HILLSBOROUGH COUNTY

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

PROCEDURES

July 1, 2017

Revised: September 11, 2020

Table of Contents

Section 1 - Statement of Commitment to Compliance

PROCEDURE

These HIPAA Procedures shall include policies and procedures designed to provide guidance to staff members regarding the standards, implementation specifications, and other requirements of the HIPAA Privacy and Security Regulations. Staff members shall have access to a copy of the HIPAA Procedures for their use. The HIPAA Procedures shall be reviewed annually and modified as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of the HIPAA Privacy and Security Regulations. If the HIPAA Regulations require that a change be made to the Notice of Privacy Practices because of the change made to the HIPAA Procedures, the HIPAA Privacy Officer shall facilitate the required change to the Notice of Privacy Practices.

To assist staff members with HIPAA Regulation compliance, each staff member shall complete the computerized HIPAA Awareness Training Program. A department may also develop additional training formats. Examples of such training may include general overviews of the HIPAA regulation requirements presented in larger group settings and more in-depth in-service training in smaller group settings designed to meet the needs of staff members in particular job roles. Individuals who are hired after initial training sessions commence will be given instructions in HIPAA compliance facilitated by a senior staff member. These instructions may occur in various settings, including individualized instruction and large or small groups. Training must be completed by the newly hired staff member before that staff member is permitted to receive, review, or otherwise handle PHI. Online training and testing must be completed within 30 days of hire.

The County shall implement, and staff members shall utilize, adequate safeguards to protect the privacy of individuals when PHI is collected, used, disclosed or maintained by staff members and to avoid accidental release of PHI. See Section 8 Safeguard Requirements, of this manual for more information.

Each covered entity department shall identify a Department HIPAA Liaison(s) to coordinate the use and disclosure of PHI. The Department HIPAA Liaison(s) will also work with others to identity how PHI is used by the department and the types of requests for disclosure of PHI received. All requests for disclosure will be forwarded to the Department HIPAA Liaison(s) for review, unless a specific policy in the HIPAA Procedures provides otherwise. The Department HIPAA Liaison(s) will also interface with the HIPAA Privacy Officer on behalf of the County's HIPAA Regulation matters. Whenever a reference is made in the HIPAA Procedures to the referral of a matter to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review or action, the initial review of the matter will be made by the Department HIPAA Liaison(s). If the Department HIPAA Liaison(s) determines that the matter need not be referred to the HIPAA Privacy Officer, then the Department HIPAA Liaison(s) may take or direct final action on the matter in consultation with the Department Director. If the Department HIPAA Liaison(s) determines that review by the HIPAA Privacy Officer is desirable under the

circumstances then, the Department HIPAA Liaison(s) will refer the matter to the HIPAA Privacy Officer.

Covered entity departments shall utilize a tracking system to account for all information that the HIPAA Privacy Regulation requires to be tracked, including but not limited to, requests for disclosure of PHI received by and disclosures of PHI. The Department HIPAA Liaison(s) shall work with the Section Managers to develop protocols for entering the required data into the HIPAA tracking system. Protocols may differ to meet individual service unit needs.

Covered entity department staff members and business associates shall use, maintain, and disclose PHI only in accordance with the HIPAA Procedures.

Section 2 – General Guidelines for Requests to Release Protected Health Information (PHI)

PROCEDURE

Requests for release of PHI for non-TPO (treatment, payment, and other administrative operations) purposes will be directed to the Department Manager or designee who will refer the matter to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review or action. The HIPAA Privacy Officer or Department HIPAA Liaison(s) will render a written determination of the request in a "timely manner" as established by law.

The Department HIPAA Liaison(s) will oversee the disclosure and tracking of all requests for PHI that are not for TPO.

Department HIPAA Liaison will consider the following when responding to requests to release PHI.

- Is the requested information PHI?
- Has the identity of the individual making the request been verified?
- Does the release require an authorization?
- Is the information being requested within the control of the department?
- Is there is a good faith belief that the release of PHI meets the standards established in this HIPAA Procedure and the applicable specific policies and procedures?

Department HIPAA Liaison(s) will limit PHI disclosed to the minimum necessary, i.e. the information reasonably necessary to accomplish the purpose for which disclosure is sought and will review requests for disclosure on an individual basis in accordance with such criteria. The Department HIPAA Liaison(s) will make reasonable efforts to limit the access. For all uses, disclosures, or requests which the minimum necessary standards apply, the Department HIPAA Liaison(s) will not use, disclose or request an entire medical record.

For requests of a routine or recurring nature, the Department HIPAA Liaison(s) will follow policies and procedures that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

Non-routine requests for disclosure will be referred to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review and action. The HIPAA Privacy Officer and/or Department HIPAA Liaison(s) will:

- Limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made.

- Review requests for disclosure on an individual basis in accordance with such criteria.

Except as otherwise permitted or required by these HIPAA Procedures or as permitted or required by law, the Department HIPAA Liaison(s) will not use or disclose PHI without an authorization that is valid as required by this Procedures Manual. See policy 5.01. When the Department HIPAA Liaison(s) obtains or receives a valid authorization satisfying the requirements of these HIPAA Procedures for its use consistent with the authorization granted. Authorizations may not be combined with any other document to create a compound authorization. See policy 3.02 and 5.01.

There are certain circumstances in which the Department HIPAA Liaison(s) may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose. See Policy 3.06.

The Department HIPAA Liaison(s) may use or disclose a limited data set that meets the requirements of these HIPAA Procedures only for the purposes of research, public health, or health care operations. The Department HIPAA Liaison(s) may use PHI to create a limited data set that meets the requirements of this HIPAA Procedures for disclosure of PHI for one of these purposes to a business associate whether or not the limited data set is to be used by the requestor. (See policy 7.02)

Except with respect to required disclosures, prior to any permitted disclosure under this Policy Manual, the Department HIPAA Liaison(s) will follow Policy 3.01 and will verify the identity of a person requesting PHI and the authority of the person to have access to PHI, when the Department HIPAA Liaison(s) does not know the identity or authority of the requesting individual. See Policy 3.01.

Section 3 – Uses and Disclosures

Subject: 3.01 - Verification of Identity and Authority

PROCEDURE

The Department HIPAA Liaison(s) shall meet with the Department Mangers to determine the types of disclosures of PHI made by staff member where the identity and authority of the requestor is "known to the Department HIPAA Liaison(s)" as described above.

All other requests for disclosure of PHI will be referred to the Department HIPAA Liaison(s) who will evaluate if appropriate documentation, statements or representations as to identity and authority have been provided; and if provided, whether the documentation, statement or representation made or provided by the requestor satisfies the identity and authority verification requirements of this Policy and the HIPAA Privacy Regulation. The Department HIPAA Liaison(s) may also consult with the appropriate Department Manager, other staff members, as needed, and the Office of the County Attorney regarding the matter.

If after review, the Department HIPAA Liaison(s) believes that the documentation, statement or representation provided by the requestor is not sufficient, the Department HIPAA Liaison(s) may request additional information from the requestor or refer the matter to the HIPAA Privacy Officer for review and final determination.

The documentation, statement or representation provided by a requestor verifying identity and authority shall be maintained in the client's file.

An entry describing the documentation, statement or representation provided by a requestor and/or requested and received by the Department HIPAA Liaison(s) to verify identity and authority shall also be made into the County's HIPAA tracking system.

Authority: Section 45 C.F.R. §164.514(h) Verification requirements.

Subject: 3.02 - Uses and Disclosure of PHI, Without an Authorization, Provided the Client is Given an Opportunity to Agree or Object to the Disclosure of the PHI or the Persons to Whom PHI is Disclosed

PROCEDURE FOR THE MAINTENANCE OF A FACILITY DIRECTORY

Information Which May Be Included

Facility Directories may include only the following types of PHI:

- The client's name.
- The client's location in the facility.
- The client's condition described in general terms that does not communicate specific medical information about the client; and
- The client's religious affiliation, which only may be disclosed to members of the clergy.

Opportunity to Restrict or Prohibit

Prior to inclusion of the client's PHI in the Facility Directory, the client must be (i) informed of the information to be included in the Facility Directory and the persons to whom such information may be disclosed; and (ii) given the opportunity to restrict or prohibit some or all of the uses or disclosures of the PHI in the Facility Directory. The restriction or prohibition of the client's PHI shall be made in writing on the appropriate County approved form by the client or their representation.

The Facility Directory shall not include any PHI the client objects to. If the client restricts the PHI to be included, the PHI may only be included in the manner required by the client. Any restricted use must be noted on the Facility Directory by the client's name.

The PHI in the Facility Directory may not be disclosed to any persons to whom the client objects. The names of such individuals must be noted on the Facility Directory by the client's name.

PROCEDURE FOR DISCLOSURE OF PHI WITHOUT AN AUTHORIZATION TO PERSONS INVOLVED IN CLIENT'S CARE OR PAYMENT FOR CARE:

The Types of Information Which May Be Disclosed

PHI, which is directly relevant to the client's care or payment related to the client's health care, may be disclosed to a family member, other relative, or a close personal friend of the client, or any other person identified by the client.

PHI for the purpose of notifying or assisting in the notification of the client's location, general condition or death may be disclosed to a family member, a personal representative of the client or another person responsible for the care of the client.

Requirements for Disclosure of the PHI Listed Above

When the client is present or available and has the capacity to make his or her own health care decisions then prior to disclosure or at the time of disclosure, the client must have agreed to the disclosure, or be provided with the opportunity to object to the disclosure and not express an objection, or the staff member may reasonably infer from the circumstances that the client does not object to the disclosure based on the staff member's professional judgment.

When the client is not present or the opportunity to agree or object to the use or disclosure cannot be practicably provided due to the individual's incapacity or because of an emergency circumstance, the staff member may exercise professional judgment to determine whether the use or disclosure is in the best interest of the client and the staff member may only disclose the PHI which is directly relevant to the involvement of the family member, other relative, or close personal friend of the client, or any other person who has been identified by the client in the client's health care.

Staff Members may use professional judgment and their experience with common practice to make reasonable inferences of the client's best interest in allowing a person to act on behalf of the client to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of PHI.

Staff members may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts for the purpose of coordinating with such entities the uses or disclosures of PHI to notify or assist in providing notice of, the location, general condition or death of the client to the family member, personal representative of the client or another person responsible for the care of the client The requirements stated in Paragraphs 1 and 2 above shall also apply to disclosures made under this Paragraph 4, if the staff member determines in the exercise of his or her professional judgment that compliance with those requirements does not interfere with the ability to respond to the emergency circumstance

Authority: 45 C.F.R. §164.510 Uses and disclosures requiring an opportunity for the client to agree or to object.

Subject: 3.04 Personal Representatives

PROCEDURE

A client may have a personal representative, and the representative must be treated just as the client would be treated by staff members. This means that the personal representative can receive PHI about the client, is able to make written authorizations for disclosure just as the client would, and can make medical decisions for the client.

If someone claims to be the personal representative of a client, you must first confirm his or her authority to act on behalf of the client.

If a person has legal authority to act on behalf of an adult or emancipated minor in making decisions related to health care, staff members must recognize this person as the client's personal representative. Staff members may request written documentation, such as a court order, that the person has legal authority. Staff members should make a copy of this documentation for the client's file for future reference. For example, you will need such verification if the person requests the client's PHI.

If a parent, guardian, or other person acting in loco parentis has authority to act on behalf of a minor, then staff member must recognize that person as the personal representative of the client. Staff members may request evidence of the representative's relationship to the client. For example, if the person is the client's parent, you may ask for a picture identification to confirm the parent's name and identity. If the representative is the legal guardian, you can ask for written documentation. Staff members should make a copy of this documentation for the client's file for future reference. For example, you will need such verification if the person requests the client's PHI.

There are some exceptions under law where un-emancipated minors may make their own decisions regarding health care.

A minor has the authority to act as an individual with respect to health information and health care service in certain circumstances prescribed by law. The consent of the un-emancipated minor in this case is sufficient.

A minor may lawfully obtain health care services without the consent of a parent or guardian, if a court or another person authorized by law gives the individual rights.

A parent or guardian may allow for an agreement of confidentiality between a covered health care provider and the minor with respect to health care services.

If an executor, administrator or other person has authority to act on behalf of a deceased person or that person's estate, staff members must recognize that person as the personal representative of the deceased client. Staff members may request documentation necessary to verify the person's legal status as the deceased client's personal representative. Staff members should

make a copy of this documentation for the client's file for future reference. For example, if the person requests additional information on the client, you will need this verification.

After you have confirmed that individuals are authorized to serve as clients' personal representatives, and before you allow them to see PHI or make medical decisions, you should verify the circumstances. There are some circumstances when access to PHI can be denied.

Staff members may elect not to treat a person as the personal representative of a client, if any of the following apply:

You have a reasonable belief that the client has been or may be subjected to domestic violence, abuse, or neglect by the person acting as the personal representative.

You have a reasonable belief that treating the person as the personal representative could endanger the client.

Existing State or other law, including applicable case law, may require that you disclose the PHI of an un-emancipated minor to a parent, guardian or other person acting *in loco parentis*, regardless of whether or not they are the client's personal representative. You must act in compliance with applicable State or other law, or

Existing State or other law, including applicable case law, may prohibit the disclosure of the PHI of an un-emancipated minor to a parent, guardian or other person acting *in loco parentis*. You must act in compliance with applicable State or other law.

When the parent, guardian, or *loco parentis* is not the personal representative of the un-emancipated minor client, and state law or other applicable case law does not prescribe access, staff members may decide whether or not to disclose PHI. This decision must be made by a licensed professional using his or her professional judgment.

You may deny access to PHI if, in the exercise of professional judgment, you decide that it is not in the best interest of the client to treat the person as the client's personal representative. Once you have verified the authority of the personal representative and the individual circumstances, staff member must treat the personal representative with the same rights as the client.

Authority: 45 C.F.R. §164.502(g) Personal representatives.

Subject: 3.05 Minimum Necessary

PROCEDURE

The following protocols shall be followed by each service unit (sections) to establish the limitations on staff members' access to PHI to conform to the "Minimum Necessary" standard:

- Each Section Manager shall meet with the HIPAA Privacy Officer and the Department HIPAA Liaison(s) to determine by service units (sections) job classification the "minimum necessary" PHI which may be accessed and used by staff members in a particular job classification in order to carry out their respective job responsibilities.

- The description of the types of information that may be accessed or used by staff members is listed in paragraph F, which follows.

The following protocols shall be followed by each service unit (section) to establish its "Minimum Necessary" standard for routine and recurring service unit (section) disclosures.

- Each Section Manager shall meet with the HIPAA Privacy Officer and the Department HIPAA Liaison(s) to determine the types of requests for disclosure of PHI received by that service unit (section) that may be categorized as routine and recurring. They shall also identify the "minimum necessary" PHI which may be disclosed by staff members in response to these routine and recurring requests.

- The description of the types of requests identified as routine and recurring for each service unit (section) and the "minimum necessary".

In the circumstances listed below a staff member may rely on the request as meeting the "minimum necessary" standard for disclosure if, under the circumstances, his or her reliance is reasonable:

- Disclosure to a public official when a valid authorization or the opportunity for the individual to agree or object is not required by the HIPAA Privacy Regulation, if the public official represents that the information is the minimum necessary needed.

- The information is requested by another covered entity.

- The information is requested by a professional who is a staff member or an employee of a business associate for the purpose of providing professional services to client, if the professional represents that the information is the minimum necessary needed.

- Documentation or a representation that complies with the requirements for disclosures for research purposes is provided to staff member. Staff member may rely on the request for disclosure of PHI for research purposes as meeting the "minimum necessary" standard for disclosure if the person requesting the information has provided documentation or

representations complying with the applicable requirements of Section 45 C.F.R. §164.512(i) of the HIPAA Privacy Regulation.

For all uses and disclosures or requests to which the "minimum necessary" requirements of this Policy apply, no staff member shall use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount which is reasonably necessary to accomplish the purpose of the use or disclosure.

Authority: Sections 45 C.F.R. §164.502(b) Minimum necessary, 45 C.F.R. §164.514(d) Minimum necessary requirements.

Subject: 3.06 De-Identified

PROCEDURE

Staff members may de-identify PHI by removing the identifiers listed below for the client or the client's relatives, employers, or household members; provided that staff member does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify a client who is a subject of PHI:

- Names
- All geographical subdivisions smaller than a State, including street, address, city, county, precinct, zip code and their equivalent geocodes; except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census.
- The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
- The initial three digits of a zip code for all such geographic units containing 20,000or fewer people is changed to 000.
    - 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.
    - Telephone numbers.
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)

- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except those permitted to re-identify the information.

Hillsborough County may assign a code or other means of record identification to allow itself to re-identify de-identified information. The code shall not be derived from or related to information about the individual and shall not be otherwise capable of translation so as to identify the individual. Hillsborough County shall treat the code or other means of record identification, or mechanism for re-identification as PHI, and shall not use or disclose the code or other means of record identification unless the use or disclosure is permitted by the standards for the use and disclosure of protected health information under the privacy rule.

Authority: 45 C.F.R. §164.502(d) Uses and disclosures of de-identified information; 45 C.F.R. §164.514(a) – (c) de-identification and re-identification of PHI.

Subject: 3.07 Uses and Disclosures Required by Law

PROCEDURE

If a request for the disclosure of PHI for any of the purposes listed above is received by staff member, the staff member who first receives the disclosure request shall notify his or her Department Manager or designee of the request.

The Department Manager or designee will refer the disclosure request to the Privacy Officer and/or Department HIPAA Liaison(s) for review and approval. After written approval is received from the HIPAA Privacy Officer and/or Department HIPAA Liaison(s), the staff member may disclose the minimum necessary PHI as authorized by the HIPAA Privacy Officer or Department HIPAA Liaison(s).

An entry shall be made into the County's HIPAA Tracking System for each disclosure of PHI made pursuant to this policy.

Authority: Section 45 C.F.R. §164.512(a) Uses and disclosures required by law.

Subject: 3.08 Releases of Protected Health Information for Public Health Activities

PROCEDURE

If a request for the disclosure of PHI for any of the purposes listed above is received by staff member, the staff member who first receives the disclosure request shall notify his or her Department Manager or designee of the request.

The Department Manager or designee will refer the disclosure request to the Privacy Officer and/or Department HIPAA Liaison(s) for review and approval. After written approval is received from the HIPAA Privacy Officer and/or Department HIPAA Liaison(s), the staff member may disclose the minimum necessary PHI as authorized by the HIPAA Privacy Officer or Department HIPAA Liaison(s).

An entry shall be made into the County's HIPAA Tracking System for each disclosure of PHI made pursuant to this policy.

Authority: Section 45 C.F.R. §164.512(b) Uses and disclosures for public health activities.

Subject: 3.09 Disclosures about Victims of Crime, Abuse or Domestic Violence

PROCEDURE

In accordance with Paragraph 1 above, a staff member who believes that an incident has occurred which requires a report to be made to the central abuse hotline, must immediately inform his or her Department Manager or the Department Manager's designee who shall be responsible for making such report or directing the staff member to make such report.

If a staff member believes a disclosure of PHI should be made, the staff member shall immediately inform the Department Manager or the Department Manager's designee who shall refer the matter to the HIPAA Privacy Officer or the Department HIPAA Liaison(s) for determination of whether the disclosure should be made and the extent of the information to be disclosed.

The Department Manager or the Department Manager's designee, in consultation with the HIPAA Privacy Officer or Department HIPAA Liaison(s), shall make the determination whether the individual about whom the disclosure has been or will be made will receive the notification discussed in Paragraph 3 above.

Authority: Section 45 C.F.R. §164.512(c) Disclosures about victims of crime, abuse or domestic violence.

Subject: 3.10 Law Enforcement Purposes

PROCEDURE

The staff member receiving a request for disclosure for law enforcement purposes, or considering a disclosure, shall immediately notify his or her Section Manager or designee.

Under conditions not governed by emergency circumstances, the Section Manager or designee, prior to the disclosure of any PHI under this Policy, will first obtain written approval for disclosure from the HIPAA Privacy Officer or Department HIPAA Liaison(s). In emergency circumstances the Section Manager or designee will immediately contact the HIPAA Privacy Officer or Department HIPAA Liaison(s) for further instructions.

Upon receipt of the approval to disclose from the HIPAA Privacy Officer or the Department HIPAA Liaison(s), the Section Manager or designee will direct the staff member to use or disclose the PHI as authorized by the HIPAA Privacy Officer or Department HIPAA Liaison(s), subject to any limitations set forth above for specific types of disclosures and the following limitations:

- Except as permitted above, staff member shall not disclose, for the purposes of identification or location, any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

- An entry shall be made into the County's HIPAA Tracking System for each disclosure of PHI made pursuant to this policy.

Authority: Section 45 C.F.R. §164.512 (f) Uses and disclosures for the information disclosed for Law Enforcement Purposes.

Subject: 3.11 Judicial or Administrative Proceedings Purposes

PROCEDURE

A staff member shall promptly notify his or her Department Manager or designee, when a request for disclosure of PHI for judicial or administrative proceeding purposes is received.

The Department Manager or his or her designee will refer the disclosure request to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review and, additionally, shall forward a copy of the request to the County Attorney's Office.

Working together, the County Attorney's Office and the Department Manager or his or her designee shall coordinate the review of and response to the disclosure request with the HIPAA Privacy Officer and/or Department HIPAA Liaison(s).

Disclosure of PHI for judicial or administrative proceedings purposes shall only be made with the prior written approval of the HIPAA Privacy Officer and/or the Department HIPAA Liaison(s) in consultation with the County Attorney's Office.

If the request for disclosure is approved, as provided above, the HIPAA Privacy Officer and/or the Department HIPAA Liaison(s), in consultation with the County Attorney's Office shall determine the minimum necessary PHI to be disclosed in response to the request. Staff member shall only disclose the minimum necessary PHI as identified and authorized by the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) in consultation with County Attorney's Office.

Authority: Section 45 C.F.R. §164.512 (e) Uses and disclosures of PHI for judicial or administrative proceedings purposes.

Subject: 3.12 Uses and Disclosures about Deceased Individuals and Cadaveric Organ, Eye or Tissue Donation Purposes

PROCEDURE

If a staff member believes in good faith that PHI constitutes evidence of criminal conduct that occurred on the premises of a County facility the staff member shall immediately contact his or her Department Manager or his or her designee. The Department Manager or his or designee shall immediately refer the matter to the HIPAA Privacy Officer and/or the Department HIPAA Liaison(s). The HIPAA Privacy Officer and/or the Department HIPAA Liaison(s) shall review the information and make a determination as to whether disclosure should be made, and if made, the information to be disclosed. Any disclosure made under these circumstances shall be made by the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) only.

If a staff member receives a request for disclosure of PHI from an entity or organization described in Paragraphs 3 through 5 above, the staff member shall promptly contact his or her Department Manager or his or her designee. The Department Manager or his or her designee shall immediately refer the matter to the HIPAA Privacy Officer and/or the Department HIPAA Liaison(s). The HIPAA Privacy Officer and/or the Department HIPAA Liaison(s) shall review the request and make a determination as to whether disclosure should be made, and if made, the information to be disclosed. Any disclosure made pursuant to Paragraphs 3 through 5 above shall only be made at the express written direction of the HIPAA Privacy Officer and/or the Department HIPAA Liaison(s).

Authority: Sections 45 C.F.R. §164.512(g) Uses and disclosures about decedents; 45 C.F.R. §164.512(h) Uses and disclosures for cadaver organ, eye or tissue donation purposes.

Subject: 3.13 Uses and Disclosures – Research

PROCEDURE

A staff member who receives a request to use or disclose PHI for research purposes shall promptly notify his or her Department Manager or designee of the request. This requirement applies regardless of who the requestor is or whether the request is accompanied by an authorization. The HIPAA Privacy Officer must approve all uses and disclosures of PHI for research purposes.

The Department Manager or designee will refer the request to the Department HIPAA Liaison(s) who will forward the request to the HIPAA Privacy Officer for review and approval. If the request to use or disclose the PHI for research purposes is approved by the HIPAA Privacy Officer, staff member shall only permit the use of or disclose the minimum necessary PHI approved to be used or disclosed by the HIPAA Privacy Officer in response to the request. Staff member may also disclose limited data sets in connection with the disclosure request provided that the requirements of Policy 7.02 and Policy 7.03 are met.

An entry shall be made into the County's HIPAA Tracking System for each request received to use or disclose PHI for research purposes. In addition, a follow-up entry must be made into the tracking system of the resolution of the request and, if the request was approved, of the PHI or, if applicable, limited data set, used or disclosed.

Authority: Section 45 C.F.R. §164.512(i) Research Purposes.

Subject: 3.14 Uses and Disclosures – Avert a Serious Threat

PROCEDURE

In the event that a staff member believes that a disclosure of PHI pursuant to this policy is necessary, the staff member will:

- Immediately, contact the staff member's Department Manager or his or her designee, who will then contact 911 and the Security Office (if applicable).
- Document the incident and forward with the case number of the police report (if applicable), and any documentation from the law enforcement agency to the administrative office, on the same day of the incident.

LIMITATIONS ON DISCLOSURE

- Disclosure of PHI under this Policy must be limited and must not include, for the purposes of identification or location, any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or issue.
- Disclosures, as described above herein, may only include the following information: name and address, date and place of birth, social security number, if permitted by Florida Public Records Law, ABO blood type and Rh factor, type of injury, if applicable, date and time of treatment, date and time of death, if applicable.

Authority: Sections 45 C.F.R. §164.512 (f)(2)(i) and (j)(1-4) Uses and disclosures for which an authorization or opportunity to agree or object is not required to avert a serious threat to health or safety.

Subject: 3.15 Uses and Disclosures – Specialized Government Function

PROCEDURE

When a staff member receives a request for use or disclosure of PHI for a specialized government function, the staff member shall notify the Section Manager or designee who shall refer the matter to the HIPAA Privacy Officer and/or Department HIPAA Liaison for review and action.

Authority: Sections 45 C.F.R. §164.512(k) Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is not Required – Specialized Government Functions.

Subject: 3.16 Workers' Compensation

PROCEDURE

Only staff members authorized to act on the behalf of the Human Resources for the purpose of worker compensation matters may disclose PHI under this policy.

When a request for disclosure of PHI under this policy appears to be non-routine in nature, the authorized staff member shall refer the request to his or her Department Manager or designee who will forward the request for PHI to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s). The HIPAA Privacy Officer and/or Department HIPAA Liaison(s) shall review the request and make the determination whether to disclose the PHI and determine the minimum necessary for disclosure.

Authority: Section 45 C.F.R. §164.512(l) Permitted Use and Disclosure of PHI, No restrictions –Workers' Compensation.

Subject: 3.17 Uses and Disclosures for Health Oversight Activities

PROCEDURE

If a request for the disclosure of PHI for any of the purposes listed in Paragraph 1 above is received by staff member, the staff member who first receives the disclosure request shall notify his or her Department Manager or designee of the request.

The Section Manager or designee will refer the disclosure request to the Privacy Office and/or Department HIPAA Liaison(s) for review and approval. After written approval is received from the HIPAA Privacy Officer and/or Department HIPAA Liaison(s), the staff member may disclose the minimum necessary PHI as authorized by the HIPAA Privacy Officer or Department HIPAA Liaison(s).

An entry shall be made into the County's HIPAA Tracking System for each disclosure of PHI made pursuant to this policy.

Authority: Section 45 C.F.R. §164.512(d) Uses and disclosures for health oversight activities.

Section 4 - Authorizations

Subject 4.01 – Authorization Requirements

PROCEDURE

When a staff member receives a request to disclose PHI information, or when a staff member desires to use PHI and no exception to the authorization requirement applies to the release or use of the PHI, the staff member shall refer the request or discuss the anticipated use with his or her Department Manager or his or her designee and provide the Department Manager or designee with a completed, but unsigned Authorization Form. The Department Manager or designee shall refer the request or the anticipated use, and the completed, but unsigned Authorization Form to the HIPAA Privacy Officer and/or the Department HIPAA Liaison(s) for review.

The HIPAA Privacy Officer and/or the Department HIPAA Liaison(s) shall review the request or anticipated use and determine whether an authorization is required, and if required, whether the completed Authorization Form has been properly completed.

If the HIPAA Privacy Officer and/or the Department HIPAA Liaison(s) determine that an authorization is required and further determine that the Authorization Form has been properly completed, the HIPAA Privacy Officer or the Department HIPAA Liaison(s) shall return the form to staff member with the direction to obtain the signature of the individual whose authorization is required.

No release or use of PHI may occur when an authorization is required, until a completed Authorization Form which has been approved by the HIPAA Privacy Officer and/or Department HIPAA Liaison(s), as required by Paragraph C above, is signed and dated by the individual whose authorization is required and delivered to staff member.

A copy of the signed Authorization Form must be provided to the individual signing the form.

Even if the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) has approved the Authorization Form and the disclosure of the PHI, no release of PHI may be made by any staff member if the staff member believes that the authorization is or has become defective, as described below. If a staff member believes that an authorization is or has become defective, the staff member shall notify his Department Manager or designee immediately, who is accountable for bringing the matter promptly to the attention of the Department Director or Director's Designee. The Director or Designee shall bring the matter to the attention of the HIPAA Privacy Officer and/or Department HIPAA Liaison(s). An authorization is defective when:

- The expiration date has passed, or staff member knows the expiration event has occurred.
- The authorization has been incorrectly completed.
- Staff member knows that the authorization has been revoked.
- The authorization violates Hillsborough County policies.

- Staff member knows that any material information in the authorization is false.

Authority: Section 45 C.F.R. §164.508 Uses and disclosures for which an authorization is required.

Section 5 – Notice of Privacy Practices

Subject 5.01 – Notice of Privacy Practices

PROCEDURE

Distribution of the Notice of Privacy Practices.

Approved Notice of Privacy Practices. At any point in time the Notice of Privacy Practices distributed and posted by the County shall be the most current Notice of Privacy Practices approved for use by all County departments. All staff member personnel and subcontractors shall utilize and distribute only the most current approved Notice of Privacy Practices.

Service Distribution. All department staff members shall distribute the Notice of Privacy Practices to each client at the time of service of that client. "Time of Service" shall mean the initial contact between the staff member and the perspective client at which PHI is received, whether that contact occurs by telephone or in person at a County facility or any other location. If service occurs through a telephone contact, then the Notice of Privacy Practices must be given to the client by the staff member who initially interviewed the client in the next face-to-face contact. Every Notice of Privacy Practices, which is given to a client, must be accompanied by a Written Acknowledgement Form, which is discussed in greater detail below. If service occurs in person at a County facility or any other location, then the Notice of Privacy Practices must be provided to the client at the time of contact by the staff member who initially interviews the client.

Each time the Notice of Privacy Practices is required to be provided to a prospective client or client, the staff member or business associate staff member shall request that the client sign a written acknowledgement form acknowledging receipt of the written Notice of Privacy Practices. Each time the Notice of Privacy Practices is mailed to a client, it shall be accompanied by the written acknowledgement form with the request that the client sign the form and return it to the appropriate Hillsborough County department.

Health Care Provider Distribution. Except in the event of emergency treatment, staff members in the Facility Based Service unit and staff members of all business associates of the County shall distribute the Notice of Privacy Practices at the date of first service delivery to the client. “First service delivery” shall mean the first visit made to the client by the staff member of the Services Program or the Facility Based Service Program or the Business Associate, respectively, after a referral for service has been made. In an emergency treatment situation, the Notice of Privacy Practices must be provided as soon as reasonably practicable to do so after the emergency situation has ended.

Written Acknowledgment. Each time a Notice of Privacy Practices is required to be given to a prospective client or a client, an approved Written Acknowledgment Form signed by the prospective client or client, must be obtained by the staff member or business associate staff member at the time the Notice of Privacy Practices is provided acknowledging receipt of the Notice of Privacy Practices. The Written Acknowledgement Form shall include a request that it be mailed back to the appropriate County Department. If for any reason a signed Written

Acknowledgment Form cannot be obtained, the staff member or business associate staff member with the responsibility of obtaining the Written Acknowledgment Form must document his or her efforts to obtain the Written Acknowledgment Form and the reason why it was not obtained. This may be documented on the Written Acknowledgement Form itself. The signed Written Acknowledgment Form or the documentation of the efforts to obtain the Written Acknowledgement Form must be maintained in the client's file.

Revised Notice. If a material revision to the Notice of Privacy Practices is made, then within sixty (60) days of the revision, a revised Notice of Privacy Practices and Written Acknowledgement Form acknowledging receipt of the Notice of Privacy Practices, shall be a distributed to all clients receiving services from a Hillsborough County Department or its Business Associates. The Written Acknowledgement Form shall include a request that it be mailed or given back to the appropriate County Department.

Posting of the Notice of Privacy Practices.

- The County shall post and make available the Notice of Privacy Practices on its website.
- The County shall post the Notice of Privacy Practices in a clear and prominent location in its administrative offices and in each of its facilities.

Authority: Sections 45 C.F.R. §164.502(i) Uses and disclosures consistent with notice; 45 C.F.R. §164.520 Notice of privacy practices for protected health information.

Section 6 – Contracts

Subject 6.01 – Contracts: Business Associate Agreements

PROCEDURE

The County will enter into Business Associate Agreements utilizing the Business Associate Agreement form approved by the County whenever circumstances permit. If changes to the approved form are requested by the business associate, the County will consult with the HIPAA Privacy Officer and the Office of the County Attorney before agreeing to such changes. All changes requested must be HIPAA compliant.

Before entering into any agreement or contract, and in keeping with county policy, the County will first obtain satisfactory assurance that the business associate will safeguard and limit use and disclosure of PHI.

The County will include the review of business associates' compliance as part of contract monitoring.

The County must record and maintain documentation to demonstrate compliance with this policy.

A contract between the County and a business associate must contain the following elements:

Establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate and contain language that the business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of the HIPAA Privacy Regulation except that:

The contract or other arrangement between the County and the business associate may permit the business associate to use and disclose PHI for the proper management and administration of the business associate or to carry out its legal responsibilities; and

The contract may permit the business associate to provide data aggregation services relating to the health care operations of the County.

Not use or further disclose the PHI other than as permitted or required by the contract or as required by law.

Use appropriate safeguards to prevent use or disclosure of PHI other than as provided by the contract.

Report to the County any use or disclosure of PHI not provided for by its contract of which it becomes aware.

Ensure that any agents, including a subcontractor to whom it provides PHI received from, or created or received by the business associate on behalf of, the County agrees to the same restrictions and conditions that apply to the business associate with respect to the PHI.

Make available PHI in accordance with Section 45 C.F.R. §164.524 of the HIPAA Privacy Regulation.

Make available the PHI for amendment and incorporate any amendments to PHI in accordance with Section 45 C.F.R. §164.526 of the HIPAA Privacy Regulation; Make available the information required to provide an accounting of disclosures in accordance with Section 45 C.F.R. §164.528 of the HIPAA Privacy Regulation.

Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the County available to the Secretary of Health and Human Services for the purposes of determining the County's compliance; and

At termination of the contract, if feasible, destroy all PHI received from, or related or received by the business associate on behalf of the County that the business associate still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protection of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

Authorize termination of the contract by the County, if the County determines that the business associate has violated a material term of the contract.

If the business associate of the County is a governmental entity, then the County may satisfy the contract requirements of this policy by entering into a memorandum of understanding with the governmental entity that contains terms that accomplish the above objectives.

The County may comply with the contract requirements of this policy if other law contains requirements applicable to the business associate that accomplish the above objectives.

If a business associate is required by law to perform a function or activity on behalf of the County or to provide a service described in the definition of business associate given in this Procedure Manual, the County may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without meeting the contract requirement above, provided that the County receives satisfactory assurances of such legal mandate.

The County may omit from its arrangements the termination requirement if such a provision is inconsistent with the statutory obligations of the County or its business associate.

The contract or other arrangement between the County and the business associate may permit the business associate to disclose the information received in its capacity as a business associate of the County, if:

- The disclosure is required by law.

- The business associate obtains reasonable assurances from the person or entity to which the PHI is disclosed that it shall be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed.

- The person or entity notifies the business associate of any instances of which it is aware in which the confidentially of the PHI has been breached.

- The contract shall not allow the use or further disclosure of PHI other than as permitted or required by the contract or as required by law.

- The contract shall direct the business associate to apply appropriate safeguards to prevent the use or disclosure of the PHI other than as provided for by the contract.

- The contract shall direct the business associate to report to the County any use or disclosure of the PHI.

- Direct the business associate to ensure than any agents, including any subcontractors, to whom it provides PHI received from, or created or received by the business associate on behalf of, the County agrees to the same restrictions and conditions that apply to the business associate with respect to PHI.

- The contract shall, in accordance with 45 C.F.R. §164.524 of the HIPAA Privacy Regulation, direct the business associate to assure that an individual has the right to inspect and obtain a copy of his/her PHI that is maintained by the business associate in a designated record set except for:

  - Psychotherapy notes.
  - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Authority: Sections 45 C.F.R. §164.502(e) Disclosures to business associates; 45 C.F.R. §164.504(e) Business associate contracts.

Subject 6.02 – Limited Data Set Agreements

PROCEDURE

Staff members must document the satisfactory assurances through a Data Set Agreement to assure the business associate or trading partner will appropriately use, maintain and safeguard the PHI.

Staff members will work with the Office of the County Attorney, the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) to develop the Data Set Agreement that will meet the standards of this policy and comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) laws and regulations.

The County staff members who receive any request for PHI in a limited data set shall inform the Section Manager or designee of the request. The Section Manger or designee is responsible to confirm with the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) that a limited Data Set Agreement is place before such information is released.

The County staff member may use or disclose a limited data set that meets the requirements of this policy and the Data Set Agreement. See Policy 7.03 for further policy and procedures for Data Set Specifications.

If a County staff member knows or learns of a pattern of activity or practice of the business associate or trading partner that constitutes a material breach or violation of the data use agreement, the staff member must notify the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) immediately.

Staff members must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful staff member must:

- Discontinue the disclosure of PHI in the limited data set to the business associate or trading partner.
- Report the problem to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s), who shall notify the Secretary of Health and Human Services.

Authority: Section 45 C.F.R. §164.514 (e)(1)(3) Standard: Limited data set. Implementation specification: Permitted purposes for uses and disclosures.

Subject 6.03 – Limited Data Set Specifications

PROCEDURE

A. The County's staff member may use or disclose a limited data set that meets the requirements of this policy and policy 7.02 - Data Set Agreement.

Authority: Section 45 C.F.R. §164.514(e) Limited data set.

Section 7 – Individual Rights

Subject 7.01 – Individual Rights of Access to Inspect and Copy Protected Health Information (PHI)

PROCEDURES

General

A staff member receiving a request for access to inspect or to obtain copy of that individual's PHI shall promptly notify his or her Department Manager or designee.

The Department Manager or designee will refer the request to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review and approval. The HIPAA Privacy Officer and/or Department HIPAA Liaison(s) shall require verification of an individual's identity and authority before approving the release of any PHI pursuant to this policy.

If the PHI requested is maintained or accessible to staff member onsite, staff member will either grant the request and provide access, or provide written notice of the denial of access in whole or in part, no later than thirty (30) days after receipt of the request. If the requested PHI is not maintained or accessible to staff member on-site, staff member will either grant the request and provide access, or provide written notice of the denial of access in whole or in part, no later than sixty (60) days from receipt of the request. The Department HIPAA Liaison(s) will monitor these time periods.

If staff member is unable to take any action required within the applicable thirty (30) day or sixty (60) day timeframes described above, staff member may extend the time for such actions by no more than thirty (30) days, provided that within the applicable initial thirty (30) or sixty (60) day time period, it provides the individual with a written statement of the reasons for the delay and the date staff member will complete its action on the request. Staff member may have only one such extension of time for action on any request for access.

If the Department does not maintain the PHI that is the subject of the individual's request for access, and staff member knows where the requested PHI is maintained, staff member must inform the individual where to direct the request for access.

Approval of a Request

If an individual's request for access to his or her PHI is granted, staff member will contact the individual in a timely fashion to arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or alternatively, mail a copy of the PHI at the individual's request. Staff member may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

Staff member will provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in that form or format; or, if not, in a readable hard copy form or such other form or format as agree to by staff member and the individual.

If the PHI requested is maintained in more than one designated record set or at more than one location, only one set needs to be provided for review.

Staff member may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if the individual agrees in advance to a summary or explanation of the PHI and to any fee which will be charged by staff member to prepare the summary or explanation.

If the individual requests a copy of the PHI or agrees in advance to a summary or explanation of the PHI, staff member may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

- Copying, including the cost of supplies for and labor of copying, the PHI requested by the individual.
- Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
- Preparing an explanation or summary of the PHI, if agreed to by the individual.

Denial of a Request

If an individual's request for access to his or her PHI is denied in whole or in part, staff member will provide the individual timely, written denial. The denial will be in plain language and contain:

- The basis for the denial.
- If applicable, a statement of the individual's review rights under Section 45 C.F.R. §164.524(a)(4) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Regulation and how the individual may exercise such review rights and
- A description of how the individual may complain to the Department HIPAA Liaison(s) pursuant to the County's complaint procedures or to the Secretary of Health and Human Services.

Staff member will also permit the individual to submit to staff member a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreements. Staff member may prepare a written response to the individual's statement of disagreement. If such written statement is prepared, a copy must be provided to the individual.

Staff member will, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which staff member has denied access.

If the individual has requested a review of a denial under Section 45 C.F.R. §164.524(a)(4), staff member must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. Staff member must promptly refer a request for

review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on his or her exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person or the request for access is made by the individual's personal representative and the provision of access to the personal representative is reasonable likely to cause substantial harm to the individual or another person.

Authority: Section 45 C.F.R. §164.524 Access of individuals to protected health information.

Subject 7.02 – Amendment of Protected Health Information (PHI)

PROCEDURES

General

A member receiving a request from an individual to amend his or her PHI will notify the Section Manager or designee of the request who will refer the matter to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review.

Requests to amend PHI must be in writing and state a reason to support the requested amendment; provided that staff member informed the individual in advance of this requirement.

An entry shall be made into the County's HIPAA Tracking System for each request for amendment of PHI received for the following types of information:

- Identify the record or PHI in the designated record set that is the subject of the amendment.
- Append, or otherwise link, the individual's request for an amendment.
- Include the HIPAA Privacy Officer's or Department HIPAA Liaison(s)'s denial of the request.
- Include the individual's statement of disagreement, if any.
- Attach the HIPAA Privacy Officer's or Department HIPAA Liaison(s)'s rebuttal, if any.

Staff member will act on a request to amend PHI or a record no later than 60 days after receipt of the request.

If staff member is unable to take any action required within 30 days after receipt of the request, staff member may extend the time period for taking action for thirty (30) days and provide the individual with a written statement of the reasons for the delay and the date staff member will complete the request. Staff member may have only one such extension of time for action on any request for access.

Acceptance of an Amendment

If staff member accepts the requested amendment, in whole or in part, staff member will:

- Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

- Timely inform the individual that the amendment is accepted and obtain the individual's identification and agreement to inform and share the information with others as described in below.

- Make a reasonable effort to inform and provide the amendment in a reasonable time to:

    - Persons identified by the individual as having received PHI about the individual and needing the amendment; and

    - Persons, including business associates, that staff member knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

Denial of the Amendment

If staff member denies the request for access in whole or in part, staff member will provide the individual with a timely denial written in plain language that contains the following:

- The basis for the denial.

- The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.

- A statement that, if the individual does not submit a statement of disagreement, the individual may request that staff member provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

- A description of how the individual may complain to the Department or to the Secretary of Health and Human Services. Staff member will provide the individual with a contact information, if available, for such purposes.

- Staff member must permit the individual to submit to the staff member a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

- Staff member may prepare a written rebuttal to the individual's statement of disagreement. If such rebuttal statement is written, a copy will be provided to the individual.

Authority: Section 45 C.F.R. §164.526 Amendment of protected health information.

Subject 7.03 – Individual Right to File a Compliant

PROCEDURE

Any staff member who receives a complaint from an individual will immediately record on the designated Complaint log the name and contact information of the individual making the complaint and the nature of the complaint. Subsequently, the staff member will promptly forward the completed Complaint Form to the Section Manager or designee. If a complaint is received in written form, it should also be attached to the completed Department Complaint Form. The Section Manager shall refer the Complaint Form and all related information to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review and investigation. The Department HIPAA Liaison(s) may request confirmation of the identity and authority of the person making the complaint.

An entry shall be made into the County's HIPAA Tracking System for each compliant filed within 48 hours.

Should there be concern of a breach of HIPAA information or evidence of misuse, the Department HIPAA Liaison shall notify the HIPAA Privacy Officer within 48 hours of becoming aware of the situation, regardless of status of internal department investigation into the concern.

The completed Department Complaint Form and all other related information will be maintained for a minimum period consistent with the State of Florida's records retention policy.

Staff Members must fully cooperate with the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for Complaint Investigations and Compliance Reviews resulting from a complaint.

If requested, HIPAA Privacy Officer and/or Department HIPAA Liaison(s) will work directly with the Secretary of Health and Social Services, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the department and the circumstances regarding any alleged acts or omissions concerning compliance.

The Department will permit access by the HIPAA Privacy Officer during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information (PHI). The Department must permit access by the HIPAA Privacy Officer, at any time and without notice, to any information required that is in their exclusive possession.

A staff member must report any other staff member, associate, business associate or representative that fails or refuses to furnish the information in connection with a complaint investigation or inquiry to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s).

The Department will cooperate with any recommendations associated with the findings of the Secretary in connection with a complaint or inquiry or investigation by the Secretary.

The Department will keep records and submit timely compliance reports that contain information in the manner requested and as required by the Secretary as necessary to ascertain the compliance of the Department.

Authority: Sections 160.306 Complaints to the Secretary; 160.310 Responsibilities of Covered Entities; 160.312 Secretarial Action Regarding Complaints and Compliance Reviews; 45 C.F.R. §160.306, §160.310 and §160.312 Administrative requirements.

Subject 7.04 – Alternate or Confidential Communication

PROCEDURE

If an individual requests to receive PHI communications by alternate methods, the staff member should direct the individual to submit a written request. If Hillsborough County has approved a form for this purpose, the staff member will provide the individual with the approved form. The written request must state the following:

- Individual's Name.
- Alternative communications being requested (mailing address, telephone restrictions, language preference, or verbal communication).
- Beginning and ending dates for alternative communication.
- Special instructions.
- Communication method for the HIPAA Privacy Officer to contact the individual.

Staff members receiving a request from an individual for alternate means of communications of their PHI shall notify the Section Manager or designee and promptly forward the written request, when received, to the Section Manager or designee. The Section Manager or designee will forward the written request to the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) for review and action.

An entry shall be made into the County's HIPAA Tracking System for each request for accommodations of alternate communications of PHI and the resolution. The records relating to the request, including the written request, must be maintained for a period consistent with the State of Florida's records retention policy.

Requests must be tracked for future review and administrative purposes using the County form or the written request and all other related information is to be maintained with the form or written request.

Authority: Sections 45 C.F.R. §164.502(h) Confidential communications; 45 C.F.R. §164.522(b) Confidential communications requirements.

Subject 7.05 – Notification of Release (Accounting of Disclosures)

PROCEDURE

If a staff member receives a request for an accounting of disclosure of his or her PHI, the Staff Member should direct the individual to submit a written request on the County developed form (see attachment).

Staff members receiving a request from an individual for an accounting of disclosure of their PHI shall promptly notify the Section Manager or designee and provide the written request to the Section Manager or designee for referral to the Department HIPAA Liaison(s). The Department HIPAA Liaison(s) may refer the matter to the HIPAA Privacy Officer for his or her review and determination.

An entry shall be made into the County's HIPAA Tracking System for each request for an individual's accounting of disclosure of their PHI.

Requests must be tracked for future review and administrative purposes using the County form (see attachment) and all other related information is to be maintained with form. The records must be maintained for a period consistent with the State of Florida's records retention policy.

Hillsborough County must act on a request for an accounting of disclosure no later than 60 days after receipt of the request.

- If the Department HIPAA Liaison(s) determines that Hillsborough County is unable to provide the accounting required within sixty (60) days after receipt of the request, the Department Manager shall immediately notify the Department HIPAA Liaison(s). The Department HIPAA Liaison may extend the time to provide the accounting by no more than thirty days provided that within the initial sixty (60) day period the Department provides the individual with a statement of the reasons for the delay and the date by which the Department will provide the accounting. The Department HIPAA Liaison(s) shall send this written statement to the individual.

- The Department may have only one such extension of time for action on any request for access.

After approval or denial is determined by the HIPAA Privacy Officer and/or Department HIPAA Liaison(s), the Staff Member may only disclose the information approved by the HIPAA Privacy Officer and/or Department HIPAA Liaison(s).

After approval or denial is determined by the HIPAA Privacy Officer and/or Department HIPAA Liaison(s), Staff Member will provide the individual with an accounting of the disclosures as directed by the HIPAA Privacy Officer and/or Department HIPAA Liaison(s). The following information for each disclosure shall be included in the accounting:

- The date of each disclosure.

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

- A brief description of the PHI disclosed; and

- A brief statement of the purpose for the disclosure or, in lieu of such statement, a copy of the written request for the disclosure, if any.

If during the period covered by the accounting, the Department has made multiple disclosures of PHI to the same person or entity for a single purpose under Section 45 C.F.R. §164.502(a)(2)(ii) of the HIPAA Privacy Regulation (Disclosures to the Secretary of Health and Human Services) or under Section 45 C.F.R. §164.512 of the HIPAA Privacy Regulation (No authorization or opportunity to agree or object required) the accounting may, with respect to the multiple disclosures, provide;

- All of the information required for the first disclosure.

- The frequency, periodicity, or number of the disclosures made during the accounting period; and

- The date of the last disclosure made during the accounting period.

If during the period covered by the accounting, the Department has made disclosures of PHI for a particular research purpose in accordance with Policy 3.16 for 50 or more individuals, the accounting may with respect to the individual's PHI provide:

- The name of the protocol or other research activity.

- A description, in plain language, of the research protocol or other research and the criteria for selecting particular records.

- A brief description of the type of PHI that was disclosed.

- The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure for the accounting period.

- The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the PHI was disclosed; and

- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If the Department provides an accounting for research disclosures, in accordance with Paragraph I of this policy, and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the Department shall at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

Authority: Section 45 C.F.R. §164.528 Accounting of disclosures of protected health information.

Section 8 – Safeguard Requirements

Subject 8.01 – Department HIPAA Liaison Security Responsibilities

Departments shall be responsible for complying with all Hillsborough County Information Technology policies, procedures, standards, and trainings. These policies and standards may be accessed on the County COIN website.

Authority: Hillsborough County IT Security Policies and Standards Section 45 C.F.R. §164.308(a)(2) Assigned security responsibility.

Subject 8.02 – Administrative Requirements – Safeguards for Release of Protected Health Information (PHI)

PROCEDURE

The Privacy Officer and Department HIPAA Liaison(s) will develop, where needed, reasonable safeguard procedures for the department, considering, among other things, the nature of the PHI handled by the department, the purposes for which it is used, received, disclosed or maintained, and any other factors which may impact the privacy of the individual's PHI.

The Department's staff members must not disclose PHI that it creates or receives, in a way that violates this policy.

The Department's staff members shall safeguard PHI when:

- Speaking on the telephone or in person; and
    - Will use reasonable care to speak quietly and avoid using client names in public places.
    - Will only discuss PHI to individuals permitted for treatment, payment, and other administrative operations (TPO) purposes or to individual who have been permitted authorization by the individual.
    - PHI may not be discussed when:
        - It can be heard by those not providing TPO.
        - Another individual is present.

Subject 8.03 – Policy Review/Compliance for HIPAA and IT Security Standards

PROCEDURE

Hillsborough County's HIPAA privacy and/or security Liaison(s) will be responsible to:

- Update these policies and procedures as necessary; and
- Periodically review and audit staff practice of such policies.

The review and audit shall be completed no less than once yearly.

Each section manager is responsible to make the initial training arrangement for HIPAA to staff members during the hiring process.

- Staff members training request should be made during the initial hiring process to establish a user account in the County's HIPAA training system and to identify the HIPAA training courses required for the staff member, based on their job responsibilities and functions.
- Staff members upon their first day in the office shall begin their HIPAA training using the County's online HIPAA training. In certain circumstances, some HIPAA tests may be written.
- After completion of training staff member must obtain a certificate of completion and provide a copy to their Department Manager.
- The Department Manager shall provide Human Resources a copy of the certificate of completion and training log.
- Human Resources shall update the staff member's HIPAA training status in their database.

Authority: Section 45 C.F.R. §164.308(a) Security management process.

Subject 8.04 – Employee User ID Accounts

PROCEDURE

COUNTY LAN SYSTEM, ID

- Human Resources department shall notify the IT Systems Coordinator by email as soon as they are aware of a new or terminated staff member.
- The Department Manager or designee(s) shall complete a New Hire Access Request form and email it to the IT Department.
- The Department shall save the form.
- The Department shall send necessary forms to the IT Department//Help Desk.
- For terminated employees, if we know in advance send the email 1 week before termination. If manager/supervisor is concerned with data corruption, the IT Department shall change the password as soon as they are escorted out the building.
- For employees that leave a Department, have all work related information transferred from the home drive of the employee leaving before their last day of service. Also collect all disks, thumb drives or any other portable media that may contain PHI.

HIPAA SYSTEMS

- Notify the HIPAA Liaison(s) and Training Coordinator by email as soon as you are aware of a user's new/terminated status.
- Only employees with a user-id and password can access any HIPAA system.
- All employees who use a HIPAA system require a user-id and/or password. The HIPAA Privacy/Security Liaison(s) or IT staff assigns these user-ids and passwords.

Authority: Section 45 C.F.R. §164.312(a)(2)(i) Unique user identification.

Subject 8.05 – Data Classification Guidelines for Electronic Data

PROCEDURE

Prior to saving an electronic document, staff member shall identify and classify the contents of the document as PHI, confidential, or public record, and shall save the record according to proper security standards.

Staff members shall save their files in accordance to the document's classification and defined security requirements, as provided for under Section 8 of this HIPAA Procedures for Storage and Handling of Electronic, Paper, and Verbal Information.

- PHI and confidential documentation shall be saved on a secured computer network drive and directory. Such network directory shall be secured with user privileges granted only to authorize staff members on a need to know basis.

- Staff members are responsible to contact the Department's systems coordinator to verify network drive/directory security.

Authority: 45 C.F.R. §164.312(a)(1) Access control.

Subject 8.06 – Personnel Security Screenings

PROCEDURE

Each Department Manager is responsible for the initiation of a criminal background screening for all staff members and such procedure shall be in accordance with the procedures as outlined by Human Resources.

Authority: Human Resource Procedures.

Subject 8.07 – Disciplinary Process

PROCEDURE

Hillsborough County staff members shall follow procedures, as outlined in this manual and other Policies and Procedures.

Authority: Sanction policy.

Subject 8.08 – Disposal of Media (Electronic & Paper)

PROCEDURE

Department staff members shall adhere to IT, and County policies when destroying electronic documentation.

- PHI and confidential documentation meeting the guidelines of this policy.
- Staff members shall notify their department manager or designee immediately. Notification must be completed as soon as knowledge of the incident occurs.
- Upon knowledge of the disclosure, the department manager or designee will refer disclosure of PHI to the County's Department HIPAA Liaison(s) for all incidents and IT Help Desk or the Department's Coordinator for redaction of PHI from public record or email disclosures.

Paper

- PHI and confidential documentation meeting the guidelines of this policy must be shredded.
- The Department's staff members shall adhere to County policy and utilize all required County forms when requesting to transfer paper documentation to the County Record Center.

Electronic Mail

- If an incident of disclosure through the County's email system or violation occurs as listed in the policy, the staff member shall follow the procedures below.
- Inbound e-mails containing PHI (1) may be saved to a secured computer drive/directory, (2) must be printed, (3) must be permanently deleted from email, and (4) deleted from the computer's "Recycle Bin." It is not a violation of the law or recognized by the County as a disclosure of PHI, unless the inbound email was originally sent through the County's email system. If the disclosure originated through County's email, the staff member shall notify their Department Manager and provide them a copy of the e-mail.
- Outbound emails containing PHI (1) must be printed, (2) permanently deleted from email, and (3) deleted from the computer's "Recycle Bin." The staff member shall notify their Section Manager and provide them with printed e-mail.

Electronic Media

- The Department's staff members shall enlist the assistance of the Department's IT Systems Coordinator for disposal of portable computer storage devices containing PHI and/or confidential material.
- Computer files saved to the hard drive or network drive shall be (1) deleted from the directory, and (2) shall be deleted from the computer's "Recycle Bin."

- Computer files containing PHI and confidential material that is saved to a portable disk/devise drive shall be permanently deleted.
    - Staff members with files on a portable disk/devise drive that cannot be reformatted shall open file, remove contents, resave empty file under the same name, close file, and delete empty file.
    - Files on a portable disk/devise drive that can be reformatted shall be deleted and such drive shall be reformatted.

Authority: Device and media controls: disposal.

Subject 8.09 – Storage and Handling of Electronic, Paper, and Verbal Information

PROCEDURE

Department Managers will work with the privacy and security Liaison(s) and other appropriate staff members to develop, where needed, reasonable safeguard procedures for sections, considering, amongst other things, the nature of the information handled by the department, the purposes for which it is used, received, disclosed, maintained, and any other factors which may impact security or an individual's right to privacy for PHI confidential information.

Hillsborough County staff members must not disclose PHI, confidential information, or public record that it creates or receives, in a way that violates HIPAA policies and procedures.

Hillsborough County staff members shall safeguard PHI and confidential information when:

- Speaking on the telephone or in person:
    - Staff members will use reasonable care to speak quietly and avoid using client names in public places.
    - Staff members will only discuss PHI to individuals permitted for treatment, payment and other administrative operations (TPO) purposes or to individuals who have been permitted authorization by the individual.
    - PHI may not be discussed when:
        - Those not providing TPO can hear it.
        - An authorized individual is present.
        - Family or guardians are present, unless authorized or permitted by the individual or policy; and
        - Using the telephone or any recording device that can be overheard by those not permitted to use PHI.
    - Staff members will not disclose confidential information to unauthorized individuals
- Accessing a computer
    - Staff members will reasonably attempt to shield the view of the computer screen from public view and will ensure that PHI and confidential information is not left viewable on the screen when the computer is idle for periods greater than five (5) minutes.
    - Staff members will have a password protected screen saver installed on their computer and will lock their workstations when their computer is temporarily unattended.

- Staff members who have PHI or confidential information on their computer will log off the system when leaving for lunch and when leaving for the day.

- Staff member will not permit individuals to use their computer, if their computer contains PHI and/or confidential files, and these files can be accessed without password protection.

- Staff members will classify their electronic data in accordance with Section 8 of this HIPAA Procedures for Data Classification Guideline for Electronic Data and will save their files according to the document's defined security.

- Prior to saving electronic PHI or confidential documentation on the County network, Hillsborough County staff members shall contact the County's systems coordinator to verify the network computer drive and directory is secure and available only to authorized staff members on a need to know basis.

- Staff members with access to the County's network system are not permitted to save, maintain or store electronic files containing PHI, confidential information, for public record on a computer storage device/disk drive or non-network drive that is not subjected to routine backup by the IT. Staff members will save, maintain, and store their electronic files on the County's network system.

- Staff members should not be automatically saving electronic files containing PHI, confidential information, or public record to their a, b, c, d, or e drive or any portable computer storage device/disk drive or non network drive without prior manager/supervisor approval for reasons that may include:
  - Limited network access.
  - No network access.
  - Temporarily working outside of the network system due to network unavailability.

- Electronic files copied and saved in a non-network environment must be transferred to the County's network drive.
  - Staff members will keep their laptops out of view when traveling in a vehicle.
  - Staff members with no network access to the County's network computer system will save their PHI, confidential documentation, and public record files to a portable computer storage device/disk drive and submit it to their program's administration office for copying to the network at a minimum of two (2) times a week.
  - Staff members temporarily working outside of their normal work environment and do not have access to the County network computer system will transfer their PHI, confidential and public record files to the County's network computer system upon return to their normal work environment.

- Portable computer storage device/disk drives containing PHI, confidential information, and public record shall be stored in a secured environment, as required by this policy under Section 8 of this HIPAA Procedures for Safeguard for Release of Protected Health Information (PHI).

- Electronic files saved on a portable computer storage device/disk shall be disposed of in accordance with IT policy and this policy under Section 8 for Disposable of Media (Electronic & Paper).

- Staff members will use reasonable safeguard methods when transporting their lap top computers.

    - Staff members with limited access will transfer their PHI, confidential and public record files to the County's network computer system each workday.

    - Staff members will not store their laptops in a vehicle unattended, unless circumstances during business travel determine vehicle storage is the highest form of security available.

- Staff members will keep their computer passwords and other user identifiers confidential.

- Laptops and computer workstations are required to have a secondary password protection when turning the computer on outside of the County network environment.

- Staff members will follow all established safeguard and security requirements establish by the Information and Technology.

- "Off Sites" that have a computer Local Area Network (LAN) are responsible to perform, store, and transport network server backup tapes in accordance to IT established procedure.

    - LAN backups are to be completed each Monday.

    - Pull weekly "Off Site" tape out and label with the site name.

    - Place tape in secure pouch.

    - Place pouch in regular inter-office envelope.

- Staff members are responsible for securing their computer equipment during emergencies.

    - Turn the computer off, unplug from the surge protector, and unplug the surge protector from the wall.

    - Disconnect all cables from the computer: power cables, monitor cable, network connection cable, keyboard cable, mouse cable, printer cable, and modem cable.

- Wrap cables that are permanently attached around the outside of the item, i.e. keyboard cable around keyboard.
- Leave loose power cables attached to the surge protector.
- Staff members will identify their equipment by attaching their name to both the computer and monitor.
- Enclose the computer and monitor in large plastic bags that will be provided to each staff member.
- Staff members are responsible to notify the County's systems coordinator when their computer equipment is ready for transport.

  - The County's Information & Innovation Office (IIO) shall be responsible for the backup of computer files and the transport of computer equipment, electronic and paper files and software during times of emergencies. Each department is responsible for determining the operational files needed for backup.

- Accessing the copier. Staff members will not leave documentation with PHI unattended when making copies, and will reasonable safeguard the PHI and confidential information from disclosure
- Accessing the Facsimile (fax)
  - Include a pre-printed confidentiality statement on all fax cover sheets. The statement will instruct the receiver to destroy the faxed materials and contact the sender immediately, in the event the transmission reached him or her in error.
  - When transmitting PHI or confidential information, staff members will not leave such documentation unattended.
  - After transmission of PHI or confidential information, staff members will verify the recipient's fax number on the confirmation fax transmittal sheet to ensure delivery to the proper telephone number.
  - Staff members will periodically remind regular fax recipients to provide notification in the event their fax number changes.
- Accessing a Printer
  - Staff members will reasonable safeguard printed PHI/confidential information from disclosure by unauthorized staff members and the public.
  - Staff members will not leave printed PHI/confidential information at the printer.
- Leaving the work area

- Staff members will ensure that PHI/confidential is not left out in the open when away from their desk. The staff member will take reasonable steps to turn their work over if they will be temporarily away from their desk for a short period of time.

- Staff member will ensure that PHI/confidential is removed from the top of their desk and placed in a locked environment when away from their desks for long periods or when leaving for the day.

- Staff members will ensure all PHI/confidential is maintained in a locked environment when not in use.

- Staff members will ensure their computer workstation is locked or shut off, as further described in these procedures for accessing a computer.

Authority: Storage and Handling of Electronic, Paper, and Verbal Information; County Policy.

Subject 8.10 – Access Controls to County Information Systems and Resources

PROCEDURES

Managers/supervisors are required to complete and submit the authorized County forms to provide staff members access to the County's computer and telephone resources. Supervisors should submit the appropriate forms with manager approval to:

- Department systems coordinator for submission to IT for:
- Access to a network account, including software and network drive and directory security rights.
- E-mail access.
- Internet access.
- Addition/update to the telephone directory, and
- Installation or relocation of a telephone, including voice mail and caller ID.

Managers/supervisors requesting to update the employee's security or rights to IT controlled computer or telephone systems shall notify the Department's systems coordinator with the requested update.

Managers/supervisors requesting a change to the employee's security shall complete the appropriate form and submit it to the appropriate department.

Managers/supervisors shall arrange for staff members to obtain a unique account.

The Human Resources Department shall issue permanent and temporary employees processed through the County's Human Resources Information System a unique ID.

Non-County staff members are required to sign in and out with the receptionist and shall be issued a numbered identification badge. Upon entry into the work area and while conducting activities in the area, visitors shall be supervised. On exit, visitors shall return their issued identification badge. This procedure does not apply to County maintenance personnel carrying out their authorized job duties for Hillsborough County; however such personnel are required to be in uniform and have their employee identification badges displayed on the outside of their uniform.

Designated staff members for each department shall carry out the responsibilities required for the maintenance, termination, and tracking of access privileges for computer equipment; computer disks, drives, and directories; keys and key cards; paper files, and other resources. Upon notification, the department manager is responsible to report the misuse, breach, or violation to the department's security Liaison(s). Permitted access shall be assigned according to job function and responsibility.

Staff members are required to immediately notify their department manager of misuse of County information and resources and any intentional or unintentional breech in security, including violation of these policies and procedures. Managers and supervisors shall permit staff members access to secured environments, such as offices and file cabinets on a need to know basis.

Authority: IT Unique user identification.

Subject 8.11 – Privilege Management for Employee Access to County Information Systems and Resources

PROCEDURES

Managers/supervisors are responsible to immediately notify appropriate County personnel to discontinue electronic and physical access to County information systems and resources, due to terminations, transfers, change in job function or responsibility. Such notification shall be done upon knowledge or notification by designated staff members that are responsible for the issuance, maintenance, termination, and tracking of access privileges, which includes, but is not limited to: computer equipment; computer disks, drives, and directories; identification cards; keys and key cards; and paper files.

Authority: Termination procedures and Access controls.

Subject 8.12 – Disaster Recovery and Business Continuity Planning

PROCEDURE

Annual Planning

- Each department is required to complete an annual Continuity of Operations Plan (COOP).
- County Personnel shall annually update disaster recovery roster to include the most up to date staff member information. An updated copy of the roster shall be provided to each department manager.
- Contingency Manager shall identify an alternate work location(s) for staff members' assignment in the event operations and resources are disrupted at permanent work sites.
- Business Impact Analyst shall annually review the County's critical business functions and software applications that are required to continue essential services and operations.

Preparation

- Department managers are responsible to identify essential work assignments, files, forms, supplies, electronic equipment, alternate data collection methods, and other resources required of their sections for continued operations and post disaster recovery efforts. In the absence of an electronic system, each section shall be responsible to record and report necessary data for daily operations for work functions such as, billing; reports; and payments.
- Department mangers shall review and coordinate assignments and responsibilities with their supervisors and department staff members prior to an emergency or disaster. The review shall also include review of each staff members' emergency information, assignment of an alternate home work location, and the department's telephone emergency contact plan.
- Continuity coordinator shall designate a person to be responsible for the back-up and transportation of electronic data and equipment necessary for continued operations at assigned alternate work locations. Staff members shall follow policy and procedure under Section 8 for Storage and Handling of Electronic, Paper, and Verbal Information for securing their computer equipment during emergencies.
- During an anticipated emergency/disaster alert, the director shall develop an emergency contact plan with the managers and shall assign designated personnel to act as a representative to perform direct disaster relief duties at the Emergency Operations Center (EOC) until further notice.

Emergency/Disaster Watch

- All staff members are responsible to ensure their family's safety and to secure their homes and pets prior to a declared emergency or disaster. Staff members are an essential part of the

County's disaster recovery process and work attendance at an alternate home work site will be necessary.

- All staff members are responsible to monitor local media (e.g. radio, TV stations) for instructions.
- Staff members assigned Emergency Operating Center personnel shall contact the director and/or section managers to disseminate the latest information, and the Department managers shall initiate their established emergency contact plan.

Recover

- Staff members shall report to their assigned work location, as directed over the telephone by their manager or assigned designee.
- Staff members shall perform their job responsibilities as assigned by their manager or supervisor to provide essential services, continue operations, and to participate in the County's emergency disaster recovery process.

Authority: Contingency plan.

Section 9 – Other Policies and Procedures

Subject 9.01 – Sanctions

PROCEDURES APPLICABLE TO STAFF MEMBERS

Hillsborough County shall require the employees who have contact with PHI to sign a confidentiality statement of adherence to privacy and security policy and procedures. The Department HIPAA Liaison(s) will maintain a folder of these signed statements. The confidential statement states that the staff member acknowledges that violations of security policies and procedures may lead to disciplinary action, for example, up to and including termination.

When a staff member fails to comply, or is believed to have failed to comply, with any HIPAA Privacy Policy or Procedure of Hillsborough County, the compliance failure shall be reported to the Privacy Officer, Department HIPAA Liaison(s), and the staff member in question or his or her personnel representative.

The HIPAA Privacy Officer, or named designee, shall coordinate efforts with the staff member's supervisor or Human Resources personnel to investigate the extent of the violation. The investigation shall be conducted in accordance with County Personnel Policies.

If, based on the investigation a determination is made that the compliance failure is unintentional, disciplinary action must be immediately imposed and retraining must immediately occur to avoid future violations.

If, based on the investigation a determination is made that the compliance failure is intentional, all access to protected health information (PHI) must immediately be removed from the individual for as long as the HIPAA Privacy Officer, Department HIPAA Liaison(s), and the personnel representative, working with administration, deem necessary, to determine the severity of the compliance failure and the appropriate disciplinary actions to be taken.

Disciplinary actions taken pursuant to this Policy may include, but not be limited to, oral and written reprimands and/or termination.

All reprimands given, whether in oral or written form, and any other disciplinary actions taken pursuant to this Policy, must be documented and signed by the HIPAA Privacy Officer, Department HIPAA Liaison(s), and the individual against whom the disciplinary action is taken, as well as any other individuals deemed necessary or appropriate by County Personnel Policies.

All disciplinary actions taken pursuant to this Policy shall be taken in accordance with County Personnel Policies.

All disciplinary actions taken pursuant to this Policy will be conducted with the assistance of the HIPAA Privacy Officer and/or Department HIPAA Liaison(s) and must be logged and tracked (either in written or electronic form) using the designated Hillsborough County disclosure

tracking system for future compliance reviews and individual (event) per notification and retained for six years from the imposition of the disciplinary action.

Access to disciplinary actions taken must be tracked as long as PHI is maintained.

PROCEDURES APPLICABLE TO BUSINESS ASSOCIATES

When a Business Associate or an employee of a Business Associate fails to comply, or is believed to have failed to comply, with any HIPAA Privacy Policy or Procedure of Hillsborough County the compliance failure shall be reported to the Department Director, or Department HIPAA Liaison and the HIPAA Privacy Officer. The Department Director may also contact the County Attorney's Office.

The Department Director or Director's designee shall immediately notify the Business Associate in writing of the failure to comply, and if the failure is such that it may be remedied, request an immediate meeting to discuss the failure and the implementation by the Business Associate of a remediation plan to protect against such failures in the future. The Department Director or Director's designee shall request that the Business Associate submit its remediation plan in writing. If the failure to comply is such that it may not be remediate, then the Department Director or Director's designee may consult with Staff from the County Attorney's Office regarding applicable legal remedies.

If an employee of a Business Associate is cited on more than one occasion for failing to comply with the HIPAA Privacy Policies or Procedures of Hillsborough County then Hillsborough County shall request that such employee no longer have access to any PHI for its clients.

If a Business Associate fails to implement the remediation plan discussed above or if, the Business Associate or employees of the Business Associate continue to fail to comply with the HIPAA Privacy Policies and Procedures of Hillsborough County then the Department Director or Director's designee may consult with Staff from the County Attorney's Office regarding applicable legal remedies.

All notices for failure to comply sent to Business Associates and the remediation plans developed by Business Associates in response to hose notices must be logged and tracked (either in written or electronic form) using the designated Hillsborough County disclosure tracking system for future compliance reviews and individual (event) per notification and retained for six years from the date of the notice.

Authority: Sanctions.

Glossary

Access—The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any information resource.

Administrative Safeguards—Administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information (ePHI) and to manage the conduct of the covered entity's staff in relation to the protection of that information.

Authentication—The corroboration that a person is the one claimed.

Availability—The property that data or information is accessible and useable upon demand by an authorized person.

Business Associate (BA)—Any organization or individual with whom you have a written contract to provide or conduct business on your behalf. This may include a laboratory that conducts tests for your clients, or an organization that bills clients and insurance companies. Business Associates may access protected health information (PHI) to the extent authorized in the contract.

Note: Other covered entities (like providers) that must comply with HIPAA have their own policies and procedures to maintain the privacy of PHI, and do not require Business Associate contracts to do business with you.

Consent—Approval given by an individual for his or her protected health information to be disclosed for the purposes of treatment, payment, or operations.

Contrary—Contrary is used when a provision of state law differs from a HIPAA standard or requirement. When a contrary law exists, the one that affords an individual greater rights or privacy will usually become the standard for compliance.

Correctional Institution—Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a state or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody include juvenile offenders, adjudicated delinquents; aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered Entity—

1) A health plan.

2) A health care clearinghouse.

3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Covered Functions—Those functions of a covered entity that make the entity a health plan, health care provider or health care clearinghouse.

Data Aggregation—The combining of PHI that it is created or received by the business associate to permit data analyses that relate to the health care operations of the respective covered entities.

Data Sharing and Use Agreement—An agreement that serves as a contract between your organization and an organization or individual who creates, uses or discloses PHI, but is not a Business Associate.

Data Use Agreement—An Agreement that serves as a contract between your organization and the organization or individual who wants to use a limited data set for research, public health or health care operations. The Data Use Agreement is meant to provide a reasonable assurance that the organization obtaining the limited data set will not violate the use and disclosure terms of the agreement. A Data Use Agreement must:

1) ensure that agents and subcontractors of the Business Associate also agree to the same restrictions and requirements.

2) establish the permitted and required uses and disclosures.

3) establish who is permitted to use or receive the limited data set.

4) not identify client contact information.

5) require appropriate safeguards to protect other uses and disclosures not allowed by the agreement.

6) require reports to the covered entity of any inappropriate use or disclosure.

7) require that the recipient not use or further disclose the information, other than as permitted by the agreement or required by law.

Designated Record Set—

1) A group of records maintained by or for a covered entity that are the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or records used, in whole or in part, by or for the covered entity to make decisions about individuals.

2) Any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Disclosure—The release, transfer, provision of access to, or divulging in any other manner, information outside the entity holding the information.

Electronic Media—Is:

1) electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

2) transmission media used to exchange information already in electronic storage media.

Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, via facsimile, and voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic Protected Health Information (ePHI)—Information that is transmitted and maintained on electronic media and fits the definition of protected health information.

Employer—Defined as in 26 U.S.C. 3401(d): a person (or an entity) for whom an individual performs or performed any service, of any nature, as the employee of that person (or that entity) except for the following:

1) If the entity for whom the individual performs or performed the services does not have control of the payment of the wages for the services, the term ''employer'' means the entity having control of the payment of the wages.

2) If the entity pays wages on behalf of a nonresident alien individual, foreign partnership, or foreign corporation, not engaged in trade or business within the United States, the term ''employer'' means that entity.

Encryption—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.

1) Ensure that agents and subcontractors of the Business Associate also agree to the same restrictions and requirements.

2) Establish the permitted and required uses and disclosures.

3) Establish who is permitted to use or receive the limited data set.

Facility—The physical premises and the interior and exterior of a building(s).

Group Health Plan—An employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as

medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that has 50 or more participants and is administered by an entity other than the employer that established and maintains the plan.

Health Care—Care, services, or supplies related to the health of an individual. Health Care includes, but is not limited to, the following: preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, and counseling, service, assessment or procedure with respect to the physical or mental condition, or functional status of an individual that affects the structure or function of the body; also, the sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Health Care Clearinghouse—A public or private entity (including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches) that does either of the following functions:

1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or

2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Component—A component or combination of components of a hybrid entity, as designated by the hybrid entity in accordance with the following:

1) Components of a covered entity that perform covered functions are part of the health care component. 2) Another component of the covered entity is part of the entity's health care component to the extent that:

a) it performs, with respect to a component that performs covered functions, activities that would make such other component a business associate of the component that performs covered functions if the two components were separate legal entities; and

b) the activities involve the use or disclosure of protected health information that such other component creates or receives from or on behalf of the component that performs covered functions.

Health Care Operations—Any of the following activities of the covered entity to the extent that the activities are related to covered functions

1) 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 clients with information about treatment alternatives; and related functions that do not include treatment.

2) reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider 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 of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

3) 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).

4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

5) 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

6) business management and general administrative activities of the entity, including, but not limited to management activities relating to implementation of and compliance with the requirements of this subchapter, customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer, resolution of internal grievances, 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 consistent with the applicable requirements of 45 C.F.R. §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health Care Provider—A provider of services (including medical or health care providers) and any other person or organization that furnishes, bills or is paid for health care in the normal course of business.

Health Information—Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and 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.

Health Insurance Issuer—As used in the definition of health plan (see definition below) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance. This term does not include a group health plan.

Health Maintenance Organization (HMO)—A federally qualified HMO, an organization recognized as an HMO under state law, or a similar organization regulated for solvency under state laws in the same manner and to the same extent as an HMO.

Health Oversight Agency—An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Plan—An individual or group plan that provides or pays the cost of medical care. Health plan includes the following, singly or in combination: a group health plan; a health insurance issuer; an HMO; Part A or Part B of the Medicare program (under Title XVIII of the Act), the Medicaid program (under Title XIX of the Act), an issuer of a Medicare supplemental policy, an issuer of a long-term care policy (excluding a nursing home fixed-indemnity policy); an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

Also included is the health care program for active military personnel, the veterans health care program, the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), the Indian Health Service program, the Federal Employees Health Benefits Program, an approved state child health plan (under title XXI of the Act, providing benefits for child health assistance), the Medicare+ Choice program, a high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals, and any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

Health plan excludes any policy, plan or program to the extent that it provides or pays for the cost of excepted benefits. It also excludes a government-funded program (other than those listed above) whose principal purpose is other than providing or paying the cost of health care; or whose principal activity is the direct provision of health care to persons, or the making of grants to fund the direct provision of health care to persons.

HIPAA—The "Health Insurance Portability and Accountability Act of 1996." The original purpose of this Act was to make health insurance more "portable" so that workers could take their health insurance with them when they moved from one job to another, without losing health coverage. The scope of the Act was broadened to require the health care industry to adopt uniform codes and forms. This would help streamline processing and use of health data and claims and contribute to better, more accessible health care for Americans. The Act also was broadened to better protect the privacy of people's health care information, and give them greater access to that information. The HIPAA Privacy Rule was finalized on August 14, 2002. The deadline for complying with the Privacy Rule was April 14, 2003.

Hybrid Entity—A single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, and that designates health care components in accordance with HIPAA regulation 45 C.F.R. §164.105(a)(2)(iii)(C).

Implementation Specification—Any specific requirements or instructions for implementing a standard identified in the HIPAA regulations.

Indirect Treatment Relationship—A relationship between an individual and a health care provider in which:

1) the health care provider delivers health care to the individual based on the orders of another health care provider; and

2) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who then provides the services or products or reports to the individual.

Individual—The person who is the subject of protected health information.

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

1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and

2) 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; and identifies the individual; or

3) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information System—An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Inmate—A person incarcerated in or otherwise confined to a correctional institution.

Integrity—The property that data or information have not been altered or destroyed in an unauthorized manner.

IP Address—The Internet Protocol (IP) address that uniquely identifies a node on an internet, which allows you to send and receive or transmit information using the Internet.

Law Enforcement Official—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, who is empowered by law to:

1) investigate or conduct an official inquiry into a potential violation of law; or

2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set—Protected health information that excludes all of the following direct personal identifiers of the applicant/beneficiary, or of his or her relatives, employers, or household members:

1) names

2) postal address information, other than town or city, state, 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, including license numbers

12) device identifiers and serial numbers

13) web universal resource locators (URLs)

14) Internet Protocol (IP) address numbers

15) biometric identifiers, including finger and voice prints; and

16) full-face photographic images and any comparable images.

Malicious Software—Software (for example, a virus) designed to damage or disrupt a system.

Marketing—

1) To make a communication about a product or service that encourages the purchase or use of the product or service.

2) An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for remuneration for the other entity or its affiliate to make a communication about its own product or service to encourage purchase or use that product or service.

Minimum Necessary—HIPAA requires that when you use or disclose protected health information (PHI), you must follow the "Minimum Necessary Standard." The Minimum Necessary Standard requires that disclosed information be limited to the minimum amount necessary to accomplish the stated purpose. These limitations apply to all paper, fax, verbal and electronic communication or records of PHI.

Modify or Modification—A change to the HIPAA regulations adopted by the Secretary, through regulation, to a new standard or an implementation specification.

More Stringent—In the context of a comparison of a provision of state law and a HIPAA standard, requirement or implementation specification adopted under HIPAA, a state law must meet one or more of the following criteria:

1) The law prohibits or restricts a use or disclosure in circumstances where such use or disclosure otherwise would be permitted under HIPAA, except if the disclosure is required by the Secretary of HHS in connection with determining if a covered entity is in compliance with this subchapter; or to the individual who is the subject of the individually identifiable health information.

2) With respect to the rights of an individual who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

5) With respect to record keeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information. Relates to the privacy of individually identifiable health information means, with respect to a State law,

that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

Notice of Proposed Rule Making (NPRM)—A document that describes and explains regulations that the Federal Government proposes to adopt at some future date, and invites interested parties to submit comments related to them. These comments can then be used in developing a final regulation.

Organized Health Care Arrangement -

1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider

2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities, hold themselves out to the public as participating in a joint arrangement and participate in joint activities that include at least one of the following:

a) utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf.

b) quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

c) payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan.

4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor.

5) The group health plans described in paragraph 4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Password - Confidential authentication information composed of a string of characters.

Payment -

1) The activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

2) The activities in paragraph 1) of this definition relate to the individual to whom health care is provided and include, but are not limited to determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims, risk adjusting amounts due based on enrollee health status and demographic characteristics, billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing, review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges, utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

a) name and address

b) date of birth

c) Social Security number

d) payment history

e) account number; and

f) name and address of the health care provider and/or health plan.

Physical Safeguards—Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Plan Administration Functions—Functions performed by the plan sponsor of a group health plan on behalf of the group health plan, and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Plan Sponsor—An entity that sponsors a health plan. This can be an employer, a union, or some other entity. Plan Sponsor is defined in the Employee Retirement Income Security Act (section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B)).

Protected Health Information (PHI)—Individually identifiable health information that is: transmitted by electronic media, maintained in electronic media, or transmitted or maintained in

any form or medium. Protected health information excludes individually identifiable health information in: education records covered by the Family Educational Rights and Privacy Act; and in employment records held by a covered entity in its role as employer.

Psychotherapy Notes—Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a counseling session that are separated from the rest of the individual's medical record. (Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date).

Public Health Authority—An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors, or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by Law—A mandate contained in law that compels a covered entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research—A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary—The Secretary of Health and Human Services, or any other officer or employee of HHS, to whom the authority involved has been delegated.

Security (or Security Measures)—Encompasses all of the administrative, physical, and technical safeguards in an information system.

Security Incident—The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

Social Security Number (SSN)—The number of a particular individual's Social Security account.

Standard—A rule, condition, or requirement describing the following information for products, systems, services or practices for classification of components, specification of materials, performance, or operations, or delineation of procedures with respect to the privacy of PHI.

Standard Setting Organization (SSO)—An organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, the HIPAA regulation.

State—One of the following:

1) for a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan; or

2) for all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

State Law—A constitution, statute, regulation, rule, common law or other State action having the force and effect of law.

Summary Health Information—Information that may be individually identifiable health information and:

1) that summarizes the claims history, claims expenses or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

2) from which the information described at 45 C.F.R. §164.514(b)(2)(i) has been deleted, except that the geographic information described in 45 C.F.R. §164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code

Technical Safeguards—The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

TPO—Treatment, Payment, and Operations. HIPAA allows the office to do routine things with PHI with no special permission from the client. These routine things are summarized as TPO.

See the definitions for each of these three items in this Glossary. In brief: Treatment includes all the things that are part of the client's medical care; Payment includes all the activities related to paying for a person's health care; Operations include all the activities done to operate a health agency.

Treatment—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 a client; or the referral of a client for health care from one health care provider to another.
Universal Billing Form, 1992 Revision (UB-92)—The National Uniform Billing Committee (NUBC) standard billing form for institutional claim billing.

Use—The sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information

User—A person or entity with authorized access.

Staff—Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation—An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.