Greater Houston HealthConnect

HIPAA/HITECH Privacy Compliance Manual

Adopted by the Board of Directors on December 14, 2011 and amended on September 12, 2012 and February 27, 2013
# Table of Contents

1. Definitions ................................................................. 3
2. Privacy Officer Policy .................................................... 7
3. Individual Authorization Policy ......................................... 9
4. Individual Access to PHI Policy ........................................ 11
5. Amendment of PHI Policy ............................................... 12
6. Policy and Procedure on Restrictions by Individual or Participant on the Use of PHI ......................................................... 13
7. Accounting to Individuals Policy and Procedure .................... 14
8. Documentation of Health Oversight Agency or Law Enforcement Request to Temporarily Suspend an Accounting to an Individual ................................................................. 17
9. Policy for Maintaining Confidentiality of PHI by GHH .......... 18
10. Confidentiality Agreement for GHH Workforce ................... 20
11. Policy on Uses and Disclosures Authorized by Law .............. 21
12. Minimum Necessary Policy and Procedure for GHH Workforce ......................................................................................... 22
13. GHH and Participant Workforce Training Policy ............... 24
14. Compliance with Texas Notice Requirements ..................... 26
15. Unsecured PHI Breach Notification Policy ......................... 28
16. Breach Notification Risk Assessment Form ......................... 37
17. Individual Breach Notification Letter Form ....................... 40
18. Destruction/Disposal of Individual PHI by GHH .............. 42
19. Certificate/Record of Destruction ...................................... 56
20. Telephone Policy for GHH ............................................... 58
18. Policy for Disciplinary Action for GHH Workforce ............ 60
19. Sanctions Record ............................................................ 63
20. Complaint Policy ............................................................ 64
22. Participant Agreement Policy ............................................ 67
23. Policy for Business Associates of GHH ............................. 69
Greater Houston Healthconnect ("GHH" or "Exchange") is a health information exchange. This Manual is designed to be used when a Participant in the Exchange has agreed to participate in the Hub Services offered by GHH. This Manual is designed to assist GHH and such Participants in complying with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy standards, the Health Information Technology for Economic and Clinical Health Act ("HITECH") (collectively referred to as "HIPAA" in this Manual), and Texas laws relating to patient privacy. GHH has a separate HIPAA Security Manual. GHH firmly believes the Protected Health Information ("PHI") of individuals must be treated with the utmost confidentiality and security.

If you have any questions or concerns at any time, please feel free to contact me directly.

Sincerely,

Phil Beckett
GHH Privacy Officer
1. DEFINITIONS

1. Designated Record Set: A designated record set includes:
   
   A. Records and billing records about individuals maintained by or for a covered health care provider; or
   
   B. A group of records used, in whole or in part, by or for the covered entity to make decisions about individuals; or
   
   C. The enrollment, payment, claims adjudications, and case or medical management record systems maintained by or for a health plan.

2. Record: The term “record” means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

3. Disclosure: applies to the external release of information outside the covered entity.

4. Exchange: is the Greater Houston Healthconnect (“GHH”).

5. HUB: means the electronic system that is made available by GHH to Participants to enable Participants to exchange PHI between Participants.

6. Health Care Operations: any of the following activities of the covered entity to the extent that the activities are related to covered functions:

   A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development case management and care coordination, contacting of health care providers and individuals with information about treatment alternatives; and related functions that do not include treatment;

   B. Reviewing the competence or qualifications of health care professionals, evaluating professional performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training on non-health care professionals, accreditation, certification, licensing, or credentialing activities;

   C. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating
to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

D. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

E. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

F. Business management and general administrative activities of the entity, including, but not limited to:

   a. Management activities relating to implementation of and compliance with the requirements of this subchapter;

   b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers provided that PHI is not disclosed to such policy holder, plan sponsor, or customer; and

   c. Resolution of internal grievances.

G. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

H. Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

7. **Individually Identifiable Health Information**: is information that is a subset of health information, including demographic information collected from an individual, and:

   A. Is created or received by a health care provider, health plan, employer or health care clearinghouse,

   B. Relates to the past, present, or future physical or mental health or 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 an individual;

   C. That identifies the individual; or
D. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

8. **Minimum Necessary Standard**: When using or disclosing PHI or requesting PHI from another covered entity, GHH must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

9. **Participant**: means a health care provider, health care entity, or payer who enters into a Participation Agreement with GHH.

10. **Payment**: consists of those activities undertaken by GHH to obtain or provide reimbursement for the provision of health care. These activities relate to the individual to whom health care is provided and include:

A. Determinations of eligibility of coverage (including coordination of benefits or the determination of cost sharing amounts), and the adjudication or subrogation of health benefit claims;

B. Billing, claims management, collection activities;

C. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

D. Utilization review activities, including pre-certification and pre-authorization of services; and

E. Disclosure to consumer reporting agencies for purposes related to collection of premiums or reimbursement. Only the following information may be disclosed: Name, address, date of birth, social security number, payment history, account number, and the name and address of the health care provider or health plan.

11. **Protected Health Information (“PHI”)**: Protected Health Information is defined as individually identifiable health information that is transmitted by electronic media, and transmitted or maintained in any other form or medium.

HIPAA considers the following personal identifiers PHI:

A. Name

B. All geographic subdivisions smaller than state of residence

C. All elements of dates (except year) for dates directly related to an individual, including birth date; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
D. Telephone number
E. Fax number
F. Electronic mail addresses
G. Social security number
H. Record number
I. Health plan beneficiary number
J. Account number
K. Certificate/license number
L. Vehicle identification numbers such as serial and license numbers
M. Device identifiers and serial number
N. Web Universal Resource Locators (URLs)
O. Internet Protocol (IP) address numbers
P. Biometric identifiers, including finger and voice prints
Q. Full Face photographic image
R. Any other unique identifier, identifying number, characteristic, or code.

12. **Treatment**: means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an individual; or the referral of an individual for health care from one health care provider to another.

13. **Use**: means with respect to individually identifiable information, means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

14. **Workforce**: means employees, volunteers, and any other individual performing work for GHH or a Participant who is under the direct control of GHH or Participant (as applicable), regardless of whether paid or not.
2. PRIVACY OFFICER POLICY

<table>
<thead>
<tr>
<th>POLICY AND PROCEDURES</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPARTMENT:</td>
<td>POSITION:</td>
</tr>
<tr>
<td>SUBJECT: Privacy Requests</td>
<td>Privacy Officer</td>
</tr>
</tbody>
</table>

| Date issued: December 14, 2011; as amended September 12, 2012 | Page: |

PURPOSE:

To maintain accountability for privacy within GHH’s practice.

POLICY:

1. GHH designates Phil Beckett as the GHH Privacy Officer. The GHH Privacy Officer may be contacted at 832-564-2599 and all correspondence may be mailed to:

   Phil Beckett  
   Greater Houston Healthconnect  
   1213 Hermann Drive, Suite 135  
   Houston, Texas 77004

   Or by email to Phil.Beckett@ghhconnect.org.

2. The GHH Privacy Officer will oversee GHH’s Privacy Program, including:

   A. Developing and implementing privacy policies, in accordance with federal and Texas privacy requirements.

   B. Overseeing that all Participants of the Workforce who come into contact with PHI are properly trained.

   C. Providing Notice as required by state law.

   D. Mitigating the effects of all disclosures that are not compliant with federal or Texas law or that are contrary to GHH’s Privacy Policies and Procedures.

   E. Conducting, at least annually, a review of GHH’s access procedures for individuals.
F. Guiding and assisting in the identification, implementation, and maintenance of privacy policies and procedures in coordination with GHH’s management, GHH Participants and legal counsel.

G. Reviewing all system-related information security plans in order to align security and privacy practices.

H. Performing initial and periodic risk assessments or “privacy audits” and conducting ongoing compliance monitoring activities.

I. Overseeing compliance with privacy practices and application of sanctions for failure to comply with privacy policies.

J. Complying with HIPAA, HITECH and Texas law on disposal of PHI.

This list provides an overview of the GHH Privacy Officer duties and is not meant to serve as an all-inclusive list.
3. INDIVIDUAL AUTHORIZATION POLICY

POLICY AND PROCEDURES

GHH

Date issued: December 14, 2011

DEPARTMENT: |
POSITION: |

Cites: |
45 CFR 164.508 |

Policy No: |

Page: |

SUBJECT: Authorization

PURPOSE:

To secure appropriate authorization from individuals prior to transmitting PHI through the Exchange

POLICY:

1. No PHI will be transmitted through the Exchange until the individual has signed an authorization allowing his or her PHI to be transmitted through the Exchange. The authorization must have language approved by GHH.

2. The Exchange will use an opt-in process, and will not segment PHI. This means that all PHI about that individual will be available through the Exchange, including alcohol and substance abuse, HIV/Aids, mental health and psychotherapy notes, STDs, hepatitis and genetic testing.

3. Participants are responsible for complying with all state laws, THSA regulations, and HIPAA requirements governing authorization. Participants shall ensure that the authorization form incorporates all law and HIPAA requirements. Participants shall indemnify the Exchange against any and all causes of action and damages based on use by Participant of an authorization form that fails to comply with state and federal law.

4. When a Participant obtains an individual’s written or electronic authorization to transmit his/her PHI through the Exchange, the Participant will be keep such authorization on file at the Participant office or facility.

5. An individual may revoke an authorization at any time, provided the revocation is in writing. GHH will stop transmitting information about that individual as soon as possible but at least within seventy-two (72) hours of receipt of written notice that an individual has revoked his/her authorization. GHH will not be liable for use or disclosure of an individual’s PHI after a revocation if:

   • GHH is not made aware that an individual revoked his/her authorization; or
• GHH, in good faith, based its actions upon a prior authorization, and has already acted in reliance on that authorization.

APPROVAL:

________________________________________________________________________
Privacy Officer
Signature

Date

________________________________________________________________________
[Office (capacity)]
Signature

Date
# 4. INDIVIDUAL ACCESS TO PHI POLICY

## POLICY AND PROCEDURES

<table>
<thead>
<tr>
<th>DEPARTMENT:</th>
<th>POSITION:</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Date issued: December 14, 2011</td>
</tr>
</tbody>
</table>

### SUBJECT: Access to PHI

### PURPOSE:
To refer all requests for access by an individual to his/her PHI to the applicable Participant(s).

### POLICY:

1. GHH is not a direct provider of care and does not maintain a Designated Record Set.

2. GHH acknowledges that individuals have a right to access, inspect and obtain a copy of PHI about them, with limited exclusions, for as long as the PHI is maintained in a designated record set. If GHH receives requests for access to PHI, GHH shall forward such requests, or inform requestors, to contact the applicable Participant(s).

3. Participant will inform individuals of the process for requesting access to information used and disclosed through the Exchange directly from the Participant in Participant’s Notice of Privacy Practices.

### PROCEDURE:

GHH will maintain a log record of all requests for access.
### 5. AMENDMENT OF PHI POLICY

<table>
<thead>
<tr>
<th>POLICY AND PROCEDURES</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEPARTMENT:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>POSITION:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SUBJECT:</strong> Amendment to Protected Health Information</td>
<td><strong>Cite(s):</strong> 45 CFR 164.526</td>
</tr>
<tr>
<td><strong>Date issued:</strong></td>
<td>December 14, 2011</td>
</tr>
<tr>
<td><strong>Policy No:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Page:</strong></td>
<td></td>
</tr>
</tbody>
</table>

**PURPOSE:**

To clarify that only Participants will amend PHI used and disclosed to or through the Exchange.

**POLICY:**

1. Individuals have the right to amend their PHI or information used and disclosed to or through the Exchange. Individuals must make requests for amendment in writing, directly to a Participant and must include the reason for making the request.

2. In the event that GHH receives a request for an amendment directly from an individual, GHH shall forward the written request, or refer the individual directly, to the applicable Participant(s).

3. GHH shall maintain a log of all requests for amendments made directly to GHH.
6. POLICY AND PROCEDURE ON RESTRICTIONS BY INDIVIDUAL OR PARTICIPANT ON THE USE OF PHI

<table>
<thead>
<tr>
<th>POLICY AND PROCEDURES</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEPARTMENT:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>POSITION:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SUBJECT:</strong> Right of an Individual to Request Restriction of Uses and Disclosures</td>
<td></td>
</tr>
<tr>
<td><strong>Date issued:</strong></td>
<td>December 14, 2011</td>
</tr>
<tr>
<td><strong>Cite(s):</strong></td>
<td>45 CFR 164.502(c); 45 CFR 164.522(a) as amended by HITECH Act §13405(a) and NPRM dated July 14, 2010</td>
</tr>
<tr>
<td><strong>Policy No:</strong></td>
<td>A008</td>
</tr>
</tbody>
</table>

**PURPOSE:**

To clarify that participation with GHH is based on authorization signed by individuals agreeing to allow use and disclosure of all his/her PHI to and through the Exchange. PHI subject to restrictions will not be transferred through the Exchange by Participants.

**POLICY:**

1. GHH will not restrict use and disclosure of an individual’s PHI.
2. Because GHH will not segment PHI in the Exchange, upon notice from a Participant that he/she has agreed to a restriction, GHH will initiate procedures to shut down further use or disclose of that individual’s PHI through the Exchange.
3. In the event GHH receives a request to restrict use and disclosure of PHI directly from an individual, GHH will forward the written request, or refer the patient who calls with such a request, to the Participant.
4. GHH shall maintain a log of all such requests for restrictions.
7. ACCOUNTING TO INDIVIDUALS POLICY AND PROCEDURE

PURPOSE:
To establish a policy and procedure by which individuals are informed of certain disclosures made regarding their PHI by GHH.

POLICY:¹

1. Upon written request, an individual has a right to receive an accounting of certain disclosures of PHI made by GHH and its Business Associates.

2. GHH must be able to provide an accounting of all transmissions made through GHH and its Business Associates per current law.

3. GHH must provide the individual with a written accounting that includes:
   A. The date of the disclosure;
   B. The name of the entity or person who received the PHI, and if known, the address of such entity or person;
   C. A brief description of the PHI disclosed; and
   D. A brief statement of the purpose of the disclosure pursuant to the Business Associate Agreement that reasonably informs the individual of the basis for the disclosure.

4. GHH must act on an individual’s request for an accounting no later than sixty (60) days after the receipt of such a request.

5. If GHH is unable to comply within the sixty (60) days of the deadline, GHH may extend the deadline by no more than thirty (30) days. GHH must notify the individual, within the initial sixty (60) days, with a written statement of the

¹ Section 13400 of the HITECH Act defines an EHR as “an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.”
reasons for the delay and the date by which the accounting will be provided. GHH is entitled to only one extension.

6. GHH shall provide the first accounting to an individual in any 12-month period without charge. GHH may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period. GHH may recoup reasonable retrieval and preparation costs, as well as any mailing costs incurred. GHH shall inform the individual in advance of the fee; and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

7. GHH shall maintain documentation of all accountings required by current law.

8. If a health oversight agency or law enforcement official provides a written statement that an accounting will reasonably likely impede the agency’s activities, GHH may temporarily suspend an individual’s right to receive an accounting.

9. If a health oversight agency or law enforcement official orally requests that the accounting of disclosures be temporarily suspended, then GHH shall:
   A. Document the statement, including the identity of the agency or official making the statement;
   B. Temporarily suspend the individual’s right to receive an accounting of such disclosures; and
   C. Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

10. GHH should contact its attorney when such requests are made.

PROCEDURE:

Maintaining Documentation of Disclosure of Information

1. GHH’s Privacy Officer is responsible for receiving and responding to requests for accountings.

2. GHH will document and retain the information required to be included in an accounting for disclosures of PHI.

3. GHH will document and retain the written accounting provided to the individual as required by law.

Initial Processing of Individual’s Request

1. Requests for an accounting from GHH must be in writing.
2. GHH provides up to two (2) accountings per individual without charge, within a 12-month period. Additional accountings requested within the same 12-month period will be provided at a cost of $5.00 each. If the individual chooses to withdraw his/her request, this should be noted on the request form and signed by both the Privacy Officer and the individual.

3. Once the signed request is received, GHH’s Privacy Officer will enter the request in an Accounting Request Log.

4. Upon receipt of the individual’s signed written request, GHH has sixty (60) days to process the request.
8. DOCUMENTATION OF HEALTH OVERSIGHT AGENCY OR LAW ENFORCEMENT REQUEST TO TEMPORARILY SUSPEND AN ACCOUNTING TO AN INDIVIDUAL

<table>
<thead>
<tr>
<th>On</th>
<th>(date)</th>
<th>(name)</th>
<th>(badge or ID number)</th>
<th>with</th>
<th>(agency)</th>
<th>in accordance with</th>
<th>(law or safety regulation)</th>
</tr>
</thead>
</table>

orally requested that Greater Houston Healthconnect (“GHH”) temporarily suspend the accounting of disclosure of **(individual’s name)**.

GHH shall comply with such request until **(date – 30 days from the date of the oral statement)**. The compliance date may be extended should a written statement be submitted.
9. POLICY FOR MAINTAINING CONFIDENTIALITY OF PHI BY GHH

POLICY AND PROCEDURES

<table>
<thead>
<tr>
<th>DEPARTMENT:</th>
<th>POSITION:</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SUBJECT: Confidentiality of PHI

Date issued: December 14, 2011

PURPOSE:

To implement procedures to protect an individual’s PHI.

POLICY:

1. **Protection of PHI:** All Workforce members, directors, officers, contractors, and agents of GHH are responsible for protecting the privacy and security of all PHI that is received, whether orally or recorded, in the course of their work. An individual’s PHI shall be protected from the moment it is received, used, stored, and eventually destroyed.

2. **Confidentiality Agreement:** Each Workforce member, full-time employee, temporary employee, consultant, contracted employee, subcontractor, vendor, and business associate shall be required to sign a confidentiality agreement or, where applicable, a business associate agreement, upon commencing work or entering into a contractual relationship with GHH.

   A. All Workforce members, as a condition of employment, are required to sign the confidentiality agreement.

   B. Copies of the agreement shall be maintained in the Workforce member’s personnel file.

   C. Where required by HIPAA or Texas law, contractors who meet the definition of a business associate shall be required to execute a business associate or chain of trust partner agreement. All other contractors must sign a confidentiality agreement if the service involves the incidental use or disclosure of PHI.

3. **Protection of PHI – Hard Copies:** All PHI shall be maintained in a confidential manner that prevents unauthorized disclosure, either internally or to third parties. GHH shall make all reasonable efforts to secure records containing PHI.
A. All PHI in hard copy form shall be kept in locked files with the number of keys limited to Workforce members whose work requires regular access to the information.

B. Documents shall be destroyed in a method that induces complete destruction of the information when the information is no longer needed.

4. **Procedure if a Breach is Alleged**: All breaches of confidentiality shall be reported to the Privacy Officer.

   A. Any Workforce member receiving an allegation of a breach of confidentiality or having knowledge or a reasonable belief that a breach of confidentiality of PHI may have occurred shall immediately notify the Privacy Officer.

   B. If it is determined that a breach of confidentiality of PHI has occurred, disciplinary action shall be taken in accordance with GHH’s disciplinary policy.

   C. The GHH Privacy Officer shall retain documentation of all allegations that have been made and any action taken in a master employee HIPAA complaint file and in the Workforce member’s personnel file. A separate, secure file shall be maintained for documentation concerning violations by non-employees.
10. CONFIDENTIALITY AGREEMENT FOR GHH WORKFORCE

I have read and understand Greater Houston Healthconnect (“GHH”) Confidentiality Policies on the use, collection, disclosure, storage, and destruction of Protected Health Information (“PHI”).

I agree to follow the Confidentiality Policies and all related policies. I agree that while I am employed or have a contract with GHH, I will not reveal or disclose PHI to any person except as authorized by this policy and Texas and federal law.

I further understand that my obligations to maintain the confidentiality of PHI will continue after my employment or association with GHH ends.

Finally, I understand that unauthorized use or disclosure of PHI may result in disciplinary action, which may include termination of employment or contract, the imposition of civil and criminal fines pursuant to Texas and federal laws, and reporting to any appropriate professional licensing board.

________________________________________________________________________
Employee Signature

________________________________________________________________________
Employee Name

________________________________________________________________________
Date

I have discussed GHH’s Confidentiality Policies and the appropriate use, collection, disclosure, storage, and destruction of PHI with named employee or Workforce member. I have also discussed the consequences of a breach and provided an opportunity for questions.

________________________________________________________________________
Privacy Officer’s Signature
11. POLICY ON USES AND DISCLOSURES AUTHORIZED BY LAW

POLICY AND PROCEDURES

GHH

Date issued: December 14, 2011

DEPARTMENT: POSITION: Cites: 45 CFR 164.512 Policy No: 
SUBJECT: Uses and Disclosure Authorized by Law Page:

PURPOSE:

To establish a procedure for releasing PHI when required by law.

POLICY:

GHH shall comply with state and federal laws that require GHH to release PHI when required by law to do so.

PROCEDURE:

Before releasing PHI as required by law, GHH must:

1. **Verify Identification**
   
   A. The identity of an individual/entity shall be verified by obtaining a written documentation, statement, or representation from the requesting individual.
   
   B. The presentation of an agency identification badge, other official credential, or other proof of government status if made in person shall be sufficient to verify a public official’s identity.

2. **Verify Authority.** Prior to releasing PHI, GHH shall make good faith efforts to verify the legal authority of any person requesting protected information to have access to the PHI.

3. **Limit Disclosure to the Minimum Necessary.** All disclosures of PHI shall be limited to the minimum amount of PHI necessary to achieve the intended purpose of the release.

4. **Uses and Disclosures Required by Law.** The release must be limited to the relevant requirements of such law.

---

2 Disclosures must be “required” as opposed to “permitted” or “authorized” by law.
12. MINIMUM NECESSARY POLICY AND PROCEDURE FOR GHH WORKFORCE

**PURPOSE:**

To limit use and disclosure of PHI by all Workforce members of GHH to the minimum amount of information necessary to accomplish their job duties or functions. Further, to make reasonable efforts to limit use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose.

**POLICY:**

**A. Uses.**

1. GHH will identify:
   
   A. The persons or classes of persons in its Workforce who need access to PHI to carry out their job duties;
   
   B. The categories or types of PHI needed; and
   
   C. The conditions appropriate to such access.

2. Workforce members’ access to PHI shall be solely on a “need to know” basis. Workforce members’ use or disclosure of PHI shall be limited to that PHI needed to perform job responsibilities and duties.

**B. Routine or Recurring Requests and Disclosures.**

1. For routine and recurring requests and disclosures, GHH will develop and implement standard protocols.

2. Non-routine requests for, and disclosures of, PHI shall be reviewed by the Privacy Officer individually or designee. GHH shall develop and implement criteria designed to limit its requests for PHI to the minimum necessary to satisfy the request or accomplish the intended purpose.

**B. Reasonable Reliance.** GHH shall rely on a GHH Participant’s request for PHI as the minimum necessary for the intended disclosure.
D. **Information Systems.** All information systems will be redesigned, in accordance with GHH’s available resources, to meet the minimum necessary provisions of HIPAA. This is to be accomplished by removing identifiers and removing data fields not necessary to performing the primary purpose of the use or disclosure.

**PROCEDURE**

1. The Privacy Officer will determine Workforce member access to PHI based on job duties and functions and will document in individual’s personnel file. Determination of access will be based on:

   A. Employees or classes of employees who need access to PHI to carry out their daily functions.
   
   B. For each class of employee, the category or categories of PHI to which access is needed.

2. In general, PHI used internally at GHH may be used by GHH personnel to facilitate exchange of information between Participants for treatment, payment or other healthcare operations of GHH Participants. PHI may not be released outside of GHH unless it is to:

   A. A business associate with whom GHH has a Business Associate Agreement or a Participant; or
   
   B. As otherwise required by law.
### 13. GHH AND PARTICIPANT WORKFORCE TRAINING POLICY

<table>
<thead>
<tr>
<th>POLICY AND PROCEDURES</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEPARTMENT:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>POSITION:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SUBJECT:</strong> Privacy Requirement Training</td>
<td><strong>Date issued:</strong> December 14, 2011</td>
</tr>
<tr>
<td><strong>Policy No:</strong></td>
<td>45 CFR 164.530</td>
</tr>
<tr>
<td><strong>Page:</strong></td>
<td></td>
</tr>
</tbody>
</table>

**PURPOSE:**

To establish a policy for privacy training.

**POLICY:**

**Training of GHH Workforce**

1. The establishment of privacy training courses for GHH will be the responsibility of the GHH Privacy Officer.

2. All members of GHH’s Workforce who come into contact with PHI in performing their job function will be trained on the privacy laws, policies, and procedures regarding PHI. The following Workforce members will be trained:

   A. All current Workforce members.

   B. Workforce members whose duties are affected by a material change in privacy policies will be re-trained within two (2) months after the change becomes effective.

   C. Workforce members who have violated privacy laws, policies, or procedures shall be re-trained within thirty (30) days of the determination.

3. The GHH Privacy Officer shall document each training session and the names of the Workforce members who completed training. Such documentation will be maintained in GHH’s privacy records.
Training of Participant Workforce

1. Each Participant shall allow access to the Exchange only by those Workforce members who have a legitimate and appropriate need to use the HIE and/or release or obtain information through the Exchange. No Workforce member shall be provided with access to the Exchange without first having been trained on these Policies.

2. **Training.** Each Participant shall develop and implement a training program for its Workforce members who will have access to the Exchange to ensure compliance with these Policies. The training shall include a detailed review of applicable Policies and each trained Workforce member shall sign a representation that he or she received, read, and understands these Policies.

3. **Discipline for Non-Compliance.** Each Participant shall implement procedures to discipline and hold Workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with these Policies. Such discipline measures shall include, but not be limited to, verbal and written warnings, demotion, and termination and provide for retraining where appropriate.

4. **Reporting of Non-Compliance.** Each Participant shall have a mechanism for, and shall encourage, all Workforce members, to report any non-compliance with these Policies to the Participant. Each Participant also shall establish a process for individuals whose health information is included in the Exchange to report any non-compliance with these Policies or concerns about improper disclosure of information about them.
14. COMPLIANCE WITH TEXAS NOTICE REQUIREMENTS

POLICY AND PROCEDURES

DEPARTMENT: | POSITION:  
---|---
SUBJECT: Provision of Notice

**GHH**

Date issued: December 14, 2011

Cite(s): 45 CFR 164.502(i);
45 CFR 164.520(a)(b)(c)(e)
Texas Health & Safety Code
§181.54

POLICY:

Provision of Notice

As required by Section 181.154 of the Health and Safety Code, GHH will provide notice to individuals that their PHI is subject to electronic disclosure and explain how an HIE facilitates the exchange of data to promote individual's health. GHH is a covered entity under state law as are Participants.

PROCEDURE:

1. GHH will post the required notice on the GHH website.
2. The notice will be reviewed annually with GHH employees having access to PHI and all new employees during their orientation to GHH.
3. A copy of any revisions to the notice will be distributed to all employees.
4. GHH’s Privacy Officer will keep a copy of the notice and revisions thereof for such period required by law.
5. Questions regarding the notice should be referred to the GHH Privacy Officer.

Content of Notice

1. The notice contains descriptions of GHH’s role as a health information exchange in facilitating the exchange of information among Participants to improve access, quality and outcomes of care, and the fact that GHH is not a direct provider of care.
2. The notice contains statements that GHH:

   A. Maintains the privacy of PHI and provides individuals with notice of its legal duties and privacy practices with respect to PHI; and

   B. Abides by the terms of the Notice currently in effect.

3. The notice contains a statement that individuals may complain to GHH if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with GHH and a statement that the individual will not be retaliated against for filing a complaint.

4. The notice contains the name and telephone number of GHH’s Privacy Officer.
15. UNSECURED PHI BREACH NOTIFICATION POLICY

**PURPOSE:**
To establish a breach notification process applicable to Unsecured PHI under HIPAA, HITECH and System Security provisions under Texas law.

**APPLICABILITY:**
This policy applies to GHH, its business associates and applicable subcontractors that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use or disclose Unsecured PHI.

**DEFINITIONS:**

1. **Breach:** Under HITECH, the term “Breach” means the acquisition, access, use or disclosure of PHI, in a manner not permitted under the Privacy or Security Rules which compromises the privacy or security of such information, except where the unauthorized acquisition, access, use or disclosure of PHI:
   a. Was unintentional by a workforce member or person acting under the authority of GHH or its business associates, if such acquisition access, or use was made in good faith and within the workforce member’s scope of authority and does not result in further use or disclosure of the PHI in a manner that violated the Privacy or Security Rules
   b. An inadvertent disclose by a person who is authorized to access PHI at GHH or its business associates, and the information received as a result of such disclosure is not further used or disclosed in violation of the Privacy or Security Rule
   c. Where GHH or a business associate 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.

An acquisition, access, use or disclosure of PHI in a manner that violates the Privacy and Security Rules is presumed to be a breach unless GHH or its business associate; as applicable
demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
b. The unauthorized person who used the PHI or to whom the disclosure was made;
c. Whether the PHI was actually acquired or viewed; and
d. The extent to which the risk to the PHI has been mitigated.

2. Breach of System Security: Under Texas law, “Breach of System Security” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Sensitive Personal Information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of Sensitive Personal Information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the Sensitive Personal Information in an unauthorized manner.

3. Data Disposed: includes discarded paper records or recycled electronic media.

4. Data in Motion: includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange.

5. Data at Rest: includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method.

6. Data in Use: includes data in the process of being created, retrieved, updated, or deleted.

7. Law Enforcement Official: means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, empowered by law to: (1) Investigate or conduct an official inquiry into a potential violation of law; (2) Prosecute or otherwise conduct an official inquiry into a potential violation of law; or (3) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

8. Sensitive Personal Information: Under Texas law, “Sensitive Personal Information” means:

a. An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:• Social Security number;
• Driver’s license number or government-issued identification number; or
• Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or

b. Information that identifies an individual and relates to:
• The physical or mental health or condition of the individual;
• The provision of health care to the individual; or
• Payment for the provision of health care to the individual.

c. The term “Sensitive Personal Information” does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

9. **Unsecured Protected Health Information:** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of HHS (“Secretary”). As of the date of this publication, the issued guidance is found under Section 13402(h) of Public Law 111-5.

**POLICY:**

**General Duty**  
GHH is under a duty to notify GHH Participants of a breach of their patients PHI or Sensitive Personal Information under both HIPAA/ HITECH provisions and Texas law.

1. **HIPAA Duty**  
a. In the event GHH discovers a breach of Unsecured PHI, GHH will notify each GHH Participant whose Unsecured PHI has been, or is reasonably believed by GHH to have been, inappropriately accessed, acquired, or disclosed as a result of such breach, as outlined below.

b. The notification requirements of this Policy apply to breaches committed by GHH’s business associates and their Subcontractors. Following discovery of a breach, business associates must: (1) notify GHH of the breach and identify those individuals whose Unsecured PHI has been, or is reasonably believed by business associate to have been breached; and (2) upon receiving the applicable GHH Participants’ prior written approval, notify individuals whose unsecured PHI has been, or is reasonably believed by business associate (upon conferring with the GHH Participants’ Privacy Officer) to have been breached as outlined below. Subcontractors of business associates must notify business associate who has the same duties under this subsection with respect to notification to GHH and the individuals whose PHI was breached.

2. **Texas Duty.** GHH shall disclose any Breach of System Security, after discovering or receiving notification of the breach, to the individual whose Sensitive Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.

**Determination of a Breach**

1. **HIPAA Duty.** Unless one of the exceptions to the definition of “breach” in Step 3 below applies, a breach is the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy or Security Rules which compromises the privacy or security of such information. GHH, its business associates and their subcontractors must conduct a risk assessment and based on that assessment demonstrates that there is a low probability that the PHI has been compromised. (Please refer to the Risk Assessment Tool below).
2. **Texas Duty.** Under Texas law, “Breach of System Security” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Sensitive Personal Information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of Sensitive Personal Information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the Sensitive Personal Information in an unauthorized manner.

3. In the event GHH or one of GHH’s business associates or their subcontractors discover a breach (under HIPAA/HITECH or Texas law, GHH’s Privacy Officer shall: (1) review such breach; (2) perform a risk assessment, and (3) unless otherwise provided in the Business associate Agreement between GHH and its business associate and its business associate and their subcontractors, determine whether the breach requires providing notice, who must be notified and who must provide the notice.

### Performance of Risk Assessment

In order to determine whether a breach of PHI requires notice to the patients of GHH Participants the Privacy Officer shall:

**Step 1:** Determine Whether a Breach of the HIPAA Privacy Rule Occurred. For an acquisition, access, use, or disclosure of PHI to constitute a breach under HIPAA, it must constitute a violation of the HIPAA Privacy or Security Rules.

**Step 2:** Determine Whether the Acquisition, Use of Disclosure Constitutes a “Breach” for Purposes of Texas Law.

1. Under Texas law, notice of a breach is required if all of the following are met:
   a. GHH conducts business in Texas;
   b. GHH owns or licenses computerized data;
   c. There is a Breach of Security System;
   d. The breach consists of Sensitive Personal Information as defined by Texas law;
   e. The individual whose Sensitive Personal Information was or is reasonably believed to have been acquired by an unauthorized person is a resident of Texas or another state that does not require notification of a Breach of System Security. If the individual is a resident of a state that requires notification of a breach of System Security, the notice of the breach of System Security provided under that state’s law is sufficient.

2. To the extent an acquisition, use, or disclosure meets all of the above requirements (subsections 1.1.a – 1.1.e), the Privacy Officer must provide notice to the applicable GHH Participant(s) as set forth by this Policy under the “Individual Notice under Texas Law.” In such case, the Privacy Officer shall mitigate and perform Step 6 Step 7. In addition, the Privacy Officer shall document his/her risk assessment process and conclusions and provide notice to the Participant(s). To the extent the breach also qualifies as a breach under HIPAA, the Privacy Officer will continue with Steps 3 to 7 and conduct notice as also required by this Policy (“Deadline for Notice”; “Methods of Notice”; “Contents of Notice”).
Step 3: Determine whether the Improper Acquisition, Use or Disclosure Constitutes a “Breach” for Purposes of HIPAA. Under HIPAA, the term “breach” does not include:

1. Unintentional acquisitions, access, or uses of PHI by an employee or individual acting under the authority of GHH or a business associate of GHH if:
   a. The acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of a Workforce Member while working under the authority of GHH or a business associate of GHH; and
   b. The information is not further acquired, accessed, used, or disclosed by any person.

2. Inadvertent disclosures from an individual otherwise authorized to access PHI at GHH or at GHH’s business associate if:
   a. The disclosure is to another individual at GHH authorized to access PHI; and
   b. The information is not further acquired, accessed, used or disclosed by any person without patient authorization.

3. A disclosure of PHI where GHH or a GHH business associate (upon conferring with GHH’s Privacy Officer) 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. GHH’s Privacy Officer should complete the analysis on Step 4 below in making this determination.

4. If information is de-identified in accordance with 45 C.F.R. §165.514, it is not PHI and thus any inadvertent or unauthorized disclosure of such information will not be considered a breach.

To the extent an acquisition, use or disclosure falls into one of these four (4) categories, the Privacy Officer need not provide notice to the Participant(s) or continue with subsequent steps. However, the Privacy Officer should document the acquisition, use or disclosure in the individuals Accounting Log in accordance with 45 C.F.R. §165.528.

Step 4: Determine the Likelihood that the PHI is Accessible and Useable by Unauthorized Persons. PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.
   a. Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices.
   b. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800–52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800–77, Guide to IPsec VPNs; or 800–113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140–2 validated.
2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
   a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
   b. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

To the extent PHI is rendered unusable, unreadable, or indecipherable by the above materials, it is not necessary to provide notice, unless the person who acquired, accessed, used or disclosed the PHI has the key to de-encrypt the PHI.

Step 5: Conduct Risk Assessment. An acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy (or specifically excepted from the definition of a breach) is presumed to be a breach unless GHH or its Business Associate (as applicable) demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The Privacy Officer should determine whether a use or disclosure of PHI included any of the following identifiers:
  - Names;
  - Postal address information, other than town or city, state;
  - Telephone numbers;
  - Fax numbers;
  - E-mail addresses;
  - Social security numbers;
  - Medical record numbers;
  - Health plan beneficiary numbers;
  - Account numbers;
  - Certificate/license plate numbers;
  - Vehicle identifiers and serial numbers;
  - Device identifiers and serial numbers;
  - Web URLs;
  - Internet Protocol (IP) address numbers;
  - Biometric identifiers, including finger and voice prints;
  - Full face photographic images and any comparable images;
  - Date of birth; or
  - Zip code.

Due to the lack of identifiers present in the PHI, entities may reasonably determine that is a low risk that the information has been compromised. However, it is important to stress that this is a fact specific determination based on the circumstances of the impermissible use or disclosure.

In reviewing this factor, the Privacy Officer should consider the type of information (i.e., mental health services, substance abuse, or sexually transmitted diseases). However, in performing the risk assessment, the Privacy Officer should keep in mind that many forms of PHI (not just
information about sexually transmitted diseases and similarly sensitive PHI) should be considered sensitive for purposes of the risk assessment. It is also necessary to consider the amount of detailed clinical or financial information involved (e.g. treatment plan, diagnosis, medication, medical history information, test results).

Additionally, in situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, the Privacy Officer should determine whether there is a likelihood that the PHI could be re-identified based on the context and ability to link the information with other available information. For example, if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers-, the PHI is obviously identifiable, and a risk assessment likely would determine that there is more than a low probability that the information has been compromised dependent on an assessment of the other factors discussed below.

The unauthorized person who used the PHI or to whom the disclosure was made: In reviewing this factor, the Privacy Officer should consider the identity of the person who impermissibly used or disclosed the PHI or who impermissibly received the PHI. (If, for example, PHI is impermissibly disclosed to another entity governed by HIPAA, there may be less risk of harm to the individual. In contrast, if PHI is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the PHI, the risk of compromise is much greater.)

Other factors to consider include (but are not limited to):
- The likelihood that unauthorized individuals will know the value of the information and use or sell it;
- Risk of potential harm (blackmail, disclosure of private facts, disclosure of sensitive PHI, mental pain and emotional distress, address information for victims of abuse, humiliation, identity theft);
- Likelihood harm will occur (which depends on manner of actual breach and types of data such as social security number, passwords, mother's maiden name and information useful for identity theft); and
- If identity theft or fraud is a risk, review. www.whitehouse.gov/obm/memoranda/fy2006/task_force_theft_memo.pdf. This factor should be considered in combination with the factor discussed above regarding the risk of re-identification
- Whether the PHI was actually acquired or viewed. The Privacy Officer should investigate an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed. For example, if the PHI were in paper form, in a sealed box, the Privacy Officer should consider whether the box was unsealed. If dealing with EPHI, consult with the Security Officer to determine if the PHI were accessed or downloaded and the time that such occurred. If it is clear that the PHI was not accessed based on the full risk assessment, then GHH may be able to demonstrate a low probability that the PHI has been compromised.
- The extent to which the PHI has been mitigated. Consider the extent to which the risk to PHI has been mitigated. Upon determining that an impermissible use or disclosure
occurred, the Privacy Officer shall take immediate steps to mitigate the impermissible risk or disclosure.

- When possible, the Privacy Officer shall obtain the recipient’s written satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. If such mitigating steps result in a low probability that the PHI has been compromised, then it is not necessary for the Privacy Officer to provide notice to the Participant(s). In such event, the inappropriate disclosure or use should be noted in the individual’s Accounting Log. In the event the Privacy Officer determines that PHI has been compromised, the Privacy Officer shall post notice in the manner set forth below.

- When appropriate, the Privacy Officer should consider purchasing identity theft insurance for individuals. This factor, when considered in combination with the factor regarding the unauthorized recipient of the information discussed above, may lead to different results in terms of the risk to PHI. For example, a covered entity may be able to rely on the assurances of an employee, while such assurances from certain third parties may not be sufficient.

The Privacy Officer’s analysis of the probability that PHI has been compromised following the impermissible use or disclosure must address each factor discussed above. Other factors may also be considered when necessary. GHH must then evaluate the overall probability that the PHI has been compromised by considering ALL the factors in combination. If an evaluation of the factors discussed above fails to demonstrate that there is a low possibility that the PHI has been compromised, breach notification is required.

Step 6: Review the Physical, Technical, and Procedural Safeguards Employed by GHH or GHH’s Business associate (as applicable). The Privacy Officer should review appropriate counter-measures, such as monitoring systems for misuse of the PHI and patterns of suspicious behavior that can be taken by GHH. The business associate should be contractually required to do the same for its Subcontractors.

Step 7: Documentation. The Privacy Officer shall document his/her Risk Assessment process and conclusions. To the extent that the Privacy Officer determines that it is not necessary to provide notice to the GHH Participant(s), the Privacy Officer’s Risk Assessment must demonstrate the factors considered in determining that breach notification was not required.

**DEADLINE FOR NOTICE:**

1. GHH shall provide notice to the applicable GHH Participants in accordance with the term so the Participation Agreement, except where law enforcement officials determine that a notification would impede a criminal investigation or cause damage to national security.

2. If a law enforcement official states to GHH or a business associate of GHH that a notice, or posting of notice impedes a criminal investigation or cause damage to national security, such law enforcement official shall be directed to GHH’s Privacy Officer. Privacy Officer shall verify the identity and authority of the law enforcement official in accordance with GHH’s Verification Policy and Procedure. In the event the law enforcement official’s identity and authority is verified, the Privacy Officer shall:

---

3 Texas Business and Commerce Code §521.052(c), as amended by H.B. 300.
a. Delay such notification, notice, or posting for the time period specified by the official if the statement is in writing and specifies the time for which delay is required; or
b. If the statement is made orally, the Privacy Officer shall document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement from the law enforcement official is obtained.

3. A breach shall be treated as discovered by GHH or a business associate as of the first day on which such breach is known to GHH or, by exercising reasonable diligence would have been known to GHH or the business associate (respectively).

4. GHH and GHH’s business associate shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a Workforce Member or agent of GHH or business associate (respectively).

5. The Privacy Officer shall be responsible for investigating and sending notices without unreasonable delay.

NOTICE:
GHH shall provide notice as required by the Participation Agreement with the applicable Participant(s).

CONTENTS OF NOTICE UNDER HITECH AND TEXAS LAW:
The notice shall include, to the extent possible:
1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, or disability code);
3. The steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what GHH or GHH’s business associate is doing to investigate the breach, mitigate losses, and to protect against any further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, website, or postal address.

DOCUMENTATION:
The Privacy Officer shall maintain an internal log of breaches and document the process and results of any Risk Assessment. The Privacy Officer shall retain such documentation and forms for at least seven (7) years.
16. BREACH NOTIFICATION RISK ASSESSMENT FORM

This worksheet must be completed for each possible breach of PHI.

1. What happened?

2. What type of PHI was involved? (STEP 3 OF BREACH NOTIFICATION POLICY.)

3. Was the PHI secured? (STEP 4 OF BREACH NOTIFICATION POLICY.)

4. Was there a breach? Answer questions a, b, and c, then conclude if there was a breach.
   a. Was it permissible under HIPAA? (STEP 1 OF BREACH NOTIFICATION POLICY.)
      Yes       No
      If it was permissible under HIPAA, explain:

   b. Is there a significant risk of harm? (STEP 5 OF BREACH NOTIFICATION POLICY.)
      Yes       No
      Explain:
c. Did if fall within an exception? *(STEP 2 OF BREACH NOTIFICATION POLICY.)*

√ Was it unintentional, by a Workforce member or a Business Associate acting in good faith and within the scope of his or her authority, and will not result in further impermissible use or disclosure?

Yes  No

If yes, explain:

√ Was it inadvertent, by a person authorized to access the PHI to another person who is authorized to access PHI our facility, and the PHI is not further impermissibly used or disclosed?

Yes  No

If yes, explain:

√ Do we believe in good faith that the unauthorized person to whom the PHI was disclosed would not reasonably have been able to *retain* the information.

Yes  No

If yes, explain:

CONCLUSION: Was there a breach?  Yes  No

5. What actions are being taken to investigate, mitigate harm, and protect against future breaches? *(STEPS 6-7 OF BREACH NOTIFICATION POLICY.)*
6. Were 500 or more individuals involved? Were 500 or more in one state or jurisdiction?
   
   Yes          No

   Explain:
16. 17. INDIVIDUAL BREACH NOTIFICATION LETTER FORM

INDIVIDUAL NOTICE
(Print on letterhead)

TO: ________________________________ Date: _________________
Address: __________________________
___________________________________

RE: Individual Breach Notice

Description of Occurrence: __________________________________________
____________________________________________________________________
____________________________________________________________________

Type of Unsecured PHI (Private Health Information) Involved: _____________
____________________________________________________________________
____________________________________________________________________

Suggested Steps for Personal Protection: _________________________________
____________________________________________________________________
____________________________________________________________________

Actions Taken & Undergoing to Investigate, Mitigate and protect Against Further Breaches:
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________

Contact Procedure for More Information:
Toll-Free Number: ________________________________
E-mail Address: _________________________________
Web-Site: ______________________________________
Postal Address: __________________________________
____________________________________________________________________
____________________________________________________________________

We recommend that you immediately take the following steps:

1. Call one of the three major credit bureaus listed below to place a ‘Fraud Alert’ on your credit report. This can help prevent anyone from opening additional accounts in your name. Once the credit bureau confirms your Fraud Alert, the other two credit bureaus will automatically place alerts on your credit report.

   A. Equifax: 1-800-525-2685; www.equifax.com
B. Experian: 1-888-EXPERIAN (397-3742); www.experian.com

C. TransUnion: 1-800-680-7289; www.transunion.com

2. Order your credit reports from all three bureaus. When you set up a Fraud Alert, you can also receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts or activities that are not yours.

3. Monitor your credit reports carefully. Even with Fraud Alerts on your credit bureau accounts, we recommend that you continue to monitor your credit reports to be sure that nobody has opened an account using your personal information.

Respectfully,

Privacy Officer

(This information will be retained for seven (7) years.)
17. 18. DESTRUCTION/DISPOSAL OF INDIVIDUAL PHI BY GHH

<table>
<thead>
<tr>
<th>POLICY AND PROCEDURES</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPARTMENT:</td>
<td></td>
</tr>
<tr>
<td>POSITION:</td>
<td></td>
</tr>
<tr>
<td>SUBJECT:</td>
<td></td>
</tr>
<tr>
<td>Date issued: December 14, 2011</td>
<td>Policy No:</td>
</tr>
</tbody>
</table>

PURPOSE:
To establish guidelines for the appropriate destruction of media which may contain PHI.

POLICY:
It is the policy of GHH to protect the privacy and security of all media containing PHI in the maintenance, retention, and eventual destruction/disposal of such media. Destruction/disposal of PHI will be carried out only after the information has reached its defined retention period in accordance with federal and state law and as defined in GHH’s retention policy (as applicable).

PROCEDURES:

1. All destruction/disposal of media containing PHI will be done in accordance with federal and state law and pursuant to GHH’s written retention policy/schedule (as applicable).

2. Media containing PHI involved in any current or anticipated investigation, audit, or litigation should not be destroyed. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for such records. When applicable, a qualified protective order will be obtained to limit the use or disclosure of PHI.

3. Media scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of individual information is complete.

4. A record of all PHI media destruction/disposal should be made and retained permanently by GHH to demonstrate that the PHI were destroyed/disposed of in the regular course of business. Records of destruction/disposal should include:
   A. Date of destruction/disposal;
   B. Method of destruction/disposal;
   C. Destruction of the destroyed/disposal record series or medium;
D. Inclusive dates covered;

E. A statement that the PHI was destroyed/disposed of in the normal course of business; and

F. The signatures of the individuals supervising and witnessing the destruction/disposal.

5. Media containing PHI should be cleared, purged, or destroyed by the following methods:

   A. Paper, film, or other hard copy media shall be shredded or destroyed such that the PHI cannot be read or otherwise be reconstructed. Redaction is specifically excluded as a means of data destruction.

   B. Electronic media shall be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media sanitization: http://csrc.nist.gov/, such that PHI cannot be retrieved.

6. The Privacy Officer must categorize the information to be disposed of, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, using information in Table A-1 below, decide on the appropriate method for sanitization (cleared, purged, or destroyed). The selected method should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risks to an unauthorized disclosure of information.
**Table A-1**  
Sanitization Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear</strong></td>
<td>One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].</td>
</tr>
</tbody>
</table>
| **Purge** | Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging.  
Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degauser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] |
| **Destroy** | There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.  
- **Disintegration, Pulverization, Melting, and Incineration.** These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.  
- **Shredding.** Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.  
Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). |

*NIST Special Publication 800-88, Guidelines for Media Sanitization (September, 2006).*
Table A-2 outlines specific sanitization methods for specific types of media. Not all types of available media are specified in Table A-2. If a specific is not included, GHH must identify and use processes that fulfill the intent to clear, purge, or destroy.

1. If GHH contracts with a vendor to provide destruction/disposal services, the Business Associate Agreement must provide that the vendor will establish the permitted and required uses and disclosures of information under federal and state law as outlined in the Business Associate Agreement, which must include the following elements:

   A. Specify the method of destruction/disposal;
   
   B. Specify the time that will elapse between acquisition and destruction of data/media;
   
   C. Establish safeguards against breaches in confidentiality;
   
   D. Indemnify GHH from loss due to unauthorized disclosure, and, if appropriate, require that the contractor (Business Associate) maintain liability insurance in specified amounts at all times the Business Associate Agreement is in effect;
   
   E. Comply with the destruction requirements as set forth by HITECH; and
   
   F. Provide proof of destruction/disposal.

2. The methods of destruction/disposal should be reassessed annually, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services or as additional guidance are made available by the Secretary.
# Table A-2
## Media Sanitization Decision Matrix

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hard Copy Storage</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper and microforms</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>- Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL.).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.</td>
</tr>
<tr>
<td><strong>Hand-Held Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Phones</td>
<td>Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer’s reset to reset the cell phone back to its factory default settings. <strong>Please contact the manufacturer for proper sanitization procedure.</strong></td>
<td>Same as Clear.</td>
<td>- Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Incinerate by burning cell phones in a licensed incinerator.</td>
</tr>
<tr>
<td>Personal Digital Assistant (PDA) (Palm, PocketPC, other)</td>
<td>Manually delete all information, then perform a manufacturer’s hard reset to reset the PDA to factory state.</td>
<td>Same as Clear.</td>
<td>- Incinerate PDAs by burning the PDAs in a</td>
</tr>
</tbody>
</table>
### Media Type

**Clear**

- **Please contact the manufacturer for proper sanitization procedure.**

**Purge**

- Physical Destruction
- licensed incinerator.
  - Shred.
  - Pulverize.

### Networking Devices

**Routers (home, home office, enterprise)**

- Perform a full manufacturer’s reset to reset the router back to its factory default settings.
- **Please contact the manufacturer for proper sanitization procedure.**

**SAME AS CLEAR.**

- Shred.
- Disintegrate.
- Pulverize.
- Incinerate. Incinerate routers by burning the routers in a licensed incinerator.

### Equipment

**Copy Machines**

- Perform a full manufacturer’s reset to reset the copy machine to its factory default settings.
- **Please contact the manufacturer for proper sanitization procedure.**

**SAME AS CLEAR.**

- Shred.
- Disintegrate.
- Pulverize.
- Incinerate. Incinerate copy machines by burning the copy machines in a licensed incinerator.

**Fax Machines**

- Perform a full manufacturer’s reset to reset the fax machine to its factory default settings.
- **Please contact the manufacturer for proper sanitization procedures.**

**SAME AS CLEAR.**

- Shred.
- Disintegrate.
- Pulverize.
- Incinerate. Incinerate fax machines by burning the fax machines in a licensed incinerator.
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Magnetic Disks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floppies</td>
<td>Overwrite media by using agency-approved software and validate the overwritten data.</td>
<td>Degauss in a NSA/CSS-approved degausser.</td>
<td>• Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator.</td>
</tr>
<tr>
<td>ATA Hard Drives</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>1. Purge using Secure Erase. The Secure Erase software can be downloaded from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** 3. Purge media by using agency-approved and validated purge technologies/tools. **Degaussing any current generation hard disk will render the drive permanently unusable.</td>
<td>• Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.</td>
</tr>
<tr>
<td>USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>1. Purge using Secure Erase. The Secure Erase software can be downloaded from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** 3. Purge media by using</td>
<td>• Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Physical Destruction</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Zip Disks</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>Degauss using a NSA/CSS-approved degausser.</td>
<td>• Incinerate disks and diskettes by burning the zip disks in a licensed incinerator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>**Degaussing any current generation zip disks will render the disk permanently unusable.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Degauss using an NSA/CSS-approved degausser.</td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape.</td>
<td>• Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a destruction facility or for recycling measures.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Physical Destruction</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>-------</td>
<td>----------------------</td>
</tr>
<tr>
<td>magnetic tape should be overwritten one time with known non-sensitive signals.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Optical Disks**

**CDs**

- See Physical Destruction.
- See Physical Destruction.

* Destroy in order of recommendations:
  * Removing the Information bearing layers of CD media using a commercial optical disk grinding device.
  * Incinerate optical disk media (reduce to ash) using a licensed facility.
  * Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). **

  ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25 mm².

**DVDs**

- See Physical Destruction.
- See Physical Destruction.

* Destroy in order of recommendations:
  * Removing the Information bearing layers of DVD media using a commercial optical disk grinding device.
  * Incinerate optical disk media (reduce to ash) using a licensed facility.

**DVDs**
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>See Physical Destruction.</td>
<td><strong>Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²).</strong> <strong>This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Pulverize.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td>Compact Flash Drives, SD</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td></td>
<td>Destroy media in order of recommendations.</td>
</tr>
<tr>
<td>Dynamic Random Access Memory (DRAM)</td>
<td>Purge DRAM by powering off and removing the battery (if battery backed).</td>
<td>Same as Clear.</td>
<td>- Shred.</td>
</tr>
<tr>
<td>Electronically Alterable PROM (EAPROM)</td>
<td>Perform a full chip purge as per manufacturer’s data sheets.</td>
<td>Same as Clear.</td>
<td>- Disintegrate.</td>
</tr>
<tr>
<td>Electronically Erasable PROM (EEPROM)</td>
<td>Overwrite media by using agency approved and validated overwriting</td>
<td>Same as Clear.</td>
<td>- Pulverize.</td>
</tr>
</tbody>
</table>

**Memory**
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear technologies/methods/tools. Remove all labels or markings that indicate previous use or confidentiality.</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erasable Programmable ROM (EPROM)</td>
<td>Clear media in order of recommendations.</td>
<td>Same as Clear.</td>
<td>• Pulverize.</td>
</tr>
<tr>
<td></td>
<td>1. Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations, but increase the time requirement by a factor of 3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td></td>
<td>• Incinerate by burning in a licensed incinerator.</td>
</tr>
<tr>
<td>Field Programmable Gate Array (Non-Volatile)</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td>Field Programmable Gate Array (FPGA) Devices (Volatile)</td>
<td>Clear functioning FPGA by powering off and removing the battery (if battery backed).</td>
<td>Same as Clear.</td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td>Flash Cards</td>
<td>Overwrite media by using agency approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>• Pulverize.</td>
</tr>
</tbody>
</table>
| Flash EPROM (FEPROM)                  | Perform a full chip purge as per manufacturer's data sheets.                                    | Purge media in order of recommendations.  
1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools.  
2. Perform a full chip purge | • Shred.                                           |
<p>|                                       |                                                                                                 |       | • Disintegrate.       |
|                                       |                                                                                                 |       | • Pulverize.          |</p>
<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
</table>
| Magnetic Bubble Memory | Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. | Purge by Collapsing the Magnetic Bubbles:  
1. Degaussing: Degauss in an NSA/CSS-approved degausser. However, care must be taken to ensure that the full field (at least 1500 gauss) of the degausser is applied to the actual bubble array. All shielding materials must be removed from the circuit card and/or bubble memory device before degaussing.  
2. Raising the Magnetic Bias Field: Magnetic bubble memory with built-in magnetic bias field controls may be purged by raising the bias voltage to levels sufficient to collapse the magnetic bubbles. Recommend that specific technical guidance be obtained from the bubble memory manufacturer before attempting this procedure. | • Incinerate by burning in a licensed incinerator.  
• Shred.  
• Disintegrate.  
• Pulverize. |
| Magnetic Core Memory | Clear media in order of recommendations.  
1. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.  
2. Degauss in an NSA/CSS-approved degausser. | Purge core memory devices either by overwriting or degaussing.  
Overwrite media by using agency approved and validated overwriting technologies/methods/tools  
Degauss in an NSA/CSS-approved degausser. Remove all labels or markings that indicate previous use or confidentiality. NOTE - Attenuation of the magnetic field due to chassis shielding and separation distance are factors that affect erasure. | • Shred.  
• Disintegrate.  
• Pulverize. |

When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.
### Media Types and Purge/Physical Destruction Methods

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Physical Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non Volatile RAM (NOVRAM)</strong></td>
<td>Purge performance and should be considered. All steel shielding materials (e.g., chassis, case, or mounting brackets) should be removed before degaussing.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td><strong>Non Volatile RAM (NOVRAM)</strong></td>
<td>1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools. 2. Each overwrite must reside in memory for a period longer than the data resided. Remove all power to include battery power.</td>
<td>Same as Clear.</td>
<td>Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.</td>
</tr>
<tr>
<td><strong>Programmable ROM (PROM)</strong></td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>Destroy by incinerating in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>Purge functioning DRAM by powering off and removing the battery (if battery backed).</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td><strong>ROM</strong></td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td><strong>USB Removable Media (Pen Drives, Thumb Drives, Flash Drives)</strong></td>
<td>Overwrite media by using agency approved and validated overwriting technologies/methods/tools.</td>
<td>Same as Clear.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Disintegrate.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Physical Destruction</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Drives, Memory Sticks) without Hard Drives</td>
<td></td>
<td></td>
<td>• Pulverize.</td>
</tr>
<tr>
<td>Smart Cards</td>
<td>See Physical Destruction.</td>
<td>See Physical Destruction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For smart card devices &amp; data storage tokens that are in credit card form, cut or crush the smart card’s internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e., SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded should instead be destroyed via incineration licensed incinerator or disintegration to 2 mm size particles.</td>
</tr>
<tr>
<td>Magnetic Cards</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Magnetic Cards</td>
<td>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</td>
<td>Degauss in an NSA/CSS-approved degausser.</td>
<td>• Shred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Incinerate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Incineration of magnetic cards shall be accomplished by burning the magnetic cards in a licensed incinerator.</td>
</tr>
</tbody>
</table>

NIST Special Publication 800-88, Guidelines for Media Sanitization (September, 2006).
19. CERTIFICATE/RECORD OF DESTRUCTION

This information described below was destroyed in the normal course of business pursuant to the organizational retention schedule and destruction policies and procedures.

Date of Destruction:  
Authorized by:

Description of Information Sanitized:

Inclusive Dates Covered:

METHOD OF SANITIZATION:

Item Disposition:  
Date Conducted:____________________________

Conducted By:____________________________

☐ Clear  
Phone #:____________________________

☐ Purge  
Validated By:____________________________

☐ Destroy  
Phone #:Phone ________________________

Sanitization Method Used:____________________________

Final Disposition of Media:

☐ Disposed

☐ Reused Internally

☐ ReusedExternally

☐ Return to Manufacturer

☐ Other:____________________________
*If records are destroyed by outside firm, must confirm a contract exists and certificate of destruction has been received:

☐ Yes

☐ No
20. TELEPHONE POLICY FOR GHH

PURPOSE:

To establish proper procedures to prevent Workforce members from improper use or disclosure of PHI by telephone.

POLICY:

1. Medical information regarding an individual should generally not be released by phone. If an individual is requesting disclosure, Workforce members may disclose information only if that Workforce member:
   
   A. Knows the individual and can verify the individual’s identity by their voice; or
   
   B. Individual provides their personal identifier number; or
   
   C. Workforce member calls the individual at the phone number(s) provided in the individual’s record.

2. Workforce members shall not disclose PHI to third parties, without individual authorization, except as authorized by law.
   
   A. All disclosures to third parties must be documented in the individual’s record.
   
   B. Disclosures made for purposes other than treatment, payment, or health care operations shall be documented in a “Disclosure Record.”
APPROVAL:

__________________________________________  ______________________
Privacy Officer                              Date
Signature

__________________________________________  ______________________
[Office (capacity)]                          Date
Signature
18. POLICY FOR DISCIPLINARY ACTION FOR GHH WORKFORCE

POLICY AND PROCEDURES

DEPARTMENT:                         POSITION:         45 CFR 164.530
SUBJECT:  Privacy Requirement Sanctions

GHH

Date issued: December 14, 2011
Policy No:

It is the responsibility of each Workforce member to comply with these policies, procedures, and applicable Texas and Federal confidentiality laws and regulations. Any concerns or questions regarding this policy should be directed to the Privacy Officer.

A. Workforce Member’s Duty to Report Violations of Policies.
   1. Any Workforce member who observes or is aware of a PHI policy violation must report the violation to the Privacy Officer.
   2. Any Workforce member who believes in good faith that a violation of PHI policy has occurred may report such violation to GHH without violating this policy. GHH will not intimidate, threaten, coerce, discriminate against, or take retaliatory action against any individual who reasonably exercises his/her rights under this policy.
   3. Failure to report a violation of GHH’s PHI policies is a violation of this policy and may lead to disciplinary action, up to and including termination.

B. Disciplinary Action.
   1. Failure to comply with PHI policies may be grounds for disciplinary action, including termination of employment. The appropriate level of disciplinary action will be determined on a case by case basis, taking into consideration the specific circumstances and severity of the violation. In cases where disciplinary action is imposed (except termination), the Workforce member shall be required to repeat confidentiality training.
   2. The following is a partial list of Workforce member conduct that will constitute a violation of the PHI policies and thus lead to disciplinary action, up to and including termination. There may be other conduct that is not listed which would also constitute policy violations.
3. **Workforce Member:**
   
   A. Demonstrates a pattern or practice of discussing individual information in a public area;
   
   B. Demonstrates a pattern or practice of leaving a record in a public area;
   
   C. Demonstrates a pattern or practice of leaving a computer containing PHI unsecured;
   
   D. Looks up an individual’s address or relative’s address for personal rather than legitimate and authorized business and claim purposes;
   
   E. Compiles a mailing list with the intent to sell or use for personal purposes; and
   
   F. Reviews or discloses PHI in order to advance a personal cause of action.

C. **Explanation of Disciplinary Actions.** GHH generally will follow a progressive discipline policy as set forth below in imposing discipline for violations of this policy. However, GHH reserves the right, in appropriate circumstances, to immediately terminate or otherwise discipline an employee without notice and/or without following the progressive discipline steps.

1. **Oral Counseling:**
   
   a. Though the counseling is oral, the counseling should be documented.
   
   b. The record should indicate that it is a verbal counseling.
   
   c. The Workforce member should sign the form.
   
   d. A refusal to sign should be indicated on the form.

2. **Written Counseling:**
   
   a. This counseling is to be documented.
   
   b. The Workforce member should sign the form.
   
   c. A refusal to sign should be indicated on the form.

3. **Termination:** The reasons for discharge should be documented and discussed with the Workforce member.

D. **Mitigation.** In an effort to protect all PHI, GHH will mitigate, to the extent practicable, any harmful effect that results from a **known** use or disclosure of PHI in violation of the PHI policies.
E. **No Retaliation.** Individuals shall be protected from retaliation if they act in good faith in the belief that the opposed behavior is unlawful, the manner of the opposition is reasonable and does not involve the disclosure of PHI in violation of the rule. Further, GHH shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for filing a complaint; testifying, assisting, or participating in an investigation or compliance review; or opposing any act or practice made unlawful by GHH’s privacy policies or by Texas and Federal laws.
19. SANCTIONS RECORD

| IDENTIFICATION                  | Last Name: __________________________ |
|                                 | First Name: __________________________ |
|                                 | Social Security Number: ____________  |
|                                 | Title: ______________________________ |

| INDIVIDUAL MAKING ENTRY         | Last Name: __________________________ |
|                                 | First Name: __________________________ |
|                                 | Title: ______________________________ |

| INDIVIDUAL TO WHOM THE REPORT WAS MADE | Last Name: __________________________ |
|                                        | First Name: __________________________ |
|                                        | Title: ______________________________ |

| DATE OF SANCTION                | |

| DESCRIPTION OF POLICY VIOLATED | |

| DATE REPORTED                  | |

| DESCRIPTION OF SANCTION        | |

| REFERENCES TO ANY CORRESPONDENCE | |

| COMMENTS                        | |

RECORD MUST REMAIN CONFIDENTIAL AND SHOULD BE FILED SEPARATELY IN THE WORKFORCE MEMBER PERSONNEL FILE.
## 20. COMPLAINT POLICY

<table>
<thead>
<tr>
<th>POLICY AND PROCEDURES</th>
<th>GHH</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPARTMENT:</td>
<td>POSITION:</td>
</tr>
<tr>
<td>SUBJECT: HIPAA Privacy</td>
<td>45 CFR 164.530</td>
</tr>
<tr>
<td>Page:</td>
<td></td>
</tr>
</tbody>
</table>

**PURPOSE:**

To implement a procedure for receiving, documenting, and taking appropriate action with respect to privacy complaints.

**POLICY:**

1. All Privacy Complaints must be submitted to the GHH Privacy Officer or his/her designees.

2. Privacy Complaints must include a statement that describes the basis of the complaint.

3. The GHH Privacy Officer will determine what health care information the individual claims was misused or improperly disclosed. If the health care information at issue was created or maintained by a Participant or a Business Associate, the complaint will be forwarded to the Participant or Business Associate.

**Responsibilities Of The GHH Privacy Officer**

1. The Privacy Officer shall determine:
   A. Whether there has been a violation of the privacy regulations or GHH’s privacy policies.
   B. What, if any, internal privacy practices need to be changed.
   C. What, if any, additional policies need to be developed.
   D. What additional training will be provided to the person who violated the privacy regulations or policies.

2. The Privacy Officer will determine whether a violation has occurred and will determine appropriate sanctions.
3. The Privacy Officer shall document all complaints received by GHH and the action taken in response to the complaint in a separately and confidentially maintained individual complaint file. Documentation of each complaint will be retained in written or electronic form.
21. POLICY FOR CHANGES TO POLICIES AND PROCEDURES

PURPOSE:

To implement a procedure for changing policies and procedures and corresponding forms, records, and agreements.

POLICY:

1. The GHH Privacy Officer is responsible for developing and maintaining all appropriate policies and procedures, prior to implementation.

2. Policies and procedures may be maintained in written or electronic form.

3. Except for changes required by law or advised by outside legal counsel, any changes to the policies and procedures must be approved by the:

   A. Privacy Officer; and

   B. The Greater Houston Healthconnect Board of Directors.

PROCEDURE

1. GHH reserves the right to make amendments to these Policies and Procedures and to the Participation Agreement. Notice of amendments may be provided by posting the amendment, along with its effective date, on the GHH website (www.ghhconnect.org).

2. If there are material changes in policies and procedures, the affected Workforce must be trained on the amended policies and procedures prior to implementation.

3. Privacy Officer must retain documentation for seven (7) years from when the documentation is created, unless a longer period applies.
### PURPOSE:

To secure written Participation Agreements with each Participant of GHH binding Participants to comply with applicable laws, requirements of THSA, and GHH policies and procedures on use of the Exchange as outlined in this Policy.

### POLICY:

When using the Exchange, each Participant will:

1. Execute a Participation Agreement.

2. Comply with applicable federal and state laws and regulations, including, but not limited to those protecting the confidentiality and security of PHI and establishing individual privacy rights and use reasonable efforts to stay abreast of any changes or updates and interpretations of laws and regulations.

3. Be aware of the provisions of certain state laws, which are [or may be] more stringent than, and not preempted by, the HIPAA Privacy and Security Regulations.

4. Have the requisite, appropriate, and necessary internal policies for compliance with applicable state and federal privacy and security laws and GHH’s Participant Agreement, including, without limitation, a sanctions policy. Participant will enforce its policies and procedures by appropriately sanctioning any employee, volunteer, contractor, subcontractor or other person who accesses the Exchange on behalf of the Participant.

5. Have policies and procedures to promote the accuracy and relevance of the PHI it makes available through the Exchange.

6. Acknowledge and agree that the PHI transmitted to the Exchange, including but not limited to the Provider Directory, Master Patient Index, and Record Locator Service does not constitute a Designated Record Set as defined by HIPAA.

7. Will not exclusively rely on documents transmitted through the Exchange to make treatment decisions.
8. Ensure that patient authorization has been obtained prior to transmitting any PHI through the Exchange.

9. Update its Notice of Privacy Practices (“NPP”) to describe its participation in the Exchange when an individual has authorized his/her PHI to be used or disclosed through the Exchange.

10. Designate individuals who may access the Exchange on behalf of Participant. Only Workforce members who have a legitimate and appropriate need to use the Exchange shall be granted access. No Workforce member will be provided with access to the Exchange without training. Participant will require that Workforce members:

   A. Receive training regarding the confidentiality and security of PHI and the requirements set forth by HIPAA, HITECH, and state confidentiality laws;

   B. Only access the Exchange for purposes of (1) treatment, (2) payment, and/or (3) necessary health care operations as allowed by law. Except for treatment, each Participant will access or enter into the Exchange only the minimum amount of PHI necessary for the purpose of the access or entry;

   C. Hold any passwords, or other means for accessing the Exchange, in a confidential and secure manner and release them to no other individual; and

   D. Comply with applicable GHH Policies and those of the Participant. Workforce members must understand that failure to comply with such policies and procedures may constitute cause for disciplinary action, up to and including termination and the imposition of civil and criminal penalties against Participant.

11. Each Participant will provide GHH with the name, telephone number, facsimile, and e-mail of its current Privacy Officer.
23. POLICY FOR BUSINESS ASSOCIATES OF GHH

POLICY AND PROCEDURES

DEPARTMENT: | POSITION: | SUBJECT: Disclosure to Business Associates and Contractors

GHH

Date issued: December 14, 2011

45 CFR 164.502(e)(1)(ii), as amended by NPRM, July 14, 2010
45 CFR 164.504(e)(1)(iii); (e)(5), as amended by NPRM, July 14, 2010
45 CFR 164.308(b)(2), as amended by NPRM, July 14, 2010
45 CFR 164.314(a)(2)(iii), as amended by NPRM, July 14, 2010
45 CFR 160.103, definition of business associate, as amended by NPRM, July 14, 2010

PURPOSE:

To comply with the business associate contract rules under HIPAA.

DEFINITION:

A “Business Associate” is a person who performs a function on behalf of GHH involving individual health information for GHH, other than as a Participant of the Workforce.

POLICY:

1. GHH must obtain satisfactory assurances that a business associate will appropriately safeguard PHI.

2. The business associate contract must establish the permitted and required uses and disclosures of business associates. A business associate can only use or disclose a covered entity’s PHI as the covered entity can under HIPAA. Therefore, GHH may not authorize business associates to use or further disclose PHI in any manner that would violate HIPAA if the use or disclosure were made by GHH and/or the applicable Participant.

3. A business associate may use and disclose PHI for the proper management and administration of the business associate and to provide data aggregation services relating to the health care operations of GHH.
4. All business associates must contractually agree:
   
   A. Not to use or further disclose the information other than as permitted or required by the contract or as required by law;
   
   B. Use appropriate safeguards to prevent use or disclosure of the information other than as provided by the contract;
   
   C. Report to GHH upon discovery any use or disclosure of the information not provided for by its contract of which it becomes aware;
   
   D. That agents and subcontractors agree to the same restrictions and conditions that apply to the business associate with respect to PHI the agent or subcontractor receives or creates on the behalf of the business associate;
   
   E. Make available PHI in accordance with the requirements imposed on GHH;
   
   F. Make available PHI for amendment and incorporate any amendments to PHI in accordance with the same requirements imposed on GHH;
   
   G. Make available the information required to provide an accounting of disclosures in accordance with the same requirements imposed on GHH;
   
   H. Provide the Secretary of HHS and GHH with access to all internal practices and records relating to PHI in order to determine whether GHH is in compliance; and
   
   I. To allow GHH, if it is determined that the business associate has violated a material term of the contract, to terminate the relationship.

5. At termination, the business associate must:
   
   A. Return or destroy all PHI;
   
   B. Not retain copies of the information; and
   
   C. If the business associate cannot return or destroy the PHI, extend the protections of the contract to the information and limit further disclosures.

6. Satisfactory assurances required of a business associate must be documented through a written contract or other written agreement with the business associate that meets the applicable requirements. The party who enters into the agreement on behalf of GHH is responsible for determining that the agreement contains the necessary business associate provisions.
7. All business associates must cooperate with GHH in performing a risk assessment of any break of unsecured protected health information in accordance with the provisions of the Business Associate Agreement. GHH must take reasonable steps to cure business associate breaches or violations. Failure to cure violations may lead to privacy violations. Sanctions may be imposed against GHH as a result of a failure to cure any action in which there was knowledge of a pattern of activity or practice conducted by the business associate that constituted a material breach or violation of the business associate’s obligations under the contract or other arrangement.

8. If steps to cure a business associate’s violation of the privacy rules are unsuccessful, GHH must:

   A. Terminate the contract or arrangement, if feasible; or

   B. If termination is not feasible, report the problem to the Secretary of HHS.

PROCEDURE:

1. GHH will identify all categories of parties/entities with whom PHI is shared in accordance with the definition of a business associate in 45 CFR 160.102, Definitions. Determination of the status of Business Associate shall be made dependent on the services provided, whether the entity could be considered part of the workforce, or whether the entity provides services to GHH as a third party service. In general, business associates are entities with which GHH subcontracts that perform a service where the provision of the service involves the disclosure of PHI. Participants of the GHH workforce are not considered business associates.

2. Further, the Participants of GHH are not considered business associates of GHH, rather they are covered entities under HIPAA for which GHH is a business associate. This policy and procedures relates to subcontractors of GHH that perform functions for GHH and are thus considered business associates of GHH.

3. A formal Business Associate Agreement, containing all elements listed in this policy, shall be entered into with each entity considered to be a “Business Associate” as defined by HIPAA Regulations 45 CFR 164. A Business Associate Agreement, or a contract providing for compliance with the Privacy Standards and Security Standards, must be entered into prior to the commencement of services.

4. The Privacy Officer shall maintain copies of all Business Associate Agreements.

5. The Privacy Officer shall investigate compliance with the agreement if a complaint is made that the business associate has violated the terms of the agreement.
APPROVAL:

_________________________________________  ___________
Privacy Officer                           Date
Signature

_________________________________________  ___________
[Office (capacity)]                        Date
Signature