Receipt of Request for Accounting.

1. "Accountable Disclosures" are all disclosures of PHI made by HSC or any of its Business Associates during the six (6) years prior to the date of the request as set forth under the Privacy Rule.

2. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for an accounting of Accountable Disclosures, the member of the Workforce must take the following steps:

a. Follow the procedures for verifying the identity of the individual set forth in Section 7.8.

b. If the individual requesting the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her of any fee for processing that will be charged and provide the individual with a chance to withdraw the request.

c. Respond to the request within 60 days by providing the accounting, or informing the individual that there have been no disclosures that must be included in an accounting. If the accounting cannot be provided within the 60 day period, the deadline may be extended, in accordance with 45 C.F.R. § 164.528.

B. Content of the Accounting.

HSC will provide the individual with a written accounting that includes all of the following with respect to each Accountable Disclosure:

1. The date of the disclosure;

2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;

3. A brief description of the PHI disclosed; and

4. A brief statement of the purpose of the disclosure.

8.4. Individual's Right to Request Restrictions on Certain Uses and Disclosures.

HSC will accommodate reasonable requests to restrict use and disclosure of PHI.

A. All requests for restrictions on the use and disclosure of an individual's PHI must be in writing. The member of the Workforce who receives the written request should follow the procedures set forth in Section 7.8.

B. HSC must honor requests to restrict disclosure of PHI to a health plan if the disclosure is for purposes of carrying out payment or health care operations and is not otherwise required by law and the PHI pertains solely to a health care item or service for which the individual (or person on behalf of the individual other than HSC) has paid in full. Other requests must be presented to the Privacy Officer, who will determine whether HSC will honor the request.

C. To the extent necessary, all Business Associates that may have access to the individual's PHI must be notified of any agreed-to restrictions.

8.5. Complaints.

The Privacy Officer will be HSC's contact person for receiving complaints about HSC's privacy procedures and for handling such complaints. No member of the Workforce may intimidate, threaten, coerce, discriminate against or take other retaliatory action against individuals for filing a complaint, participating in an investigation or opposing any improper practice under the Privacy Rule. No individual shall be required to waive his or her privacy rights under the Privacy Rule as a condition of treatment, payment, enrollment or eligibility.

9. Responding to Breaches and Unauthorized Uses and Disclosures.

HSC will presume that any acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule is a Breach that requires notification to affected individuals or to their personal representatives, unless an exception applies or HSC demonstrates there is a low probability that the Unsecured PHI has been compromised based on a risk assessment (HSC's Breach Notification Risk Assessment form is attached as Exhibit A).

9.1. Breach of Unsecured PHI. In the event of a Breach of Unsecured PHI or suspected Breach of Unsecured PHI, HSC shall comply with its Breach Notification Policy (see ET.23 HSC Breach Notification Policy).

9.2. Investigate and Mitigate. HSC will conduct an investigation of an event that is an actual or potential Breach, an unauthorized use or disclosure of PHI, and/or a Security Incident. HSC will take appropriate corrective and remedial action of a confirmed Breach, unauthorized use or disclosure, and/or Security Incident.

9.3. Additional State Law Considerations. HSC will evaluate applicable state laws individually to comply with any additional requirements pertaining to Breaches, including more restrictive reporting timeframes.

9.4. Workforce Reporting. If a member of the Workforce becomes aware of a disclosure of PHI, either by a Workforce member or a Business Associate that is not in compliance with this Policy, the Workforce member shall contact the Privacy Officer and work with the Privacy Officer and legal counsel, as applicable.

10. Documentation.

This Policy, and HIPAA-related policies and procedures, shall be maintained for at least six (6) years from the later of the date of creation or when it was last in effect and shall be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including HIPAA changes and modifications). Any changes to this Policy, and to HIPAA-related policies and procedures, shall be documented.

10.1. Procedures.

A. The Privacy Officer shall maintain copies of the following items.

1. "Notices of Privacy Practices" that are issued to individuals who receive services from HSC.

2. The information required to provide an accounting of disclosures of Accountable Disclosures, in compliance with the requirements of 45 C.F.R. § 164.528.

3. Individual Authorizations received by HSC.

4. Restrictions on PHI to which HSC has agreed.

5. This Policy, and related HIPAA policies/procedures, and revisions to them.

6. Records of training.

7. Sanctions applied to members of the Workforce who violate this Policy.

8. Business Associate Agreements.

9. Complaints and resolutions regarding HIPAA.

B. Documentation of the foregoing may be maintained in either written or electronic form.

11. Notice of Privacy Practices.

HSC must publish and provide to individuals a Notice of Privacy Practices that generally describes its privacy practices. HSC must at all times maintain a Notice of Privacy Practices that conforms to the requirements of the Privacy Rule.

11.1. HSC must provide a copy of its Notice of Privacy Practices to the individual no later than the date of the first service delivery.

11.2. HSC must make available its Notice of Privacy Practices to any person who requests it.

11.3. Except in an emergency situation, upon the initial provision of the Notice of Privacy Practices, members of the Workforce will make a good faith effort to obtain the individual's signed acknowledgement of receipt of the Notice of Privacy Practices. If an acknowledgement is not obtained, members of the Workforce will document on the unsigned acknowledgement the members of the Workforce's good faith efforts to obtain such acknowledgement and the reason why the acknowledgement was not obtained.

11.4. If the Notice of Privacy Practices is materially changed, HSC will make it available upon request and post the revised version on its website.

12. Mobile Devices and Media.

12.1. Protecting Mobile Devices.

All users of Mobile Devices and Mobile Media, including but not limited to all USB or portable hard drives (collectively, "Mobile Device"), whether the equipment or media is personal or owned by HSC, assume responsibility for ensuring compliance with this Policy. This particularly means that Workforce members must take the necessary precautions to prevent potential loss or theft. When traveling, Workforce members should be aware of the location and circumstances of the Mobile Device at all times and may additionally take the following measures to protect the Mobile Device: (1) on flights, carry the Mobile Device in your hand luggage; (2) in a vehicle, lock it in the luggage compartment when you leave the vehicle; (3) in hotels, lock it in a safe or cabinet; and (4) in public areas, never leave the Mobile Device unattended.

No EPHI shall be maintained on HSC's Mobile Devices unless authorized and necessary and HSC's encryption program/system functions have been activated to ensure that the EPHI is secure.

12.2. Unauthorized Access; Password Protection.

A Mobile Device must be protected against unauthorized access at all times. Workforce members must take reasonable actions to secure the Mobile Device. Password protection must be enabled on all Mobile Devices. This is to protect against information loss should the Mobile Device be lost or stolen.

12.3. Stolen or Lost Mobile Device or Media.

If any Mobile Device is lost or stolen, the Workforce member must report the incident immediately to the Privacy Officer and advise if any confidential information was contained on the Mobile Device. Personal passwords must be immediately changed. HSC may remotely wipe

or otherwise disengage any data or program on the stolen or lost media to limit risks to confidentiality of material maintained on the Mobile Device.

12.4. Removal from Facilities.

Workforce members may take Mobile Devices out of HSC's facilities only within the framework of the work required of them. The Workforce member assumes personal responsibility for taking any protective measures that may be necessary during transport, use, and storage, including but not limited to encryption where reasonable and appropriate. He or she is also responsible for returning HSC's equipment and information intact.

Chief HR and Compliance Officer _4/11/2018_

Approval Signature Title Date

Exhibit A

<table>
<tr><th colspan="4">Breach Notification Risk Assessment</th></tr>
<tr><td colspan="2">Investigator</td><td>Start Date</td><td>End Date</td></tr>
<tr><td colspan="2">Department</td><td colspan="2">Location of Incident</td></tr>
<tr><td>Occurrence Date</td><td>Discovery Date</td><td>Date Reported</td><td>Number of Affected Individuals (Scope)</td></tr>
<tr><td colspan="4"><u>Breach of PHI</u>?</td></tr>
<tr><td colspan="4">1. Was information acquired, accessed, used or disclosed?

If no, it is unlikely that a Breach has occurred.</td></tr>
<tr><td colspan="4">2. Is the information involved PHI?

If no, it is unlikely that a Breach has occurred.</td></tr>
<tr><td colspan="4">2a. Is the incident a HIPAA Privacy Rule violation?

If yes, it is unlikely that a Breach has occurred.</td></tr>
<tr><td colspan="4">2b. Is the PHI involved secure (i.e. encrypted or otherwise rendered unusable, unreadable to unauthorized individuals)?

If yes, it is unlikely that a Breach has occurred.</td></tr>
<tr><td colspan="4"><u>Breach Exception?</u></td></tr>
<tr><td colspan="4">Does the incident fall under one the following exceptions?

1) A good faith unintentional acquisition, access or use of PHI by a workforce member, acting under the authority of a covered entity or business associate, if such acquisition, access or use was made within the scope of authority and does not result in the further use or disclosure in a manner not permitted under the Privacy Rule; or

2) An inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, and the information received is not further used or disclosed in a manner not permitted under the Privacy Rule; or

3) A disclosure of PHI, where a covered entity or business associate has a good faith belief that an unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

If yes, it is unlikely that a Breach has occurred.</td></tr>
</table>

Note! **An acquisition, access, use or disclosure of unsecured PHI is presumed to be a Breach unless an exception above is met or a low probability that the PHI has been compromised is demonstrated based on the Risk Assessment herein. Automatic Notification is permitted without conducting the Risk Assessment.**
Risk Assessment
1. What is the nature and extent of the PHI involved in the incident? (Required under HIPAA)
1a. What PHI is involved (e.g. SSN, DOB, diagnosis, medications)?
1b. What sensitive PHI is involved (e.g. mental health, HIV, substance abuse)?
1c. What financial information is involved (e.g. SSN, credit card or bank account numbers)?
1d. What is the likelihood the data could be re-identified based on the context and ability to link the data with other available information (e.g. could an individual be identified based on a trait in conjunction with public records)?
2. Who used the PHI or to whom was the impermissible disclosure made? (Required under HIPAA)
2a. Does the person in receipt of the PHI have an obligation to protect the information (e.g. another entity governed by HIPAA)?
2b. Was the PHI disclosed outside of an entity or defined group?
3. Was the PHI actually acquired or viewed? (Required under HIPAA)
4. To what extent has the risk to the PHI been mitigated? (Required under HIPAA)
4a. What corrective action steps have been taken?

4b. Has the date been returned, remotely wiped, destroyed?
4c. Has unauthorized recipient of the PHI provided satisfactory assurances that the information will not be further used or disclosed or will be destroyed?
5. What employee, department and/or Business Associate is responsible for the Breach?
6. What applicable safeguards were in place prior to incident (e.g. locked file cabinets, badge entry, encryption, firewalls, passwords, biometrics or other technological barriers)?
7. In the following questions, the probability that PHI has been compromised increases with the chosen response (moving left to right, with the last response having the highest probability of compromise):
7a. Method of incident: Verbal. Paper. Electronic. 7a.1. If electronic: Desktop computer. Portable device. Server.
7b. Recipient(s) of PHI: Internal workforce. External workforce. General public/Unknown.
7c. Circumstances of incident: Unintentional. Lost/Theft. Hack/Malicious/Targeted theft.
7d. Location of PHI subsequent to incident: Returned. Destroyed. Unknown. Re-disclosed.
7e. Controls implemented: PHI de-identified. PHI encrypted. PHI password protected. None.
7f. Future risk: None/Destroyed. PHI re-identifiable. PHI reusable. PHI re-disclosed.

8. What additional facts, specific to this incident, are notable in determining the probability that the PHI has been compromised?

Status of Risk Assessment: Open / Closed

Based on the preceding, is there a low probability the PHI involved in the Breach has been compromised?

☐ **Yes, based on the Risk Assessment, there is low probability of compromise and, therefore, HSC is not required to provide Notification.**

☐ **No, based on the Risk Assessment, the probability of compromise is greater than "low," therefore, HSC will provide Notification.**

Risk Assessment completed by:

Print Name	**Title**
Signature	**Date**