Policy/Procedure: SDM Honest Broker Certification Policy and Procedures

Policy and Procedure:

SDM Honest Broker Certification Policy and Procedures

Purpose: This policy describes the policy and procedures of application for the SDM Certification of Honest.

Audience: Honest brokers

Department: Office of Faculty Development and Information Management

Written by: Fen Zheng

Effective: 09/21/2009

Approved by: Dr. Thomas Braun

Created: 08/13/2009

Last updated: 11/12/2014

Keywords: Policies, procedures, PHI, HIPAA, honest broker, certification, application

Related docs: Honest Broker BAA

PHI Data Extraction, Export, Print and Report Policy

Comments: Please send comments and corrections to: cdi_offmgr@dental.pitt.edu

Application for SDM Certification of Honest Broker System/Processes

1. Specify the School, Department, Division, or Center for which this Honest Broker System/Process is being developed:

   University of Pittsburgh, School of Dental Medicine

2. Specify the individual who will assume responsibility for the appropriate management and oversight of this Honest Broker System/Process:

   Name: Patrick L. Hetherington

   Title: Manager, Electronic Health Records

   Address: SALK 328

   3501 Terrace Street

   Pittsburgh, PA 15261

   Telephone Number: 412-648-3495

   FAX Number: 412-648-9960

   E-mail Address: plh@pitt.edu

11/21/2014
3. Specify the names of all additional individuals who will be involved in performing honest broker services under this Honest Broker System/Process:

4. HIPAA Complete (i.e., "Safe Harbor") De-Identification of Medical/Dental Record Information:

   a. For electronic medical/dental record information, address the processes and/or systems that will be used to fully de-identify (i.e., HIPAA "Safe Harbor" compliant) the information for subsequent use by your affiliated researchers. (Note: See Attachment A for HIPAA "Safe Harbor" de-identification requirements.)

   Protected Health Information (PHI) is defined as personal and identifiable health information about patients under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Frequently, PHI is required for research and/or teaching purposes within the School of Dental Medicine. PHI can be made available for research and teaching purposes within the School of Dental Medicine as long as the following occur:

   **Written HIPAA Authorization under an IRB Approved Protocol**

   Where the IRB has approved a research protocol where research subjects provided prospective, written informed consent combined with the necessary elements of a HIPAA authorization, PHI within the scope of that consent/authorization may be extracted from the EHR. In each case, the investigator must provide a copy of the IRB approval letter, and the signed consent/authorization for each subject to SDM IT with the service request. The copies are attached to the request ticket in the IT ticketing system FootPrints.

   **Provision of a De-Identified Data Set**

   In order to make the data available for research under this provision, they must be de-identified. The following 18 identifiers listed in the HIPAA Privacy Rules must be removed by a SDM-qualified honest broker:

   1. Names
   2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial 3 digits of a zip code if, according to the currently publicly available data from the Bureau of Census:
      i. the geographic unit formed by combining all zip codes with the same 3 initial digits contains more than 20,000 people; and
      ii. the initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
   3. All dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; 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.
   4. Telephone numbers
   5. FAX numbers
   6. Electronic mail addresses
   7. Social Security numbers

11/21/2014
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet protocol (IP) addresses
16. Biometric identifiers (including finger and voice prints)
17. Full face photos and comparable images
18. Any unique identifying number, characteristic or code

**De-identification Procedure**

The de-identification procedure will be a manual process. When the PHI is strictly a data extract the Honest Broker will first ensure that only the fields indicated in the IRB are pulled. Once pulled that data will not contain of any of the above 18 identifiers. In the case the an internal EHR id is used as a primary key to other related extracted information another id will be created to maintain relational integrity and the EHR’s id field(s) will be removed.

At times the data may consist of images, specifically radiological imagery, which will be de-identified by the investigator associated with the IRB with the use of Adobe Photoshop or other photo editing software. Those images will be place within a HIPAA compliant folder where only the names of those listed on the IRB will have access to. Once the images are placed in the specified folder the Honest Broker will inspect every image for PHI information contained in the image itself or within the image’s metadata. All approved images will be renamed and moved to another approved folder, finally the previous filename and their new names will be recorded in a log file only accessible by the Honest Broker and the investigator(s).

Under certain circumstances, the IRB may approve a waiver of the requirement for prospective informed consent/authorization, in which case the investigator must provide a copy of the IRB approval letter including the specific scope of the waiver granted to SDM IT with the service request. Any researcher in this case must sign a SDM PHI Research Agreement (which is available at PHI Research Agreement [http://pre.dental.pitt.edu/current-policies-pertaining-hipaa]) before data access is permitted. Even if such a waiver is granted, the SDM requires that the following four identifiers are removed. The removal can be done by either qualified de-identification software or qualified database expert paid by the principal investigator.

1) Patient name
2) Patient SSN
3) Patient home street address
4) Patient phone number

b. For paper-based medical/dental record information, address the processes and/or systems that will be used to fully de-identify (i.e., HIPAA “Safe Harbor” compliant) the

11/21/2014
information for subsequent use by your affiliated researchers. (Note: See Attachment A for HIPAA "Safe Harbor" de-identification requirements.)

Not Applicable

5. Limited Data Sets of Medical/Dental Record Information:

a. For electronic medical/dental record information, address the processes and/or systems that will be used to develop Limited Data Sets of the information for subsequent use by your affiliated researchers. (Note: See Attachment A for HIPAA Limited Data Set requirements.)

Provision of a Limited Data Set:

PHI data extraction, export, print or report generation for any research purpose for existing PHI, including clinical studies, sample size estimation and pilot testing (if the investigator is not also the attending clinician), require an IRB approval with valid dates. A copy of the IRB approval letter must be presented to SDM IT with the service request.

In order to make the data available for research under this provision, only a "limited data set" may be provided. The following 16 identifiers listed in the HIPAA Privacy Rules must be removed by a qualified "honest broker." An honest broker must be a party who has legitimate access to the PHI requested (such as a member of the records staff or a treating clinician) and who is separate from the research team. Only a SDM certified honest broker with signed "SDM Business Associate Agreement for Honest Brokers" is allowed to provide honest broker services within the SDM. Any other proposed honest broker must be prospectively approved by the SDM (see "SDM Honest Broker Certification Policy" and "SDM Business Associate Agreement for Honest Brokers":

1) Names
2) Postal address information (other than town or city, state and zip code)
3) Telephone numbers
4) Fax numbers
5) E-mail addresses
6) Social security numbers
7) Medical record numbers
8) Health plan beneficiary numbers
9) Account numbers
10) Certificate/license numbers
11) Vehicle identifiers & serial numbers, including license plate numbers
12) Device identifiers & serial numbers
13) Web Universal Resource Locators (URL's)
14) Internet Protocol (IP) address numbers
15) Biometric identifiers, including finger and voice prints
16) Full face photographic images and any comparable images

11/21/2014
De-identification Procedure

The de-identification procedure will be a manual process. When the PHI is strictly a data extract the Honest Broker will first ensure that only the fields indicated in the IRB are pulled. Once pulled that data will not contain of any of the above 16 identifiers. In the case the an internal EHR id is used as a primary key to other related extracted information another id will be created to maintain relational integrity and the EHR's id field(s) will be removed.

At times the data may consist of images, specifically radiological imagery, which will be de-identified by the investigator associated with the IRB with the use of Adobe Photoshop or other photo editing software. Those images will be place within a HIPAA compliant folder where only the names of those listed on the IRB will have access to. Once the images are placed in the specified folder the Honest Broker will inspect every image for PHI information contained in the image itself or within the image's metadata. All approved images will be renamed and moved to another approved folder, finally the previous filename and their new names will be recorded in a log file only accessible by the Honest Broker and the investigator(s).

Under certain circumstances, the IRB may approve a waiver of the requirement for prospective informed consent/authorization. in which case the investigator must provide a copy of the IRB approval letter including the specific scope of the waiver granted to SDM IT with the service request. Any researcher in this case must sign a SDM PHI Research Agreement (which is available at PHI Research Agreement [http://ore.dental.pitt.edu/current-policies-pertaining-hipaa]) before data access is permitted. Even if such a waiver is granted, the SDM requires that the following four identifiers are removed. The removal can be done by either qualified de-identification software or qualified database expert paid by the principal investigator.

5) Patient name  
6) Patient SSN  
7) Patient home street address  
8) Patient phone number

b. For paper-based medical/dental record information, address the processes and/or systems that will be used to develop Limited Data Sets of the information for subsequent use by your affiliated researchers. (Note: See Attachment A for HIPAA Limited Data Set requirements.)

Not Applicable

c. Address your policies, procedures and controls for ensuring that Limited Data Sets of medical/dental record information that you provide to your affiliated researchers contain only the minimum necessary information needed to perform the research. (Note: These policies should include statements specifying that the medical/dental record information provided to researchers under a Limited Data Set will be consistent with the specific data elements requested in the corresponding IRB-approved research application and Data Use Agreement.)

11/21/2014 5
The policies and procedures in place currently focus on the following major issues:

**Written HIPAA Authorization under an IRB Approved Protocol**

Where the IRB has approved a research protocol where research subjects provided prospective, written informed consent combined with the necessary elements of a HIPAA authorization, PHI within the scope of that consent/authorization may be extracted from the EHR. In each case, the investigator must provide a copy of the IRB approval letter, and the signed consent/authorization for each subject to SDM IT with the service request. The copies are attached to the request ticket in the IT ticketing system FootPrints.

**Provision of a De-Identified Data Set**

In order to make the data available for research under this provision, they must be de-identified. The following 18 identifiers listed in the HIPAA Privacy Rules must be removed by a SDM-qualified honest broker.

6. Assignment of Re-Identification Codes to De-Identified (HIPAA "Safe Harbor") Medical/Dental Record Information and Limited Data Sets:

Address your policies, procedures and controls for the assignment of re-identification codes to the de-identified (HIPAA "Safe Harbor") medical/dental record information and/or Limited Data Sets of medical/dental record information provided to your affiliated researchers. (Note: These policies should include statements specifying that the assignment of re-identification codes will be based on project-by-project verification that the IRB granted approval of the use of re-identification codes. In addition, include statements addressing how re-identification codes will be appropriately managed by the honest broker so as to prevent researcher access to information linking these codes with corresponding patient-subject identifiers.)

A document will be in a secured area on the server that is HIPAA compliant that will store the cross referencing material prior to the extract. Access is limited to the Honest Broker and the IT Manager.

When de-identifying images for teaching purposes, images will be renamed following this schema: "name-of-image.jpg" to "name-of-image-HB-2014-10-04--001.jpg". The requestor is allowed to rename the part "name-of-image," but must retain the "HB-2014-10-04--001.jpg." A spreadsheet will be maintained a log for all de-identified images.

7. Documentation and Quality Assurance:

a. Address your policies, procedures and controls for ensuring that Institutional Review Board approval has been granted for the use of de-identified (HIPAA "Safe Harbor") medical/dental record information or a Limited Data Set of medical record information prior to providing such to your affiliated researchers.

The School of Dental Medicine will not provide access to any information to any researcher until IRB submission and approval documentation is provided. No requests are entertained without prior IRB approval. The SDM will make no exceptions on this issue. Once attained the Honest Broker will verify any exemption form the IRB and/or requested fields to be pulled.
As part of the oversight process, regular reviews by the Security Officer will be performed to evaluate the requests fulfilled. This exercise will focus on the information provided and make sure that this was consistent with the IRB submission and approval. This exercise will also assess the temporal workflow and make sure that information was released only after the appropriate approvals were in place. Any discrepancies and errors will be initially locally evaluated and corrective measures taken, including teaching and training. The IRB will also be informed of any errors.

b. Address your policies and procedures for documenting each honest broker transaction with your affiliated researchers (e.g., documentation of the identity of researcher, identity of the research study, the nature of the information provided, corresponding IRB approval information, etc.)

The historical requests will be logged in the SDM IT ticketing system FootPrints. Any action by the Honest Broker associated with an IRB will not occur until this ticket is submitted with a copy of the approval letter and the signed consent/authorization for each subject. Only current School of Dental Medicine students, residents, and/or faculty submitting an IRB request will be accepted as valid. FootPrints facilitate an easy means of communication between the Honest Broker and the investigators involved with the IRB. This communication may involve questions and/or the status of Honest Broker tasks including the date and time the information was provided to the researcher.

Once receiving an exempt form via FootPrints the Honest Broker will print the form, sign the form, scan the signed form into FootPrints, and finally return the signed Assurance.

When receiving a revised exempt form via FootPrints the Honest Broker will associate that FootPrint ticket with the original submittal.

Oversight, request tracking and training

All submittals to the Honest Broker will be tracked in the IT ticketing system Footprints. This will enable the ability to easily lookup an IRB, view the IRB approval letter as well as the signed consent/authorizations for each investigator, and finally track any changes or additional request or IRB modifications.

A quarterly review will be conducted by the Honest Broker and the Security Officer, compliance will be documented. Possible changes to workflow will be discussed as well as any issues or questions.

Anyone wishing to assist the Honest Broker will be trained as a certified honest brokers via UPMC/Pitt Research Fundamentals Modules.

c. Address your policies and procedures for routine monitoring (auditing) of de-identified (HIPAA “Safe Harbor”) medical/dental record information and Limited Data Sets of medical/dental record information provided to affiliated researchers so as to ensure that this information has been de-identified in compliance with respective HIPAA requirements.

The workflow that the Honest Broker will follow ensures that all de-identified datasets will be compliant with the needs of HIPAA. The Honest Broker will also make sure the information provided is consistent with the requirements of “Safe Harbor” and “Limited Data Set” requirements, as appropriate for each individual request.
The stated workflow will be reviewed regularly by the Honest Broker and the Security Officer and will be revised as needed.

d. Address your policies and procedures for managing and ensuring the security of all identifiable medical/dental record information that is in the Honest Broker's possession during the performance of its de-identification (HIPAA "Safe Harbor") or creation of Limited Data Set functions.

   The data is stored electronically on systems that are regularly audited by University of Pittsburgh approved HIPAA auditors and are compliant with the HIPAA standards. No data with PHI will be stored temporarily or permanently on a non-compliant HIPAA device and/or non-compliant HIPAA systems.

   Access to the electronic systems is password protected and any access to these systems is monitored in accordance with the University of Pittsburgh HIPAA System Security policies. The staff are trained via UPMC/Pitt HIPAA modules. They will be aware of their responsibilities in keeping passwords secure and contacting the appropriate personnel in case they think their passwords has been compromised or if there is any other breach of confidentiality.

8. **Business Associate Agreement:**

   Are all individuals serving as honest brokers employees of SDM?
   [ ] No. Please submit a completed signed business associate agreement. (Note: the standard SDM Business Associate Agreement can be found at [http://pre.dental.pitt.edu/current-policies-pertaining-hipaa](http://pre.dental.pitt.edu/current-policies-pertaining-hipaa)).
   [ X] Yes. A business associate agreement is not required.
CERTIFICATION OF HONEST BROKER RESPONSIBILITIES

By signing below I agree/certify that:

1. I am cognizant of and will comply with the Federal Policy (Common Rule) and HIPAA regulations and the IRB and SDM policies governing research involving the use of identifiable medical/dental record information.

2. I have reviewed this Honest Broker System/Process application in its entirety and I am fully aware of and in agreement with all submitted statements.

3. I will ensure that the Honest Broker System/Processes will be implemented and followed in strict accordance with this application.

4. I will request and obtain IRB and SDM HIPAA Security Officer approval for any proposed modifications to this application prior to implementing such modifications.

5. I will ensure that all individuals involved in providing the Honest Broker System/Process services are provided with a copy of this current version of this application.

6. I and/or my Honest Broker staff will not provide identifiable medical/dental record information, de-identified medical/dental record information, or Limited Data Sets of medical/dental record information to affiliate researchers until evidence of IRB approval of the corresponding research study is provided.

7. I will respond promptly to all requests for information or materials solicited by the SDM HIPAA Security Officer or the IRB.

8. I will maintain adequate documentation of all Honest Broker transactions with affiliated researchers.

9. I and/or my Honest Broker staff will, under no circumstances, provide the researchers with information that would permit de-identified (HIPAA "Safe Harbor") medical/dental record information or Limited Data Sets of medical/dental record information to be linked to patient identifiers.

10. I and/or my Honest Broker staff will not intervene or interact with patients in the conduct of Honest Broker functions.

11. I and/or my Honest Broker staff will maintain complete confidentiality of identifiable medical/dental record information in our possession during the performance of Honest Broker functions.

11/21/2014
Policy/Procedure: SDM Honest Broker Certification Policy and Procedures

Signature of Individual Responsible for Honest Broker System/Processes: [Redacted] HB103

Date: 11/20/2014

Honest Broker System/Process Application Approved: [Redacted]

SDM HIPAA Security Officer: [Redacted]

Date: 11/26/2014

IRB Chair/Vice Chair: [Redacted]

Date: [Redacted]

11/21/2014
ATTACHMENT A

A. HIPAA “Safe Harbor” De-Identification of Medical/Dental Record Information

HIPAA requires that each of the following identifiers of the individual or of relatives, employers, or household members of the individual must be removed from medical record information in order for the records to be considered de-identified (HIPAA “Safe Harbor”)

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial 3 digits of a zip code if, according to the currently publicly available data from the Bureau of Census:
   a. The geographic unit formed by combining all zip codes with the same 3 initial digits contains more than 20,000 people; and
   b. The initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changes to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; 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.
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers; license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, except a code to permit re-identification of the de-identified data by the Honest Broker.
ATTACHMENT A (continued)

B. Limited Data Sets

For Limited Data Sets, HIPAA requires that each of the following identifiers of the individual or of relatives, employers, or household members of the individual must be removed from medical/dental record information.

1. Names
2. Postal address information, other than town or city, State, and zip code
3. Telephone numbers
4. FAX numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers; license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers
16. Full face photographic images and any comparable images

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of revision</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/19/2008</td>
<td>Document created</td>
<td>Fen Zheng</td>
</tr>
<tr>
<td>9/18/2009</td>
<td>Document reviewed</td>
<td>Wilbert Milligan</td>
</tr>
<tr>
<td>09/21/2009</td>
<td>Approved by the Division Director</td>
<td>Titus Schleyer</td>
</tr>
<tr>
<td>09/21/2009</td>
<td>Approved by the Department Chair</td>
<td>Robert Weyant</td>
</tr>
<tr>
<td>09/21/2009</td>
<td>Approved by the Dean of the School</td>
<td>Thomas Braun</td>
</tr>
<tr>
<td>05/09/2011</td>
<td>Document division name updated</td>
<td>Fen Zheng</td>
</tr>
<tr>
<td>5/12/2012</td>
<td>Document reviewed</td>
<td>Heiko Spallek</td>
</tr>
<tr>
<td>9/17/2014</td>
<td>Document reviewed</td>
<td>Fen Zheng</td>
</tr>
<tr>
<td>11/12/2014</td>
<td>Document reviewed and modified</td>
<td>Patrick L. Hetherington</td>
</tr>
<tr>
<td>11/12/2014</td>
<td>Document reviewed</td>
<td>Heiko Spallek</td>
</tr>
</tbody>
</table>