HILLSBOROUGH COUNTY

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

POLICIES

Effective: July 1, 2017

Revised: September 11, 2020

Table of Contents

Section 1 – Statement of Commitment to Compliance

PURPOSE

This policy articulates Hillsborough County's commitment to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Regulations for use and disclosure of Protected Health Information (PHI). PHI is any written, spoken, or electronic information that contains an individual's identity and his or her health information.

POLICY

Hillsborough County and its subsequent covered entity departments are committed to complying with the requirements of the HIPAA Privacy and Security Regulations, as outlined in 45 C.F.R. §§ 164.103, 164.105, when using, maintaining or disclosing protected health information (PHI).

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

PURPOSE

This policy states general policies and procedures to guide the use and disclosure of PHI by Hillsborough County.

POLICY

Hillsborough County has established the general guidelines set forth in this policy to guide its staff in complying with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Regulations, as outlined in 45 C.F.R. §§ 164.103, 164.105.

Section 3 – Uses and Disclosures

Subject: 3.01 - Verification of Identity and Authority

PURPOSE

This policy describes when staff members must verify the identity and authority of persons to whom they disclose Protected Health Information (PHI).

POLICY

Except for disclosures under Policy 3.03, prior to any disclosure of PHI by the Covered Entity Department, the Department Liaison(s) will:

- Verify the identity of the person requesting PHI and the authority of that person to have access to PHI (see #3 and #4 of this policy), if the identity or authority of that person is unknown to the Privacy Liaison(s); and

- Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when any policy in these HIPAA Procedures requires documentation, or a statement or representation as a condition of the disclosure.

With respect to disclosing PHI, the Department Liaison(s) may rely on documentation, statements, or representations that meet the applicable requirements in the following circumstances:

- For an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand or similar process authorized under law, the condition may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

- For research purposes, the documentation of the approval by a privacy board of an alteration or waiver of an individual authorization may be satisfied by one or more written statements, provided that each statement is appropriately dated and signed in accordance with HIPAA Privacy Regulation requirements.

The Department Liaison(s) may rely, if such reliance is reasonable under the circumstances, on any one of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

- If the request is made in person, presentations of agency identification badge, other official credentials, or other proof of government status;

- If the request is in writing, the request is on the appropriate government letterhead; or

- If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding or purchase order, that establishes that the person is acting on behalf of the public official.

The Department Liaison(s) may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

- A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

- If a request is made pursuant to a legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

The verification requirements of this Policy are met for disclosures under Policy 3.03 when the Department Liaison(s) relies on the exercise of professional judgment, as and when permitted by Policy 3.03, to make disclosures of PHI as permitted by Policy 3.03.

The verification requirements of this Policy are met for disclosures under Policy 3.17 when the Department Liaison(s) acts on a good faith belief, as and when permitted under Policy 3.17, to make disclosures of PHI as permitted by Policy 3.17.

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

PURPOSE

This policy describes certain limited circumstances in which staff members may use or disclose PHI for non-TPO (treatment, payment, and other administrative operations) purposes without obtaining a written authorization provided that the client is given an opportunity to agree or object to the disclosure of the PHI or the persons to whom PHI is disclosed.

POLICY

A department may use the PHI for non-TPO purposes without a written authorization in the following limited circumstances, provided that the client is informed in advance of the use or disclosure and is given the opportunity to agree to, or prohibit, or restrict the use or disclosure and the client does not object to the disclosure:

- In-home Services and Facility Based Services Units (sections) may maintain a facility directory of clients receiving services for disclosure to members of the clergy or other persons who ask for the client by name.

- A department's staff members may disclose PHI to a family member, close personal friend, or other person identified by the client as being involved in the client's care or payment for care.

Subject: 3.03 No Restrictions (Authorization or Opportunity to Agree or Object Is Not Required)

PURPOSE

This policy describes when Staff Members may use Protected Health Information (PHI) without (i) the client's written authorization or (ii) giving the client the opportunity to agree to, prohibit or restrict the use or disclosure of PHI.

The policy also describes when Staff Members may tell individuals about uses and disclosures and needs only oral authorization to use or disclose the PHI.

Subject: 3.04 Personal Representatives

PURPOSE

This policy is designed to address the uses and disclosures of Protected Health Information (PHI) to a client's personal representative.

POLICY

Staff Members will treat a personal representative the same as the individual he or she represents in the following situations:

- If under applicable law a person has the authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat this person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

- If under applicable law a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

    - The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

    - The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or

    - A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

- Notwithstanding the provisions above:

    - If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with 45 C.F.R. §164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

    - If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance

with the Privacy Rule to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and

- Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under this policy and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under the Privacy Rule to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

- If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

- Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:

  - The covered entity has a reasonable belief that:

    - The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

    - Treating such person as the personal representative could endanger the individual; and

  - The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

Subject: 3.05 Minimum Necessary

PURPOSE

The purpose of this policy is to describe the protocols staff members will implement to satisfy the minimum necessary standard for the use and disclosures of Protected Health Information (PHI) on both a routine and non-routine basis.

POLICY

Staff members' access to PHI shall be limited to the specific types of PHI actually needed by those staff members in order for them to carry out their service unit (sections) responsibilities.

When requesting PHI, staff members must limit access and disclosure of PHI to that which is reasonably necessary to accomplish the purpose for which the request is made.

When disclosing PHI in response to requests that are made on a routine and recurring basis, staff members must limit disclosure of PHI to that which is reasonably necessary to accomplish the purpose for which the request is being made.

Requests for disclosure of PHI that are not of a routine and recurring nature must be forwarded immediately by the staff member to his or her supervisor, who will in turn forward the request to the Department Liaison(s), who will make the determination as to the "minimum necessary" to be disclosed. Any staff member without the written authorization of the Department Liaison(s) may not make disclosures of PHI under this Paragraph.

All requests for PHI to be disclosed for purposes of research shall be treated as non-routine and non-recurring.

If applicable, requests to disclose "minimum necessary" PHI must be accompanied by safeguarding agreements with recipients of the PHI.

Releases of PHI under this Policy that must be logged into and tracked with the County's HIPAA tracking system include:

- Disclosure for Abuse, Neglect and Domestic Violence
- Disclosure about a decedent
- Disclosure to another Health Care Provider that is not for treatment
- Disclosure to Law Enforcement
- Disclosure for Legal or Judicial orders
- Disclosure for Oversight and Regulatory
- Disclousre to a Payer that is not for payment
- Disclosure for Research

- Exceptions to the minimum necessary policy include disclosure that are:
  - Made by a health care provider for treatment purposes
  - Made by the individual who is the subject of the PHI
  - Made pursuant to a valid authorization
  - Required by law
  - Required by the Secretary of the U.S. Health and Human Services

Subject: 3.06 De-Identified

PURPOSE

This policy explains how and when protected health information (PHI) is to be de-identified, that PHI has been removed from the individual records, whenever possible.

POLICY

Staff members will use de-identified information in disclosures, when possible. If PHI is de-identified, it is no longer considered PHI and therefore is not subject to the provisions of the HIPAA privacy regulation regarding PHI.

Staff members may only use the two methods of de-identification described in the procedure and release de-identified PHI if the identifiers listed in the procedure are removed before disclosure is made.

Subject: 3.07 Uses and Disclosures Required by Law

PURPOSE

This policy explains how staff members may use and disclose protected health information (PHI) to the extent and as required by law for which an authorization or opportunity to agree or object is not required.

POLICY

Staff member shall use and disclose PHI to the extent and as required by law and when the use and disclosure complies with, and is limited to, the relevant requirements of the law and for which an authorization or opportunity to agree or object is not required.

Staff member shall meet the requirements described in the sections listed below, for the uses or disclosures required by law:

- Uses and Disclosures of Information Related to Victim of Crime, Abuse or Domestic Violence - Policy 3.09
- Uses and Disclosures for Law Enforcment Purposes - Policy 3.10
- Disclosures for Judicial and Administrative Proceedings - Policy 3.11

Where a specific policy is referred above, staff members shall consult that policy for specific rules applicable to the particular type of disclosure requested.

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

PURPOSE

This policy describes the instances when staff members may disclose protected health information (PHI) for public health activities without obtaining an authorization and without providing the client with the opportunity to agree or object.

POLICY

Staff member may disclose PHI for public health activities in the five instances listed below without obtaining an authorization or without providing the client with the opportunity to agree or object.

- To a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.

- To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

- To those subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include.

    - To collect or report adverse events (or similar activities with respect to food or dietary supplements), products defects or problems (including problems with the use or labeling of a product), or biological product deviations.

    - To track FDA-related products.

    - To enable product recalls, repairs, or replacement, or look back (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of look back); or

    - To conduct post market surveillance.

    - To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if staff member or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

    - An employer, about an individual who is a staff member of the employer, if:

- The Department is a covered health care provider who is a member of the staff of such employer or who provides health care to the individual at the request of the employer:

  A. To conduct an evaluation relating to medical surveillance of the workplace; or

  B. To evaluate whether the individual has a work-related illness or injury; or

- The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance; and

- Staff member needs such findings in order to comply with its obligations, under federal or state law, to record illness or injury or to carry out responsibilities for workplace medical surveillance; and

- The health care provider within Hillsborough County provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to Hillsborough County;

  A. By giving a copy of the notice to the individual at the time the health care is provided; or

  B. If the health care is provided on a Hillsborough County work site, by posting the notice in a prominent place at the location where the health care is provided.

  C. If a health care provider within Hillsborough County discloses work-related illnesses and injuries to an employer or performs medical surveillance of the workplace, it shall provide written notice of the disclosure to the client.

- Staff member is also permitted to use or disclose a limited data set (protected health information from which direct identifiers, such as name and social security number have been removed) for public health purposes. For example, staff member may disclose a limited data set to a private disease registry for a public health purpose without the individual's authorization. In contrast, the disclosure of fully identifiable PHI to such a registry would require authorization.

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

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

PURPOSE

This policy addresses when protected health information (PHI) may be disclosed about an individual, other than a child, whom the staff member reasonably believes to be a victim of abuse, neglect, domestic violence, or exploitation without obtaining an authorization or providing the individual with the opportunity to agree or object. Disclosures in connection with child abuse are covered under the Policy for Disclosures Relating to Health Activities.

POLICY

Staff members shall comply with the mandatory reporting requirement of abuse, neglect, or exploitation of vulnerable adults and the mandatory reports of deaths and may release PHI in connection with such reporting provided that the PHI released is limited.

To the extent authorized by law a staff member may disclose PHI about an individual when the staff member reasonably believes in his or her professional judgment that the disclosure is necessary to prevent serious harm to the victim of abuse, neglect, or domestic violence. This disclosure shall be made only to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, domestic violence, or exploitation and requires that:

- The individual agrees to the disclosure; or
- If the individual cannot agree because incapacitated, a law enforcement or other public official authorized to receive the report represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
- If a disclosure is made pursuant to this policy, the individual about whom the disclosure is made must be informed promptly that the disclosure has been or will be made unless:
    - The staff member, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
    - The staff member would be informing a personal representative, and the staff member reasonably believes the personal representative is responsible for the abuse, neglect, or other injury and that informing such person would not be in the best interest of the individual, as determined by the professional judgment of staff member, Department Manager, or Director.
- An entry shall be made into the County's HIPAA Tracking System for each disclosure made under this policy.

Subject: 3.10 Law Enforcement Purposes

PURPOSE

This policy describes the circumstances when protected health information (PHI) may be disclosed for law enforcement purposes without an authorization or opportunity to agree or object and the procedures, which will be followed by staff member in making such disclosures.

POLICY

Staff members may disclose PHI for law enforcement purposes to a law enforcement official without an authorization or opportunity to agree or object in the following circumstances subject to the limitations on disclosure given in the Procedures section below.

As required by law as described below, including when laws require the reporting of certain types of wounds or other physical injuries. (This does not apply to a governmental authority authorized by law to receive reports of child abuse and neglect or the disclosure of protected health information to a government authority about an individual who is the victim of abuse, neglect or domestic violence.).

- In compliance with and limited to the relevant requirements of:
    - A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
    - A grand jury subpoena;
    - An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law provided that:
        - The information that is sought is relevant and material to a legitimate law enforcement inquiry.
        - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
        - De-identified information could not reasonably be used.
- In response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person provided that the disclosure of PHI is limited to the following:
    - Name and address

- Date and place of birth
- Social Security Number
- ABO blood type and Rh factor
- Type of injury
- Date and time of treatment
- Date and time of death, if applicable; an
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or mustache), scars and tattoos.

The staff member may disclose to law enforcement official, PHI about an individual who has died for the purpose of alerting law enforcement of the death of the individual if the staff member has suspicion that such death may have resulted from criminal conduct.

Staff member may disclose PHI in response to law enforcement official's request for such information about an individual who is, or is suspected to be, a victim of a crime, other than disclosures that are specifically governed by other sections of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Regulation, if:

- The individual agrees to the disclosure; or if staff member is not able to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:
  - The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim.
  - The law enforcement official represents that immediate law enforcement activity depends upon the disclosure and would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
  - The disclosure is in the best interest of the individual as determined by the staff member, in the exercise of his or her professional judgment.

The staff member may disclose to a law enforcement official PHI that the staff member believes in good faith constitutes evidence of criminal conduct that occurred on the premises occupied by the service unit (section).

Except as provided below, a staff member providing emergency health care in response to a medical emergency, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

- The commission and nature of a crime.
- The location of such crime or of the victim(s) of such crime.
- The identity, description and location of the perpetrator of such crime.

If a staff member believes that the medical emergency described is the result of abuse, neglect or domestic violence of the individual in need of emergency treatment, the requirements to disclosure shall not apply and the staff member shall follow the County's policy on Uses and Disclosures for Victims of Abuse, Neglect, or Domestic Violence.

Subject: 3.11 Judicial or Administrative Proceedings Purposes

PURPOSE

This policy explains when protected health information (PHI) may be disclosed by staff members for judicial or administrative proceedings purposes without obtaining an authorization or without providing the client with an opportunity to agree or object.

POLICY

Staff members may disclose PHI in the course of any judicial or administrative proceeding without obtaining an authorization, or without providing the client with an opportunity to agree or object, if the disclosure is in response to an order of a court or administrative tribunal, provided that staff members discloses only the PHI expressly authorized by such order.

Staff members may disclose PHI in the course of any judicial or administrative proceeding without obtaining an authorization, or without providing the client with an opportunity to agree or object, if the disclosure is in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, provided that the conditions in subparagraphs below are met:

- Staff members receives satisfactory assurance from the party requesting the PHI that reasonable efforts have been made by that party to ensure that the individual who is the subject of the PHI has been given notice of the request. Satisfactory assurance means here that staff members has received a written statement and documents from the individual seeking the PHI that show:
    - The party requesting the PHI has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
    - The notice included sufficient information about the litigation or proceeding in which the PHI is being requested, to permit the individual to raise an objection to the court or administrative tribunal; and
    - The time for the individual to object to the court or administrative tribunal has passed, and
        - No objections were filed; or
        - The court or administrative tribunal has resolved all objections filed by the individual and the disclosures being requested are consistent with the resolution of the court or administrative tribunal.
- Staff member receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by that party to secure a qualified protective order.

- For purposes of this sub-paragraph, qualified protective order means an order of a court or administrative tribunal or a stipulation by the persons involved in the legal matter or administrative proceeding that

  - prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and

  - requires the PHI (including all copies made) be returned to staff member or destroyed at the end of the litigation or proceeding

  - for purposes of this subparagraph, satisfactory assurance means that staff member receives a written statement and accompanying documentation showing that:

    A. The parties involved in the legal action have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

    B. The party requesting the PHI has requested a qualified protective order from such court or administrative tribunal.

An entry shall be made into the County's HIPAA Tracking System for each request for disclosure of PHI received and each disclosure of PHI made by staff member for judicial or administrative proceedings purposes.

The provisions of this policy regarding the disclosures of PHI for judicial and administrative proceedings purposes do not supersede other provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy regulation that otherwise permit or restrict uses or disclosures of PHI.

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

PURPOSE

This policy establishes staff member rules regarding disclosures of protected health information (PHI) relating to deceased persons.

POLICY

In the event a staff member finds a client deceased, the staff member shall immediately call 911. The staff member shall then promptly notify his of Department Manager or designee of the death. Upon arrival of a law enforcement officer at the scene, the staff member may disclose the client's name and contact information to the law enforcement officer if requested to do so. Law enforcement personnel shall make contact of next of kin. It is not the staff member's responsibility to communicate with the medical examiner, coroner, or funeral director, unless specifically directed to do so by his or her Department Manager or designee after approval by the Department Liaison(s).

Staff member may disclose to a law enforcement official PHI that staff member believes in good faith constitutes evidence of criminal conduct that occurred on the premises of a County Facility.

Staff member may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

Staff member may disclose PHI to a funeral director, consistent with applicable law, as necessary to carry out his or her duties with respect to the decedent. If necessary for the funeral director to carry out his or duties, staff member may disclose PHI prior to, and in reasonable anticipation of, the individuals death.

Staff member may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

All requests for disclosure and all disclosures of PHI pursuant to this Policy shall be entered into the County's HIPAA tracking system.

Subject: 3.13 Uses and Disclosures – Research

PURPOSE

This policy explains when protected health information (PHI) may be used or disclosed for research purposes.

POLICY

Staff member may use or disclose PHI for research purposes, regardless of the source of funding, provided that the request for PHI for research purposes has been reviewed and the use or disclosure authorized by the HIPAA Privacy Officer.

All uses and disclosures approved by the HIPAA Privacy Officer for research purposes must adhere to applicable Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations, state law and other laws.

Where applicable, staff member may use limited data sets for disclosure of PHI for research purposes. See Policy 7.02 and Policy 7.03.

Subject: 3.14 Uses and Disclosures – Avert a Serious Threat

PURPOSE

This policy describes the three circumstances when protected health information (PHI) can be used and disclosed without an authorization or opportunity to agree or object to avert a serious threat to health or safety.

POLICY

Subject to the limitation in the last paragraph of the Procedure Section, staff members may use and disclose PHI without an authorization or opportunity to agree or object to avert a serious threat to health or safety when the staff member believes, based either on the staff member's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority that:

- The disclosure will prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the use or disclosure is to a person or persons reasonably able to prevent the threat, including the target of the threat.
- The use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual because of a statement an individual makes admitting to participating in a violent crime and staff member reasonably believes the individual may have caused serious physical harm to the victim. In this circumstance, a use or disclosure may not be made if the information is learned:
    - in the course of treatment, counseling or therapy of the individual for the tendency to commit the criminal conduct that is the basis for the disclosure to law enforcement authorities; or
    - through a request by the individual to initiate or to be referred for treatment, counseling or therapy for the tendency to commit the criminal conduct that is the basis for the disclosure to law enforcement authorities.
- Where it appears, given all of the information available, that the individual has escaped from a correctional institution or from lawful custody.

All requests for disclosures and disclosures made under this policy shall be entered into the County's HIPAA tracking system.

Subject: 3.15 Uses and Disclosures – Specialized Government Function

PURPOSE

This policy explains how protected health information (PHI) can be used and disclosed for specialized government functions without obtaining a written authorization or affording the client the opportunity to agree or object.

POLICY

Staff member may use or disclose PHI for the following specialized government functions without a obtaining a written authorization or affording the client the opportunity to agree or object:

- Military and veterans activities.
- National security and intelligence activities.
- Protective services for the President and others.
- Medical suitability determinations.
- Correctional Institutions and other law enforcement custodial situations.
- Government programs providing public benefits (with the exception of enrollment for clients to the Medicaid Waiver Program).

An entry shall be made into the County's HIPAA tracking System for each use, request for disclosure and disclosure of PHI for all Specialized Government Functions.

Enrollment of clients into the Medicaid Waiver Program shall not require referral to, the review by or approval of the Privacy Liaison(s) as described below. Enrollment of clients into the Medicaid Waiver Program shall be completed by utilizing the service unit (section)'s enrollment packet and following the enrollment procedures established by the service unit (section).

Subject: 3.16 Workers' Compensation

PURPOSE

This policy describes when protected health information (PHI) may be disclosed for purposes of workers compensation without obtaining an authorization or providing the client with the opportunity to agree or object.

POLICY

Staff member may disclose PHI to as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law that provide benefits for work-related injuries or illness without regard to fault without obtaining a written authorization or without providing the client with the opportunity to agree or object.

An entry shall be made into the County's HIPAA tracking System for each disclosure request and disclosure made under this policy.

Subject: 3.17 Uses and Disclosures for Health Oversight Activities

PURPOSE

This policy describes the instances when staff member may disclose protected health information (PHI) for health oversight activities without obtaining an authorization and without providing the client with the opportunity to agree or object.

POLICY

Staff member may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

- The health care system.
- Government benefit programs for which health information is relevant to beneficiary eligibility.
- Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- Entities subject to civil rights laws for which health information is necessary for determining compliance.

Staff member's exception to disclosures permitted by policy 1, above, is that health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

- The receipt of health care.
- A claim for public benefits related to health; or
- Qualification for, or receipt of, public benefits or services when a client's health is integral to the claim for public benefits or services.

Staff member considers the joint activity or investigation a health oversight activity for the purposes of this policy when a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health.

If the department is a health oversight agency, it may use protected health information for health oversight activities as permitted by this policy.

Section 4 - Authorizations

Subject 4.01 – Authorization Requirements

PURPOSE

This policy addresses when an authorization is required for the use or disclosure of protected health information (PHI) and the exceptions to that requirement.

POLICY

A written authorization will be required to use or disclose PHI, unless the disclosure is for treatment, payment, and other administrative operations (TPO) or an exception to the authorization requirement is provided elsewhere in this Policy Manual.

Any use or disclosure of PHI pursuant to an authorization must be consistent with the authorization.

Authorizations are not required in emergency situations, but staff members must immediately inform their Section Managers or their designees of the emergency situation.

Specific authorization rules for psychotherapy notes.

An authorization is required for any use or disclosure of psychotherapy notes, except to carry out the following:

- Treatment, payment, or health care operations as described herein.
- Use by the originator of the psychotherapy notes for treatment.
- Use or disclosure by provider for its own training programs in which supervised students, trainees, or practitioners in mental health learn to practice or improve their skills in group, joint, family, or individual counseling.
- Use or disclosure by staff member to defend itself in a legal action or other proceeding brought by the individual; or
- A use or disclosure that is required by policy with respect to the oversight of the originator of psychotherapy notes.

Specific authorization rules for using or disclosing PHI for marketing purposes.

Staff member must obtain a written authorization for any use or disclosure of PHI for marketing, except if the communication is made in the form of a face-to-face communication by staff member to an individual or in the form of a promotional gift of nominal value provided by staff member to the individual.

When obtaining authorization, staff members must use the most recent Authorization Form approved by the department and the HIPAA Officer. This form will encompass the requirements for a valid authorization set forth in 45 C.F.R. § 164.508 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Regulation, as such may be amended from time to time.

Authorizations may not be combined with any other document to create a compound authorization, except as permitted by the HIPAA Regulation and as approved by the HIPAA Officer.

An individual may revoke an authorization at any time, provided that the revocation is in writing, except when staff member has taken action because of the authorization

Staff member shall not condition the availability of service to an individual based on receiving an authorization except in the following limited circumstances:

- Non-case management units or services may condition the availability of research - related treatment on the ability to obtain an authorization for the use or disclosure of PHI for such research.

- Staff member may condition enrollment in its programs or eligibility for benefits on provision of an authorization requested by it prior to the individual's enrollment in its programs, if the authorization is not for the use or disclosure of psychotherapy notes; and

- Staff member may condition the availability of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization or the disclosure of the PHI to such third party.

All requests for disclosures, including the identification of the individual receiving the PHI (even though an authorization was obtained) and all disclosures of the PHI, and the purpose and conditions for release of the PHI, which are made pursuant to this policy must be entered into the County's HIPAA tracking system.

Section 5 – Notice of Privacy Practices

Subject 5.01 – Notice of Privacy Practices

PURPOSE

This Policy describes the policy and procedures, which shall be followed by staff member with regard to the distribution of the Notice of Privacy Practices, the distribution of renewal Notice of Privacy Practices or revised Notice of Privacy Practices to clients, and to the posting of the Notice of Privacy Practices in all County facilities and locations.

POLICY

It is the policy of Hillsborough County that clients shall have the right to notice of:

- The uses and disclosures of protected health information (PHI) that may be made by staff member and its Business Associates, and
- The clients' rights and duties with respect to PHI.

Section 6 – Contracts

Subject 6.01 – Contracts: Business Associate Agreements

PURPOSE

The County may contract with third parties to perform work or provide services on its behalf. These contracts may create business associate relationships when they perform functions on behalf of the County. The purpose of this policy is to discuss the ways the County may use Business Associate Agreements.

POLICY

When the County enters into contracts and agreements with business associates, the contract must state the requirement for compliance with the County policies. Alternatively, the County may enter into a separate Business Associate Agreement with a third party which sets forth the requirement for compliance with the County policies.

Contracts containing compliance language and Business Associate Agreements will be reviewed for compliance at regular intervals.

Associates; 45 C.F.R. § 164.504(e) Business associate contracts.

Subject 6.02 – Limited Data Set Agreements

PURPOSE

This policy establishes the uses and disclosures for limited data sets that are prepared in connection with disclosures to a business associate. A limited data set is a record about an individual that has certain information removed.

POLICY

Staff members may use or disclose protected health information (PHI) in a limited data set, if staff member obtains satisfactory assurance, in the form of a Data Use Agreement signed by the County's business associate receiving the limited data set.

The County's staff members are not permitted to use or disclose a limited data set to a Business Associate without first having a Data Use Agreement in place.

The Data Use Agreement between the County and the business associate must establish the permitted uses and disclosures of such information for the purpose of research, public health, or health care operations. The Data Set Agreement must contain the following:

- Establish who is permitted to use or receive the limited data set; and
- Provide that the limited data set recipient will:
  - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law.
  - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement.
  - Report to staff member any use or disclosure of the information not provided for by its data use agreement of which it become aware.
  - Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
  - Not identify the information or contact the individuals.

Subject 6.03 – Limited Data Set Specifications

PURPOSE

This policy defines the information that must be removed from an individual record before that record can be shared or exchanged.

POLICY

Staff members must create limited data sets by removing identifiable information prior to sharing or exchanging protected health information (PHI) with a Business Associate.

A limited data set is PHI that has any of the following information removed, as well as any other information that links the record to an individual's health information. This includes naming relatives, employers or household members of the individual. Limited data sets require the removal of:

- Names.
- Postal address information, other than town or city, State, and zip code.
- 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 voiceprints.
- Full face photographic images and any comparable images.

Section 7 – Individual Rights

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

PURPOSE

This policy explains when an individual has a right of access to inspect and obtain a copy of his or her protected health information (PHI).

POLICY

It is the policy of the County to afford individuals the right to access to inspect and obtain a copy of their PHI in a designated record set, pursuant to a written request, and subject to the conditions in this Policy, for as long as the PHI is maintained in the designated record set. Exceptions to this right include the following:

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

As used in this policy "designated record set" means a group of records maintained by a Department that is:

- 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.
- Used in whole or in part by a department to make decisions about individuals.

Individual access may be denied in whole or in part, without providing an opportunity for review in the following circumstances:

- The PHI is one of the exceptions listed in Paragraph 1 above.
- The provider of the PHI is functioning as a correctional institution or a covered health care provider acting under the direction of the correctional institution, and the inmate's request to obtain a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee or other person at the correctional institution, or individuals responsible for transporting the inmate.
- An individual's access to PHI created or obtained by the County or its Business Associates in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress; provided that the individual agreed to the denial of access when

consenting to participate in the research that includes treatment and the staff member has informed the individual that the right of access must be reinstated upon completion of the research.

- The requested information is contained in records that are subject to the Privacy Act, 5 U. S. C. Section 552a, if the denial meets the requirements of that law.

- If the PHI was obtained from someone other than the Hillsborough County under a promise of confidentiality and the access requested would reasonably reveal the source of the information.

Individuals denied access to their PHI have the right to have the denial reviewed unless:

- Licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

- The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person;

- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

An entry shall be made into the County's HIPAA tracking system for each request for PHI received. In addition, a follow-up entry must be made into the tracking system for resolution of the request and/or if disclosure or is made. It should also be noted if any denials for disclosure are made.

Staff members will also document and retain the following:

- The designated record sets that are subject to access by individuals.

- The title of the persons or offices responsible for receiving and processing requests for access by individuals.

The County will notify all clients that any requests for access for PHI under this policy are to be made in writing. This notification may be provided by staff member in a variety of ways, including but not limited to inclusion in the Notice of Privacy Practices provided by the County and its Business Associates to clients.

Subject 7.02 – Amendment of Protected Health Information (PHI)

PURPOSE

This policy explains that an individual has a right to amend their protected health information (PHI).

POLICY

- Staff member will permit individuals the right to request an amendment of their PHI.
- All requests for amendments must be made in writing and submitted to the HIPAA Department Liaison(s).
- Staff member may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request:
    - was not created by the individual unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
    - is not part of the designated record set;
    - would not be available for inspection under 45 C.F.R. § 164.524 of the HIPAA Privacy Regulation; or
    - is accurate or complete.

An individual will have the right to request to amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

If staff member is informed by another covered entity of an amendment to an individual's PHI, it will amend the PHI in the designated record sets.

Staff member will document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by Section 164.530(j) of the HIPAA Privacy Regulation.

Subject 7.03 – Individual Right to File a Complaint

PURPOSE

This policy specifies the manner for complaints.

POLICY

It is the policy of Hillsborough County to protect the right of individuals to file a complaint when it is believed that requirements for privacy compliance are not being met.

Hillsborough County shall cooperate with any review or investigation by the Secretary of Health and Human Services or any individual or office designated to respond to complaints.

Subject 7.04 – Alternate or Confidential Communication

PURPOSE

This policy explains how staff member will accommodate reasonable requests by individuals to receive communications of protected health information (PHI) from the Department by alternative means or at alternative locations.

POLICY

It is the policy of Hillsborough County to permit individuals to request alternate methods of communication of their PHI and to accommodate those requests. Such alternate methods may include, but not be restricted to alternate mailing addresses, phone numbers, or fax numbers.

Hillsborough County will accommodate a reasonable request by an individual to receive communications of PHI by alternative means or at alternative locations, if the individual clearly states that the disclosure of part, or all of the PHI could endanger the individual.

Hillsborough County may condition the provision of a reasonable accommodation on:

- When appropriate, information as to how payment, if any, will be handled; and
- Specification of an alternative address or other method of contact.

Subject 7.05 – Notification of Release (Accounting of Disclosures)

PURPOSE

This policy describes the requirements for Individual Notification of Release or Accounting of Disclosures of Protected Health Information (PHI).

POLICY

It is the policy of Hillsborough County that an individual has the right to an accounting of disclosures of PHI made by Hillsborough County in the six years prior to the date on which the accounting is requested, except for disclosures:

- to carry out treatment, payment, and other administrative operations (TPO) as provided in this Policy Manual;
- to individuals of PHI about them, as provided in 45 C.F.R. § 164.502 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Regulation;
- Incident to a use or disclosure otherwise permitted or required, as provided in 45 C.F.R. §164.502 of the HIPAA Privacy Regulation;
- pursuant to an authorization as provided in 45 C.F.R. § 164.502 of the HIPAA Privacy Regulation;
- for the directory of a department facility or to persons involved in the individual's care or other notification purposes as provided in 45 C.F.R. § 164.510 of the HIPAA Privacy Regulation;
- for national security or intelligence purposes as provided in 45 C.F.R. § 164.512(k)(2) of the HIPAA Privacy Regulation;
- to correctional institutions or law enforcement officials as provided in 45 C.F.R. § 164.512(k)(5) of the HIPAA Privacy Regulation;
- as part of a limited data set in accordance with 45 C.F.R. § 164.514(e) of the HIPAA Privacy Regulation; or
- that occurred prior to April 14, 2003.

The accounting of disclosure required by this policy shall provide the individual with the information described in the Procedures, as applicable.

Hillsborough County must provide the first accounting to an individual in any 12-month period without charge. Hillsborough County may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that Hillsborough County informs the individual in advance of the fee and provides the

individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Hillsborough County will temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official as provided in 45 C.F.R. §164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

Hillsborough County will document the following:

- the documentation as required by 45 C.F.R. § 164.530(j) of the HIPAA Privacy Regulation;
- the written accounting that is provided to an individual pursuant to this policy; and
- the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Section 8 – Safeguard Requirements

Subject 8.01 – Liaison Security Responsibilities

PURPOSE

This policy describes the Department's responsibility to identify a primary and secondary Department HIPAA liaison(s) and further describes the Department HIPAA liaison(s)'s responsibilities.

POLICY

The Department Director/Manager shall appoint a primary and secondary Department HIPAA liaison(s) to represent and act on behalf of the Department for issues and standards relating to HIPAA and Hillsborough County. The Department HIPAA liaison(s) shall provide guidance in establishing, implementing, and monitoring the basic elements of electronic and physical security. The Department HIPAA liaison(s) shall ensure the Department adheres to Hillsborough County's Security Policies, security responsibilities, and ensures continued compliance to HIPAA laws and regulations regarding electronic and physical security. Additionally, should the Department liaison(s) become aware of a potential privacy or security concern or a potential breach, the Department liaison(s) should report this to the County Privacy Officer without undue delay, and no more than 48 hours beyond becoming aware of the issue.

Authority: 45 C.F.R. §164.308(a)(2) Assigned security responsibility.

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

PURPOSE

This policy explains the administrative safeguards that are required to protect protected health information (PHI).

POLICY

The Department's staff members shall protect or safeguard personally identifiable health information or PHI from unauthorized disclosure (accidental or willful release of PHI without written approval or legal authority).

The Department's staff members are prohibited from disclosing or sharing of passwords, access codes, key cards, or other user identifiers.

The Department's staff members will access only information needed to do his or her job responsibilities.

The Department's staff members will

- Not destroy original documentation containing PHI. All PHI records must be maintained for six years.
- Not dispose of PHI in the trash container. All unneeded and duplicated PHI records must be properly shredded.

If the Department is a covered entity it must not permit unauthorized disclosure of PHI:

- To any business units that functions as separate or distinct legal entities without written agreements or authorization.
- That it creates or receives in a way that violates this policy.
- To a person who performs duties in both the health care portion of the Department and the non-health care portion for purposes not related to the health care portion of a job. That is, PHI that is authorized for one purpose may not be used for other job functions or purposes without specific authorization.

The Department's staff members must safeguard PHI from intentional and unintentional disclosures. Policies and procedures for safeguards must include the following levels:

- Administrative.
- Technical.

- Physical.

Reasonable safeguard procedures may vary by departments depending on factors such as the nature of the PHI held by the department and the potential risks to the privacy of an individual's PHI in the various departments.

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

PURPOSE

To ensure staff compliance to HIPAA, and IT security issues, and to ensure best practices are in place and in use for access to County controlled information systems; resources; and facilities and such access is not misused by staff members.

POLICY

The Liaison is responsible to periodically review written policies and procedures to reflect appropriate safeguards for access to information and resources by the Department and its staff members.

The Department's staff members must safeguard PHI/confidential information and public record from intentional and unintentional disclosures. Policies and Procedures for safeguards must include the following levels:

- Administrative.
- Technical.
- Physical.

Staff members who fail to comply with established policies and procedures will be subjected to disciplinary action.

The Department HIPAA liaison(s) and the HIPAA Privacy Officer and other designated staff members will work with IT, including the HIPAA Security Officer, for the review of computer hardware/software and guidelines utilized by the Department to ensure electronic security for HIPAA and to develop contingency policies and procedures for:

- Data backup.
- Disaster recovery plan to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure, and
- Emergency mode operation plan in the event of fire, vandalism, natural disaster, or system failure.

The County will provide web-based training to staff members for the awareness of HIPAA regulation for privacy and security to provide further training on the County's policies and procedures for the use and disclosure of PHI and the need to safeguard such information from unauthorized individuals.

Subject 8.04 – Employee User ID Accounts

PURPOSE

To establish a policy and related procedures for establishing and terminating an employee's user rights to Hillsborough County's systems.

POLICY

It is Hillsborough County's policy to ensure security and data integrity. The following group of programs may or may not apply to the Department(s).

Subject 8.05 – Data Classification Guidelines for Electronic Data

PURPOSE

This policy describes Hillsborough County's responsibility to identify and classify electronically stored material.

POLICY

Electronic documentation shall be identified by contents as PHI, confidential information or public record and shall be stored in an electronic environment that is appropriate to its classification.

PHI and confidential documentation shall be stored in a secured environment.

Subject 8.06 – Personnel Security Screenings

PURPOSE

The purpose of this policy and related procedures is to establish uniform guidelines for conducting background screenings for volunteers, new, and current employees.

POLICY

Human Resources will conduct a comprehensive national background screening on all selected potential applicants and new volunteers. Additionally, we will conduct consistent in-state background screenings for all current staff members with procedures that ensure that all employees are screened at least once every five years.

Subject 8.07 – Disciplinary Process

PURPOSE

This policy is designed to implement formalized discipline for staff members who fail to comply with the Security Polices, and HIPAA policies and procedures.

POLICY

Hillsborough County shall discipline staff members who fail to comply with Security Policies, Health Insurance Portability and Accountability Act (HIPAA) of 1996, or County policies and procedures.

Subject 8.08 – Disposal of Media (Electronic & Paper)

PURPOSE

The purpose of this policy is to establish uniform guidelines for the proper disposal of electronic and paper documentation.

POLICY

Original electronic documentation or original paper documentation containing PHI shall be retained at a minimum of six years or a maximum of time greater than six years as mandated by contract prior to permanent disposal.

Original electronic documentation or original paper documentation containing confidential or public record information shall be retained at a minimum of five years or a maximum of time greater than five years as mandated by law or contract prior to permanent disposal.

Duplicate documentation that is not of official record shall be allowed to be permanently disposed or rendered unrecoverable prior to the above retention requirements.

Department staff members will not dispose of PHI or confidential material in the trash or recycle container in whole. Duplicate PHI and confidential record or PHI and confidential documentation meeting disposal requirements must be shredded or permanently destroyed beyond recognition.

Whenever possible, Departments shall store paper documentation at the County Record Center. Each box shall list the disposal date. Storage boxes containing PHI or confidential material shall be clearly marked. The Transmittal And Receipt For Records Storage form shall provide special instructions, which notes the contents of the box contains PHI, and the material must shredded beyond recognition.

PHI received through an inbound e-mail is not permitted; and if the staff member receives an e-mail containing PHI, the staff member must follow approved procedures.

Outbound e-mails containing PHI are forbidden by County policy, and if accidental disclosure of PHI through an e-mail occurs, the staff member must follow approved procedures.

Staff members shall report violations of this policy to their department manager or designee.

Should the Department liaison(s) become aware of a potential privacy or security concern or a potential breach, the Department liaison(s) should report this to the County Privacy Officer without undue delay, and no more than 48 hours beyond becoming aware of the issue.

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

PURPOSE

This policy explains the safeguards that are required to protect protected health information (PHI), confidential information, and public record.

POLICY

Hillsborough County staff members must safeguard PHI, confidential information, and public record from intentional and unintentional disclosures. Safeguards include, but are not limited to written, electronic, and verbal communication; storage of information; and physical surroundings.

- Reasonable safeguard procedures may vary by department depending on factors such as the nature of information held by the department and the potential risk to security and privacy.

- Hillsborough County staff members shall follow proper procedures as described throughout this manual for unauthorized disclosure (accidental or willful release of information without written approval or legal authority) of PHI, confidential information, and public record or when a request for disclosure is received.

    - Hillsborough County staff members shall abide by Administrative Regulations and Release of Public Information when a member of the public receives a request for disclosure.

    - Hillsborough County staff members shall abide by HIPAA Policies and Procedures when a request for disclosure of PHI is received.

    - Hillsborough County staff members shall abide by County policies and procedures when a request for confidential information is received.

    - Hillsborough County staff members will dispose of stored electronic and paper documentation, as required by Section 8 of this HIPAA Policy - Disposal of Media (Electronic & Paper).

Hillsborough County staff members are prohibited from disclosing or sharing of passwords, access codes, key cards, or other user identifiers.

Staff members will not use un-secured e-mail to communicate PHI, including the use of e-mail attachments, which contain PHI.

Application software requiring installation on County equipment must be security compliant and must be installed by IT, or an authorized staff.

Subject 8.10 – Access Controls to County Information Systems and Resources

PURPOSE

This policy defines controls that permit authorized staff members access to County information systems and resources.

POLICY

Access to County information systems and computing resources will be granted and based on each user's access privileges relating to their job functions and on a need to know basis. Access security must be approved and authorized by each staff member's manager/supervisor or authorized designee, prior to access.

Staff members shall be issued an employee ID.

Visitors visiting the County Administration Office shall be required to sign in with the receptionist and be issued a visitors identification badge.

Each department shall assign a designee to be 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.

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

PURPOSE

This policy describes Hillsborough County's policy on the continued management of access privileges granted active staff members to County information systems and resources.

POLICY

The Department is responsible to ensure staff members who are no longer in need of County information systems and resources are immediately terminated from access.

Subject 8.12 – Disaster Recovery and Business Continuity Planning

PURPOSE

To ensure Hillsborough County develops and maintains a disaster recovery and business continuity plan and process to allow the County to deliver essential business functions despite damage, loss, or disruption of County information systems and resources due to the unexpected occurrence of a natural or man-made emergency or disaster.

POLICY

Hillsborough County is responsible to develop, periodically update and regularly test disaster recovery and business continuity plans designed to ensure the availability of the County's essential services and communications in the event of a natural or manmade emergency or disaster event.

Section 9 – Other Policies and Procedures

Subject 9.01 – Sanctions

PURPOSE

This Policy is designed to implement formalized disciplinary actions (sanctions) for staff members and Business Associates who fail to comply with the HIPAA policies and procedures of Hillsborough County.

POLICY

Hillsborough County shall discipline staff members and Business Associates, who fail to comply with the HIPAA Privacy Policies and Procedures of Hillsborough County.

This Policy shall not apply to staff members, with respect to actions that are covered by and meet the conditions of 45 C.F.R. §164.502(j) of the HIPAA Regulation relating to whistleblowers and 45 C.F.R. §164.530(g)(2) relating to complaints, investigations and other actions in connection with possible violations of the HIPAA Regulation.

Although this Policy addresses specific procedures which Hillsborough County will follow in the event that a staff member fails to comply with the HIPAA Privacy Policies and Procedures of Hillsborough County, it is not a limitation on the disciplinary actions available to Hillsborough County through County Human Resources Personnel Policies ("County Personnel Policies").

Hillsborough County's sanction policy provides the following examples of potential violations of policy and procedure:

- Sharing user id and passwords with other staff members.
- Not protecting the client's right to privacy of protected health information.
- Not disposing of media that contains PHI appropriately.

Failing to complete the annual training by the required deadline will result in a disciplinary action as outlined below:

- First Violation: Informal Couseling
- Second Violation: Formal Couseling
- Third Violation: Written Reprimand
- Fourth Violation: Pre-Disciplinary Hearing

County Administrator Policy 7.6 Employee Counseling and Progressive Discipline permits the adjustment of disciplinary actions based on the severity of the violation and previous disciplinary history.