CITY OF LOS ANGELES

HIPAA POLICY

Policy Number: 1
Effective Date: 09-11-13
Last Revised: _____

General HIPAA Compliance Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this General HIPAA Compliance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs overall HIPAA compliance for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY.
- CITY and its HEALTH CARE COMPONENTS must comply with HIPAA and the HIPAA-implementing regulations, in accordance with the requirements of Sections 164.104, 164.306, and HITECH Act Section 13401.
- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- Compliance with HIPAA will strengthen our non-HIPAA compliance obligations, and in fact, will support and strengthen our non-HIPAA compliance requirements and efforts.

Policy

- It is the Policy of CITY to become and to remain in full compliance with all the requirements of HIPAA.
- It is the Policy of CITY to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy. [Policy No. 3]
- All HIPAA compliance-related documentation will be managed and maintained for a minimum of six years from the date of creation or last revision, whichever is later, in accordance with CITY'S Document Retention Policy. [Policy No. 4]

Compliance and Enforcement

All Managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 2
Effective Date: 09-11-13
Last Revised: _____

Policies and Procedures Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Policies and Procedures Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the creation, documentation and use of Policies and Procedures for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- HIPAA law and the implementing HIPAA regulations, at § 160.310, § 164.306, § 164.312, § 164.316 and § 164.530(i), require the creation and implementation of specific Policies and Procedures.
- Good business practices and general business ethics call for the creation and implementation of clear and reasonable Policies and Procedures.
- The Policies and Procedures created and implemented by CITY should provide clear guidance to all workforce members about our obligations under the law and how we do business.

Policy

- It is the Policy of CITY to create and implement appropriate Policies and Procedures as required by law and as suggested by good business practices and general business ethics.
- All Policies and Procedures shall be updated and amended as needed or as required by law.
- All Policies and Procedures shall be distributed to, or made otherwise available to, the entire workforce.
- All Policies and Procedures shall be regularly maintained and secured, and copies shall be stored offsite with other important business records for safekeeping.
- All members of the workforce are required to read, understand, and comply with this and all other Policies and Procedures created and implemented by CITY.

Compliance and Enforcement

All Managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 3
Effective Date: 09-11-13
Last Revised: _____

Documentation Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Documentation Policy in order to recognize the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the creation, use, and maintenance of documents related to HIPAA compliance for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- CITY must comply with HIPAA and the HIPAA implementing regulations concerned with documentation at § 164.312(b)(2)(i), § 164.316, § 164.530(j)(1)(ii), and § 164.530(j)(1)(iii), among others.

Policy

- Officers, agents, employees, contractors, temporary workers, and volunteers who work for or perform any services (paid or unpaid) for CITY must document all HIPAA-related activities that require documentation.
- All HIPAA-related documentation must be created and maintained in written form, which may also include electronic forms of documentation.
- Any action, activity or assessment that must be documented, shall be documented in accordance with this and other policies and procedures implemented by CITY.
- All HIPAA-related documentation must be forwarded, used, applied, filed, or stored in accordance with this and other policies and procedures created and implemented by CITY.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 4
Effective Date: 09-11-13
Last Revised: _____

HIPAA Documentation Retention Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this HIPAA Documentation Retention Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs HIPAA documentation retention for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY must comply with HIPAA and the HIPAA implementing regulations concerned with documentation retention at § 164.316 and § 164.530(j), among others.
- Proper and lawful retention of HIPAA-related documentation is both a requirement under HIPAA and good business practice.
- Proper and lawful retention of HIPAA-related documentation is essential to proving our compliance with HIPAA, responding to investigations, and to effectively serving our constituents.

Policy

- It is the Policy of CITY to retain all HIPAA-related documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 5
Effective Date: 09-11-13
Last Revised: _____

Documentation Availability Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Documentation Availability Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the availability of HIPAA-related documentation for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY must comply with HIPAA and the HIPAA implementing regulations concerned with the availability of HIPAA-related documentation, in accordance with the requirements at § 164.310, § 164.316, § 164.530(j), among others.

Policy

- It is the Policy of CITY to make all HIPAA-related documentation available to those persons responsible for implementing the Policies and/or Procedures to which such documentation pertains.
- All HIPAA-related documentation shall be distributed or made otherwise available to all workforce members who are affected by the documentation.
- Workforce members affected by specific HIPAA-related documentation shall have access to such documentation prior to their beginning or executing work that depends on such documentation.
- No member of the workforce shall be held accountable for compliance with any HIPAA-related documentation, Policies, or Procedures unless they have been given access to such documentation.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 6
Effective Date: 09-11-13
Last Revised: 09-10-13

Documentation Updating Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Documentation Updating Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the updating and maintenance of HIPAA-related documentation for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY must comply with HIPAA and the HIPAA implementing regulations concerned with the updating of HIPAA-related documentation, in accordance with the requirements at § 164.310, § 164.316, § 164.530(j), among others.
- Appropriate and timely updating of HIPAA-related documentation is both a requirement under HIPAA and good business practice.
- Appropriate and timely maintenance of HIPAA-related documentation is essential to proving our compliance with HIPAA, responding to investigations, and to effectively serving our constituents.

Policy

- It is the Policy of CITY to review all HIPAA-related documentation periodically, and update such documentation as needed, in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.
- Reviews of HIPAA-related documentation shall be made periodically, but at least every 12 months for the purposes of this Policy.
- Reviews and updates of HIPAA-related documentation that occur as a result of this Policy shall be made by CITY'S designated Privacy Officer or HIPAA Officer.
- Reviews and updates of HIPAA-related documentation that occur as a result of this Policy shall be documented according to CITY'S Documentation Policy. [Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 7
Effective Date: 09-11-13
Last Revised: _____

HHS HIPAA Investigations Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this HHS HIPAA Investigations Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs responses to and activities during HIPAA-related investigations conducted by the U.S. Department of Health and Human Services ("HHS"), or its designees, that involve CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY.
- CITY and its HEALTH CARE COMPONENTS must comply with HIPAA and the HIPAA-implementing regulations concerned with HIPAA-related investigations by HHS, in accordance with the requirements at § 164.308, § 164.310, and § 164.312, among others.

Policy

- It is the Policy of CITY to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS.
- It is the Policy of CITY to not impede or obstruct any HIPAA-related investigations conducted by HHS.
- It is the Policy of CITY to provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS.
- Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following:
- Whenever a HHS investigation is discovered, the following persons must be immediately notified:
    - Attorneys (HIPAA counsel AND local counsel, if different)
    - Executive Management
    - Privacy Officer
    - Security Officer
    - Compliance Officer
    - Health Information Management Department and/or the Custodian of Records

- ❑ Cooperate, but do not volunteer information or records that are not requested
- ❑ Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel
- ❑ Have at least one, if not two witnesses available to testify as to your requests and their responses.
- ❑ Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under NO circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.
- ❑ Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation. Generally, guns strapped to hips are a good indicator of the presence of law enforcement personnel; but, if in doubt, ask.
- ❑ Permit the investigators to have access to protected health information ("PHI"), in accordance with our notice of privacy practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
- ❑ Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
- ❑ Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that we provide witnesses to be questioned during the initial phase of an investigation.
- ❑ Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators.
- ❑ Ask the investigators for documents related to the investigation. For example, request:
    - o copies of any search warrants and/or entry and inspection orders
    - o copies of any complaints
    - o a list of patients they are interested in
    - o a list of documents/items seized
- ❑ Do NOT expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
- ❑ Don't leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- ❑ Don't offer food (coffee, if already prepared, and water, if already available, is ok). Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.
- ❑ Don't be "chatty." Only tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 8
Effective Date: 09-11-13
Last Revised: _____

Breach Notification Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Breach Notification Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs consumer notifications of breaches of individually identifiable health information for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY and its HEALTH CARE COMPONENTS must comply with HIPAA and the HIPAA implementing regulations concerned with notifications to consumers, the media, and the Secretary of the Department of Health and Human Services ("HHS") about breaches of individually identifiable health information, in accordance with the requirements at Sections 164.400 to 164.414.
- Compliance with HIPAA's breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.
- Timely notifications to consumers about breaches of individually identifiable health information can help reduce or prevent identity theft and fraud.
- Timely notifications to consumers about breaches of individually identifiable health information can help protect our business and reputation.
- Only breaches of "unsecured" (unencrypted or not rendered unusable, unreadable or indecipherable to unauthorized persons) protected health information trigger HIPAA's breach notification requirements.

Policy

- It is the Policy of CITY to provide timely notifications to affected (patients and/or) consumers about breaches of individually identifiable health information.
- Model Breach Notification letters or emails shall be developed and prepared to be used as needed.
- It is the Policy of CITY to timely provide:

- Notice to patients alerting them to breaches "without unreasonable delay", but no later than 60 days after discovery of the breach.
- A breach is treated as "discovered" as of the first day it is known or, by exercising reasonable diligence would have been known to the CITY, HEALTH CARE COMPONENT or their business associates.
- Notice to CITY by Business Associates ("BAs") when BA discovers a breach "without unreasonable delay" and not later than 60 days after discovery of the breach.
- Notice to the Secretary of HHS and prominent media outlets about breaches involving more than 500 patient records.
- Notice to next of kin about breaches involving patients who are deceased.
- Notices are to be in plain language via first class mail or substitute notice and include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the patient, contact procedures and the CE's response to the breach.
- Annual notice to the secretary of HHS not later than 60 days after the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records.
- Delay of notification is permitted if a law enforcement official states that notice would impede a criminal investigation or damage national security. 45 CFR 164.412

- An acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA regulations (i.e. the Privacy Rule) is presumed to be a breach unless the covered entity (CITY, HEALTH CARE COMPONENTS, business associate) demonstrates that there is a low probability that the PHI has been compromised based upon a risk assessment of at least the following factors:
  - Nature and extent the PHI was involved including the identifiers and likelihood or re-identification;
  - Whether the person(s) involved in the disclosure were authorized persons;
  - Whether the PHI was actually acquired or viewed; and
  - The extent to which the risk to the PHI has been investigated. [45 CRF 164.402; Emphasis added.]
- Business Associates of CITY are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to the designated HIPAA Officer or Privacy Officer "without unreasonable delay" and not later than 60 days after discovery of the breach.
- Business Associate contracts, whether existing or new, are required to have corresponding breach notification requirements included in them.
- Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to CITY's Sanction Policy. [See Policy No. 18]
- All breach-related activities and investigations shall be thoroughly and timely documented in accordance with CITY's Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 9
Effective Date: 09-11-13
Last Revised: _____

Privacy-Official Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Privacy-Official Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the designation and duties of a HIPAA Privacy-Official for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY and its HEALTH CARE COMPONENTS must comply with HIPAA and the HIPAA implementing regulations concerning the designation of a Privacy Official, in accordance with the requirements at § 164.530(a).

Policy

- It is the Policy of CITY to designate and maintain at all times an active HIPAA Privacy-Official.
- The HIPAA Privacy-Official's general responsibilities are to:
    - Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related Policies and Procedures.
    - Conduct various risk analyses, as needed or required.
    - Manage breach notification investigations, determinations, and responses, including breach notifications.
    - Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.
- The HIPAA Privacy-Official's potential duties may include:
    - Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce,

extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.

- Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
- Administer patient requests under HIPAA's Patient Rights.
- Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
- Develop specific policies and procedures mandated by HIPAA.
- Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- Draft and disseminate the Privacy Notice required by the Privacy Rule.
- Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
- Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that confidential data is adequately protected when such access is granted.
- Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- Conduct periodic privacy audits and take remedial action as necessary.
- Oversee employee training in the areas of information privacy and security.
- Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
- Remain up-to-date and advise on new technologies to protect data privacy.
- Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- Track pending legislation regarding data privacy and if appropriate, seek to favorably influence that legislation.
- Anticipate patient or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns and questions.
- Evaluate privacy implications of online, web-based applications.
- Monitor data collected by or posted on our website(s) for privacy concerns.
- Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to our privacy practices.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 10
Effective Date: 09-11-13
Last Revised: _____

HIPAA State Law Preemption Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this HIPAA State Law Preemption Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs determinations and applications of preemption of HIPAA by State Law for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All affected personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations concerning state law preemptions of HIPAA regulations, in accordance with the requirements at § 160.201 to § 160.205.
- HIPAA generally preempts state laws regarding medical or health privacy. However, state laws that provide stronger protections for confidential health data, or that provide for better access to data than HIPAA, will preempt HIPAA regulations.
- Generally, HIPAA Covered Entities and Business Associates must follow both HIPAA law and state law when possible. If there is a conflict between the two, a preemption analysis and determination must be made to assess which laws (HIPAA, state laws, or both) must be followed.

Policy

- It is the Policy of CITY to comply, whenever possible, with both state law in the state(s) where we operate, as well as HIPAA law and regulations.
- It is the responsibility of the designated Privacy Official to analyze HIPAA preemption issues, in cooperation with legal counsel, and make preemption determinations.
- The designated Privacy Official shall create, modify, or amend organization policies to accurately reflect preemption determinations and provide guidance to management on HIPAA and state law preemption issues.

- If off-the-shelf or custom preemption analyses are obtained from external sources, it is the responsibility of the designated Privacy Official, in cooperation with legal counsel, to certify the validity and accuracy of such external preemption analyses before applying those analyses to our operations.
- The designated Privacy Official shall conduct ongoing research to monitor legislative changes in the state(s) where we operate that could affect HIPAA preemption issues.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 10A
Effective Date: 09-11-13
Last Revised: 09-10-13

California Confidential Medical Information Act [CMIA] Compliance and Preemption Analysis Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this California Confidential Medical Information Act ["CMIA"] Compliance and Preemption Analysis Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics. To the extent compliance with the CMIA exceeds compliance requirements for HIPAA, compliance with the CMIA will control.

This Policy governs determinations and applications of preemption of HIPAA by State Law for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All affected personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with the CMIA as codified in California Civil Code §§ 56 to 56.16, HIPAA and the HIPAA implementing regulations concerning state law preemptions of HIPAA regulations, in accordance with the requirements at § 160.201 to § 160.205.
- HIPAA generally preempts state laws regarding medical or health privacy. However, state laws such as the CMIA which provide stronger protections for confidential health data, or that provide for better access to data than HIPAA, will preempt HIPAA regulations.
- Generally, HIPAA Covered Entities and Business Associates must follow both HIPAA law and state law when possible. If there is a conflict between the two, a preemption analysis and determination must be made to assess which laws (HIPAA, state laws, or both) must be followed.

Policy

- It is the Policy of CITY to comply, whenever possible, with both state law in the state(s) where we operate, as well as HIPAA law and regulations.
- It is the responsibility of the designated Privacy Official to analyze HIPAA preemption issues, in cooperation with legal counsel, and make preemption determinations.

- The designated Privacy Official shall create, modify, or amend organization policies to accurately reflect preemption determinations and provide guidance to management on HIPAA and state law preemption issues.
- If off-the-shelf or custom preemption analyses are obtained from external sources, it is the responsibility of the designated Privacy Official, in cooperation with legal counsel, to certify the validity and accuracy of such external preemption analyses before applying those analyses to our operations.
- The designated Privacy Official shall conduct ongoing research to monitor legislative changes in the state(s) where we operate that could affect HIPAA preemption issues.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 11
Effective Date: 09-11-13
Last Revised: _____

HIPAA Training Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this HIPAA Training Policy to comply with our responsibility to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs HIPAA training-related issues for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations concerning the training of workforce members, in accordance with the requirements at § 164.530(b).
- Clear and complete HIPAA training, in combination with appropriate HIPAA awareness resources, can significantly reduce the likelihood of breaches of confidential information and HIPAA violations.

Policy

- It is the Policy of CITY to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, contractors, temporary workers, and volunteers.
- HIPAA training, at minimum, shall include the basics of HIPAA itself; the basics of HIPAA's privacy and security requirements and restrictions; and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.
- HIPAA training shall be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with individually identifiable health information.
- HIPAA training shall be conducted periodically for all employees, but no less than every six months.

- Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training. The designated HIPAA Privacy Official shall be responsible for the development (or acquisition), and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce.
- The designated HIPAA Privacy Official is responsible for the development or acquisition of appropriate HIPAA training and awareness resources.
- HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, and a protective attitude toward confidential data on an ongoing, daily basis.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 12
Effective Date: 09-11-13
Last Revised: _____

PHI Uses and Disclosures Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this PHI Uses and Disclosures Policy to comply with our responsibility to protect individually identifiable health information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs uses and disclosures of Protected Health Information ("PHI") for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.
- HIPAA-regulated entities must implement Policies and Procedures to ensure that all uses and disclosures of PHI are made or denied in accordance with HIPAA law and regulations.
- For especially sensitive information, such as AIDS/HIV, alcohol and drug abuse prevention and treatment, and the like, patient consent to disclosure must be *informed* that is, made with knowledge of the risks and benefits of the disclosure.
- Any disclosure of confidential patient information carries with it the potential for an unauthorized redisclosure that breaches confidentiality.
- CITY incurs costs when releasing patient information (copying, postage, and so forth) and is permitted under the law to charge a reasonable fee to offset those costs.

Policy

- It is the Policy of CITY to conduct its operations in accordance with HIPAA's rules governing uses and disclosures of Protected Health Information.
- CITY will process requests for information from patient records in a timely, consistent manner as set forth in this Policy.

- The following priorities and time frames shall apply to requests for disclosures of PHI:
  - *Emergency requests involving immediate emergency care of patient:* immediate processing.
  - *Priority requests pertaining to current care of patient:* within one workday.
  - *Patient request for access to own record:* within three (3) workdays.
  - *Subpoenas and depositions:* as required.
  - *All other requests:* within five (5) workdays.
- Courtesy Notifications to Practitioners -- As a courtesy, records processing personnel shall notify the appropriate healthcare practitioner when any of the following occur:
  - Patient or his or her representative requests information from the medical record.
  - Patient or representative requests direct access to the complete medical record.
  - Patient or representative institutes legal action.
- Disclosure Monitoring and Logging -- Medical records personnel will maintain a log to track the step-by-step process towards completion of each request for the release of PHI. Health Information Management personnel and/or the Privacy Official will review and update this log daily to give proper priority to requests and to provide early intervention in problem situations. The log shall contain the following information:
  - Date department received the request.
  - Name of patient.
  - Name and status (patient, parent, guardian) of person making request.
  - Information released.
  - Date released.
  - Fee charged.
- Fee Schedule – CITY will charge a reasonable fee to offset the costs associated with specific categories of requests. The HIPAA Privacy Official shall develop and implement a Fee Schedule related to disclosures of PHI. Fees shall be based on an assessment of such factors as the costs of equipment and supplies, employee costs, and administrative overhead and shall include postage (including express mail or courier costs) when incurred at the request of the authorizing party. For requests for records in electronic format, HIPAA permits fees to include only direct labor costs when responding to such requests. Individual states have also established maximum fees for copies of patient records.
- Unless the request specifies release of the complete medical record, the Health Information Management Department shall release only selected portions of the record. The department shall prepare an appropriate cover letter detailing the items included.
- Prohibition of Redisclosure -- Unless a law or regulation requires a more specific prohibition on redisclosure (usually for AIDS/HIV, alcohol and drug abuse, and other particularly sensitive medical information), each disclosure outside the facility shall contain the following notice:
  - *The attached medical information pertaining to [Name of patient] is confidential and legally privileged. [Name of facility] has provided it to [Name of recipient] as authorized by the patient. The recipient may not further disclose the information without the express consent of the patient or as authorized by law.*
- Retention of Disclosure Requests -- The Health Information Management Department and/or Privacy Officer will retain the original request, the authorization for release of information, and a copy of the cover letter in the patient(s) medical record for the appropriate record retention period.
- Use of Copying Services -- To facilitate the timely processing of release of information requests, CITY may use the services of a commercial copying service on terms that protect the integrity and confidentiality of patient information.
- Disclosure Quality Control -- The director of the Health Information Management Department and/or Privacy Official shall conduct a routine audit of the release of information at least quarterly, paying particular attention to the following:
  - Validity of authorizations.

- Appropriateness of information abstracted in response to the request.
- Retention of authorization, request, and transmitting cover letter.
- Procedures for telephone, electronic, and in-person requests.
- Compliance with designated priorities and time frames.
- Proper processing of fees.
- Maintenance of confidentiality.

- In-service Training on Disclosures -- The Director of Health Information Management and/or Privacy Official shall give periodic in-service training to all employees involved in the release of information.
- Semi-Annual Policy Review - The Director of Health Information Management and/or Privacy Official shall review this policy and associated procedures with risk management and legal counsel at least semiannually.

- Capacity to Authorize -- [Name of facility] requires a written, signed, current, valid authorization to release medical information as follows:

Patient Category	**Required Signature**
Adult Patient	The patient or a duly authorized representative, such as court-appointed guardian or attorney. Proof of authorized representation required (such as notarized power of attorney).
Deceased Patient	Next of kin as stated on admission face sheet (state relationship on authorization) or executor/administrator of estate.
Unemancipated Minor	Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).
Emancipated Minor	Same as adult patients above.
Psychiatric, drug, alcohol program patients/clients	Same as adult patients above, but check for special requirements.
AIDS/HIV or other sexually transmitted disease patients	Same as adult patients above, but check for special requirements.

- Authorization Forms -- The Director of Health Information Management and/or Privacy Official shall develop and use an approved authorization form. All personnel will use this form whenever possible. All personnel shall, however, honor letters and other forms, provided they include all the required information.
- Revocation of Authorization -- A patient may revoke an authorization by providing a written statement to us. The revocation shall become effective when the facility receives it, but shall not apply to disclosures already made.
- Refusal to Honor Authorization -- Health Information Management Department personnel and/or the Privacy Official or others authorized to release information will not honor a patient authorization when they have a reasonable doubt or question as to the following information:
  - Identity of the person presenting the authorization.
  - Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person.
  - Legal age or status as an emancipated minor.

- Patient capacity to understand the meaning of the authorization.
- Authenticity of the patient(s) signature.
- Current validity of the authorization.
- In such situations, the employee shall refer the matter to the Director of Health Information Management and/or Privacy Officer for review and decision.

- Electronic Records -- The above requirements apply equally to electronic records. No employee shall release electronic records without complying with this policy.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 13
Effective Date: 09-11-13
Last Revised: 09-10-13

Patient Rights Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Patient Rights Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs all matters pertaining to patient rights for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements pertaining to the rights of patients at § 164.520 to § 164.528, as amended by the HITECH Act of 2009 (ARRA Title XIII).
- Patients information related to patient rights includes only that information contained in each patient's Designated Record Set ("DRS"), which is defined in the HIPAA regulations at § 164.501 as:
    - A group of records maintained by or for a covered entity that is:
    - The term "record" means 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.
- The provision of patient rights in a timely and positive manner can enhance the quality of care we provide to patients, by providing certain rights and controls to patients over their individually identifiable health information.

Policy

- ❑ It is the Policy of CITY to provide all the patient rights to our patients that are called for in the HIPAA regulations. **[Form: Notice of Privacy Rights]**
- ❑ Patient Rights that we provide and support include:
  1. The Right to receive a copy of our "Notice of Privacy Practices", which details how individually identifiable health information may be used or disclosed by this organization.
  2. The Right to review or obtain a copy of medical records about that patient, or about the patient's minor children.
  3. The Right to request restrictions on the use or disclosure of the patient's medical records.
  4. The Right to receive individually identifiable health information at an alternate address or through alternate delivery means, such as by fax or courier.
  5. The Right to request amendments to medical records, with certain limitations.
  6. The Right to an accounting of certain disclosures of individually identifiable health information.
  7. The Right to file a privacy complaint directly with us, or with the federal government.
- ❑ It is the Policy of CITY to provide all the patient rights to our patients that are called for in the HIPAA regulations in a timely and positive manner.
- ❑ No retaliation of any kind is permitted against any person, patient, or workforce member for exercising any Right guaranteed by HIPAA.
- ❑ It is the Policy of CITY that our Designated Record Set, for purposes of fulfilling HIPAA Patient Rights includes the following types or categories of data and items:
  - 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
  - Used, in whole or in part, by or for the covered entity to make decisions about individuals.
  - _____
  - _____
- ❑ It is the Policy of CITY that our Designated Record Set, for purposes of fulfilling HIPAA Patient Rights excludes the following types or categories of data and items:
  - Any data not designated in the City's Designated Record set above
  - _____
  - _____
  - _____
  - _____

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 14
Effective Date: 09-11-13
Last Revised: _____

Privacy Complaints Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Privacy Complaints Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the management of, and response to privacy complaints for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII).
- HIPAA regulations, at § 164.530(g), prohibit intimidating or retaliatory acts against any person or patient who files a privacy complaint or exercises any Right guaranteed under HIPAA.

Policy

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

- It is the Policy of CITY to respond in a timely and positive manner to all complaints submitted by any persons or parties, including patients, workforce members, and any other person or party.
- Responsibility for the acceptance of, management of, and responses to complaints shall reside with the designated HIPAA Officer, who shall establish a process and appropriate forms to receive and process complaints.
- All complaints must be submitted in written form, dated and signed by the complainant.
- CITY shall investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing. If more time is required to investigate and resolve a specific complaint, the complainant shall be notified in writing within 30 days of the time each complaint is submitted in writing, that additional time is required to investigate and resolve the

complaint. In no case shall more than 60 days elapse between the time a complaint is submitted in writing and the resolution of the complaint.

- The HIPAA Officer shall investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner.
- The final resolution or disposition of each complaint shall be documented in accordance with CITY's Documentation Policy [See Policy No. 3], and shall be retained in accordance with CITY 's Documentation Retention Policy. [See Policy No. 4]
- The final resolution or disposition of each complaint shall be documented and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30-days of response time is invoked, as above.
- In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediations may include, but are not limited to:
    - A written apology to the complainant from our organization.
    - Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured individually identifiable health information that has been compromised or put at risk by our actions.
    - Financial compensation, if determined to be appropriate by legal counsel and senior management.
    - Sanctions against workforce members, as appropriate to the circumstances.
    - Other unspecified remediation(s), as determined by legal counsel and senior management.
- For complaints submitted to the federal government, it is the Policy of CITY to cooperate fully and openly with federal authorities as they conduct their investigation, as specified in this organization's HHS Investigations Policy.
- No officer, agent, employee, contractor, temporary worker, or volunteer of this organization shall obstruct or impede any investigation in any way, whether internal or federal.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 15
Effective Date: 09-11-13
Last Revised: _____

Risk Management Process Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Risk Management Process Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the establishment and management of a risk management process for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and management of an appropriate risk management process, in accordance with the requirements at § 164.302 to § 164.318.
- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. [See Sanctions Policy; Policy No. 18]
- The establishment and maintenance of an appropriate risk management process will generally reduce our privacy and security risk, can reduce the likelihood of creating HIPAA violations, whether inadvertent or intentional.

Policy

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

- It is the Policy of CITY to establish, implement, and maintain an appropriate risk management process.
- Such risk management process shall be under the direct control and supervision of the HIPAA Official or HIPAA Officer, and shall involve legal counsel, information technology, records management, senior management, and any other parties or persons deemed to be appropriate to the process.

- Business and information-technology "best practices", along with the research and recommendations of the National Institute for Standards and Technology ("NIST"), shall be included in the development and execution of the risk management process.
- Our risk management process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
- The results of the risk management process shall be input into management's decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 16
Effective Date: 09-11-13
Last Revised: _____

Risk Analysis Policy [Required]

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Risk Analysis Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the risk analysis process for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to risk analysis, in accordance with the required requirements at § 164.308(a)(1)(ii)(A).
- Risk analysis is an integral part of this organization's overall Risk Management Process Policy.

Policy

- It is the Policy of CITY to conduct periodic assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI") that we are entrusted with.
- Responsibility for conducting periodic risk analyses shall be with the designated HIPAA Privacy/Security Officer, who shall establish a plan and procedures for the conduct of such analyses.
- All such risk analyses and assessments shall be conducted periodically, but at least twice each year.
- The risk analysis process shall be modeled upon the risk analysis process recommended by the National Institute for Standards and Technology ("NIST").
- The results of risk analyses and assessments shall become an integral part of management's decision-making process, and shall guide decisions related to the protection of Protected Health Information.
- All such risk analyses and assessments shall be documented in accordance with this organization's Documentation Policy. [See Documentation Policy, Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 17
Effective Date: 09-11-13
Last Revised: _____

Risk Management Implementation Policy [Required]

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Risk Management Implementation Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the risk management implementation for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to risk management implementation, in accordance with the required requirements at § 164.308(a)(1)(ii)(B).
- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- This Risk Management Implementation Policy shall be considered an integral part of our other Risk Management policies, including, but not limited to our:
    - Risk Management Process Policy [See Policy No. 15], and our
    - Risk Analysis Policy [See Policy No. 16]

Policy

- It is the Policy of CITY to fully and completely implement our risk management process and all related policies.
- The implementation of our risk management process, analyses, and improvements shall be under the direct supervision of the designated HIPAA Privacy/Security Officer.
- The designated HIPAA Privacy/Security Officer shall develop and implement a plan, procedures, and a timetable for the implementation of our risk management process in all its aspects. Such actions shall be consistent with our other risk management policies.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 18
Effective Date: 09-11-13
Last Revised: _____

Sanction Policy [Required]

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Sanction Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs sanctions of workforce members for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce-member sanctions, in accordance with the required requirements at § 164.308(a)(1)(ii)(C).
- Appropriate, fair and consistent sanctions have a deterrent influence on workforce transgressions; can help prevent breaches of individually identifiable health information, and can help prevent or reduce the severity of HIPAA violations.

Policy

- It is the Policy of CITY to establish and implement appropriate, fair and consistent sanctions for workforce members who fail to follow established policies and procedures, or who commit various offenses.
- Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- Certain offenses can invoke immediate termination, including, but not limited to:
    - Theft
    - Intentional lying or deception
    - Drug or alcohol use while on the job
    - Violence against persons or property
- Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.

- ☐ It is the Policy of CITY to fully document all workforce sanctions and their dispositions, according to our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 19
Effective Date: 09-11-13
Last Revised: _____

Information Systems Activity Review Policy [Required]

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Information Systems Activity Review Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs overall information of systems activity review for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing required regulations pertaining to information systems activity review, in accordance with the requirements at § 164.308(a)(1)(ii)(D).

Policy

- It is the Policy of CITY to regularly review various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports.
- The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
- It is the Policy of CITY to fully document all information system activity review activities and efforts.
- This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 20
Effective Date: 09-11-13
Last Revised: _____

Assignment of Security Responsibility Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Assignment of Security Responsibility Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the assignment of overall security responsibility for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the assignment of security responsibility, in accordance with the requirements at § 164.308(a)(2).
- The assignment of overall security responsibility is an important and integral part of our overall risk management process, and shall be conducted in accordance and coordination with our Risk Management Process Policy.

Policy

- It is the Policy of CITY to assign overall responsibility for the security of individually identifiable health information, in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
- The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be the designated HIPAA Security Officer, who shall report directly to [Superior of the Privacy/Security Officer].
- The responsibilities and duties of the designated HIPAA Security Officer with overall security responsibility shall include, but are not limited to:
    - Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.

- Maintain an accurate inventory of (1) all individuals who have access to the Practice's confidential information, including PHI, and (2) all uses and disclosures of the Practice's confidential information by any person or entity.
- Administer patient requests and processes under HIPAA's patient rights.
- Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Cooperates with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Work with appropriate technical personnel to protect the Practice's confidential information from unauthorized use or disclosure.
- Develop specific policies and procedures mandated by the Privacy Rule.
- Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- Draft and disseminate the Privacy Notice required by the Privacy Rule.
- Determine when the Practice might need member consent or authorization for use or disclosure of PHI, and draft forms as necessary.
- Ensure that any research efforts conducted or supported by the Practice comply with appropriate privacy laws and policies and adequately protect the privacy of the data subjects.
- Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that the Practice's confidential data is adequately protected when such access is granted.
- Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- Ensure that future Practice initiatives are structured in such a way to ensure patient privacy.
- Conduct periodic privacy audits and take remedial action as necessary.
- Oversee employee training in the area of privacy.
- Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
- Remain up-to-date and advise on new technologies to protect data privacy.
- Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- Track pending legislation regarding data privacy and if appropriate seek to influence that legislation.
- Anticipate members' concerns and questions about the Practice's use of their confidential information and develop policies and procedures to respond to those concerns and questions.

- Evaluate privacy implications of any future on-line, web-based application procedure.
- Monitor any data collected by or posted on the Practice's Web sites for privacy concerns.
- Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to the Practice's privacy practices.

- ☐ It is the Policy of CITY to fully document the assignment of overall security responsibility, and all related activities and efforts, according to our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 21
Effective Date: 09-11-13
Last Revised: _____

Authorization and Supervision Policy and Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Authorization and Supervision Policy and Procedures document in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the authorization to access, and the supervision, of all workforce members who will access individually identifiable health information for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, in accordance with the requirements at § 164.308(a)(3).
- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, are essential components of a well-managed risk management system.
- Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, can help reduce our overall risk, and reduce the likelihood of data breaches and HIPAA violations.

Policy

- It is the Policy of CITY to only permit workforce members who have been appropriately authorized, to have access to individually identifiable health information.
- It is the Policy of CITY to properly and appropriately supervise workforce members who have access to individually identifiable health information.

- Workforce members shall have access only to the individually identifiable health information that they need in order to perform their work-related duties.
- It is the Policy of CITY to fully document the authorization and supervision of all workforce members who have access to individually identifiable health information.

Procedures

- Itemize specific authorization and supervision procedures in this section.
- Itemize specific authorization and supervision procedures in this section.
- Itemize specific authorization and supervision procedures in this section.
- Itemize specific authorization and supervision procedures in this section.
- Etc.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 22
Effective Date: 09-11-13
Last Revised: _____

Workforce Clearance Policy and Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Workforce Clearance Policy and Procedures document in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs overall workforce clearance for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to workforce clearance, in accordance with the requirements at § 164.308(a)(3).
- Providing for appropriate workforce clearance can help reduce the likelihood of data breaches and HIPAA violations.

Policy

- It is the Policy of CITY to provide the appropriate level of access to individually identifiable health information to all members of the workforce.
- The level of access to individually identifiable health information for workforce members shall be based upon the nature of each workforce member's job and its associated duties and responsibilities. Workforce members shall have access to all of the individually identifiable health information that they need to do their jobs, but no more access than that.
- No member of the workforce shall have access to a higher level of individually identifiable health information than the level for which they have been cleared.
- The designated HIPAA Privacy/Security Officer shall develop specific procedures to ensure that the intent of this Policy is executed in fact.
- Workforce clearance shall specifically incorporate various levels of background screening to ensure that persons with criminal records or histories of financial or legal difficulties do not have inappropriate access to individually identifiable health information.

- The designated HIPAA Privacy/Security Officer shall coordinate background screening requirements with Human Resources and legal counsel to ensure that appropriate background screening requirements are established and met, which can include pre-employment and post-employment screening.
- It is the Policy of CITY to fully document the authorization and supervision of all workforce members who have access to individually identifiable health information.

Procedures

- List and describe specific procedures in this section.
- List and describe specific procedures in this section.
- List and describe specific procedures in this section.
- List and describe specific procedures in this section.
- Etc.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 23
Effective Date: 09-11-13
Last Revised: _____

Access Termination Policy and Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Access Termination Policy and Procedures document in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the termination of workforce member access to individually identifiable health information for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the termination of workforce member access to individually identifiable health information, in accordance with the requirements at § 164.308(a)(3).
- Prompt and appropriate termination of workforce member access to individually identifiable health information can greatly reduce the likelihood of data breaches and HIPAA violations.

Policy

- It is the Policy of CITY to terminate any workforce member's access to individually identifiable health information when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy, in accordance with our Sanction Policy. [See Policy No. 18]
- Termination of workforce member access to individually identifiable health information must be effected immediately upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy or HIPAA offense.
- In no case shall the termination of access to individually identifiable health information be delayed more than 30 minutes from the moment of such a triggering event.
- It is the Policy of the CITY to fully document all access termination-related activities, in accordance with our Documentation Policy. [See Policy No. 3]

Procedures

- Itemize specific access termination procedures in this section.
- Itemize specific access termination procedures in this section.
- Itemize specific access termination procedures in this section.
- Itemize specific access termination procedures in this section.
- Etc.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 24
Effective Date: 09-11-13
Last Revised: _____

Access Authorization Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Access Authorization Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the authorization of access to individually identifiable health information for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to access authorization, in accordance with the requirements at § 164.308(a)(4).
- The implementation of appropriate processes to grant workforce members access to individually identifiable health information can help ensure that our uses and disclosures of individually identifiable health information are lawful and appropriate.

Policy

- It is the Policy of CITY to grant workforce members an appropriate level of access to individually identifiable health information that is based on their work-related duties and responsibilities.
- The level of access to individually identifiable health information granted to each member of the workforce shall be independent of the technology used to access such information, and shall apply to access through a workstation, transaction, program, process, or other mechanism.
- It is the Policy of CITY to fully document all access authorization-related activities and efforts.

Compliance and Enforcement

All Managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 25
Effective Date: 09-11-13
Last Revised: _____

Access Establishment and Modification Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Access Establishment and Modification Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the establishment and modification of workforce member access to individually identifiable health information for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and modification of workforce member access to individually identifiable health information, in accordance with the requirements at § 164.308(a)(4).
- Establishing and modifying an appropriate level of workforce member access to individually identifiable health information can help reduce the likelihood of data breaches and HIPAA violations.

Policy

- It is the Policy of CITY to provide a lawful and appropriate level of access to individually identifiable health information for each and every workforce member.
- Such access to individually identifiable health information shall be granted based on the nature and duties of the workforce member's job.
- Higher levels of access shall be provided only to those who need it.
- Any workforce member's ability to access to individually identifiable health information shall be modified immediately when the nature of their job changes and requires a different level of access, whether greater or lesser.
- It is the Policy of CITY to fully document all access establishment and modification-related activities and efforts, according to our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All Managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 26
Effective Date: 09-11-13
Last Revised: _____

Security Reminders Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Security Reminders Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the use of security reminders and security awareness resources for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to security reminders, in accordance with the requirements at § 164.308(a)(5).
- The frequent use of appropriate security reminders and other information security awareness resources can reduce the likelihood of data breaches and HIPAA violations.

Policy

- It is the Policy of CITY to develop or acquire and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
- The designated HIPAA Privacy/Security Officer shall assume responsibility for developing or acquiring such reminders and resources, and for implementing a plan and program ensuring their frequent use.
- It is the Policy of CITY to fully document all information security reminder-related activities and efforts, according to our Documentation Policy.

Compliance and Enforcement

All Managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline, up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 27
Effective Date: 09-11-13
Last Revised: _____

Malware Protection Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Malware Protection Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the use of various malware (malicious software) protection techniques, technologies and methods for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to protection from so-called malware, in accordance with the requirements at § 164.308(a)(5).
- The use of appropriate techniques, technologies, and methods to protect information systems from malicious software ("malware") is a proven approach to reducing the likelihood of data breaches, system malfunctions, and HIPAA violations.

Policy

- It is the Policy of CITY to develop and apply a rigorous program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software.
- Responsibility for malware protection shall reside with the designated HIPAA Privacy/Security Officer, who shall ensure that the most powerful and appropriate techniques, technologies, and methods are continuously used to protect our information system, and the individually identifiable health information they contain, from malicious software.
- The workforce must be trained regarding its role in protecting against malicious software and system protection capabilities, including educating its workforce on how malicious software is brought into an organization through email attachments and programs that are downloaded from the Internet.
- It is the Policy of CITY to fully document all malware protection-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All Managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 28
Effective Date: 09-11-13
Last Revised: _____

Log-In Monitoring Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Log-In Monitoring Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs activities related to log-in monitoring for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to log-in monitoring, in accordance with the requirements at § 164.308(a)(5).
- Regular monitoring of log-ins and log-in attempts is a proven approach to controlling access to sensitive information systems and data, and to detecting inappropriate information systems activity.

Policy

- It is the Policy of CITY to establish a program of regular monitoring and review of log-ins and log-ins attempts.
- The designated HIPAA Privacy/Security Officer shall assume responsibility for log-in monitoring and analysis, and for ensuring that such activities are executed on a continuous basis.
- All workforce members are to be trained on log-in policy, awareness of log-in attempts that are not appropriate, on how to manage and safeguard their passwords and how to report discrepancies.
- Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of senior management, legal counsel, and/or Human Resources, as appropriate.
- It is the Policy of CITY to fully document all log-in monitoring-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 29
Effective Date: 09-11-13
Last Revised: _____

Password Management Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Password Management Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs password management, including creating, changing, and managing passwords, for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to password management, in accordance with the requirements at § 164.308(a)(5).
- The creation and management of strong passwords is one of the simplest and most effective methods of protecting access to electronic systems containing, transmitting, receiving, or using individually identifiable health information.

Policy

- It is the Policy of CITY to require the use of strong passwords and pass-phrases by all workforce members who access, use, maintain systems that contain, transmit, receive, or use individually identifiable health information.
- The responsibility for implementing this policy and any attendant procedures is hereby assigned to the designated HIPAA Privacy/Security Officer, who shall develop and implement this policy in coordination with the most senior information technology personnel.
- All passwords or pass-phrases used to access systems containing, transmitting, receiving, or using individually identifiable health information shall be a minimum of six (6) characters in length, and must or should include non-alphanumeric characters or symbols in them.
- Passwords and pass-phrases must or should be changed by users or management at least every three (3) to six (6) months.
- In the event of an information system compromise, as determined by the designated HIPAA Privacy/Security Officer, some or all workforce-member passwords and pass-phrases may need to be changed. This determination shall be made by the designated HIPAA Privacy/Security Officer.

- Under no circumstances shall passwords or pass-phrases be written down and kept at or near computers and workstations where they may be found by others. Passwords and pass-phrases may, however, be written down and stored in a workforce member's wallet or purse, if the password or pass-phrase is thus afforded protection equal to the protection afforded to workforce members' cash, credit cards, and other critical documents.
- It is the Policy of CITY that any workforce member who loses, misplaces, forgets, or experiences any compromise of their password or pass-phrase shall immediately notify the designated HIPAA Official or HIPAA Officer, or, if they are unavailable, shall notify specify alternate notification contact. Such notification of password or pass-phrase compromise must be made *immediately* to the contact(s) indicated herein, but in no case shall such notification be delayed more than one (1) or alternate number hour(s).
- Proper password management shall be emphasized in HIPAA training programs, in security reminders, and in any HIPAA awareness resources used by this organization.
- It is the Policy of CITY to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]
- Etc.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 30
Effective Date: 09-11-13
Last Revised: _____

Policy on Security Incident Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Policy on Security Incident Procedures in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs security incident procedures for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.
- Security Incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. A security incident includes
    - Virus attacks that interfere with the operations of information systems with ePHI
    - An unauthorized entry
    - An information breach
    - An attack on the information system
    - Unauthorized probing
    - Unauthorized use of computer accounts and systems
    - Unauthorized browsing of files
    - Disruption of service by any means
    - Alteration or destruction of information
    - Improper use of information system
    - Stolen or otherwise inappropriately obtained passwords that are used to access ePHI
    - Corrupted backup tapes that do not allow restoration of ePHI
    - Physical break-ins leading to the theft of media with ePHI
    - Failure to terminate the account of a former employee that is used by an unauthorized user to access information systems with ePHI
    - Providing media with ePHI, such as a PC hard drive or laptop, to another user who is not authorized to access the ePHI prior to removing the ePHI stored on the media
- Appropriate responses to security incidents include, but are not limited to:
    - Rapid identification and classification of the severity of security incidents.

- Determination of the actual risk to individually identifiable health information, and the subject(s) thereof.
- Repairing, patching, or otherwise correcting the condition or error that created the security incident.
- Retrieving or limiting the dissemination of individually identifiable health information, if possible.
- Determining if the security incident rises to the level of a reportable breach under the HIPAA regulations.
- Making a lawful and appropriate report of a breach, if required, to the appropriate parties. Appropriate parties to whom breaches must be reported, as defined by HIPAA regulations, may include, but are not limited to:
  - Patients
  - Consumers
  - Regulatory Authorities, including HHS and/or the Federal Trade Commission
  - Law Enforcement
  - The local media, if necessary and required by law
- Mitigating any harmful effects of the security incident.
- Fully documenting security incidents, along with their causes and our responses.
- Expanding our knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.

- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.

Policy

- It is the Policy of CITY to rapidly identify and appropriately respond to all suspected or known security incidents, regardless of their severity, to mitigate to the extent practicable harmful effects of security incidents that are known to CITY and to document all security incidents and their outcomes.
- Responsibility for responding to and managing security incidents shall reside with the designated HIPAA Privacy/Security Officer, or specify other responsible party.
- The designated HIPAA Privacy/Security Officer or, specify other responsible party shall develop specific forms and procedures that shall be implemented in response to security incidents.
- It is the Policy of CITY to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy. [See Policy No. 3]

Security Incident Procedures

- All workforce members are required to immediately report a security incident or suspected incident. The incident or suspected incident is required to be reported on the Security Incident Form.
- The Privacy or Security Officer has the responsibility of immediately investigating the incident, to isolate the problem and to take the necessary steps to protect the ePHI, system and other vital information.
- The Privacy or Security Officer shall notify management immediately of a security incident that cannot be immediately corrected.
- The Privacy or Security Officer shall notify management if any ePHI or other vital information is altered or destroyed.

- Management shall be notified of the completed investigation and the outcome thereof. Any suspected computer crime or other unlawful activity involving the use of the computer system may be reported to local, state or federal law enforcement. Whether the unlawful activity is reported to law enforcement will be made by management with the recommendation of the Privacy or Security Officer.
- Remedial action shall be taken, including action against workforce members, when it had been confirmed that they caused o contributed to the incident.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 31
Effective Date: 09-11-13
Last Revised: _____

Data Backup Plan

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Data Backup Plan in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This plan and policy governs data backups for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to data backups, in accordance with the requirements at § 164.308(a)(7).
- The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and electronic protected health information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- Timely access to health information is crucial to providing high quality health care, and to our business operations.
- Physicians and others must have immediate, around-the-clock access to patient information.
- No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Data Backup Plan Specifics

- The Name of Responsible Party or Person is responsible for performing daily backups on Name of Entity or Facility's network, including shared drives containing application data, patient information, financial data, and crucial system information.
- CITY will back up all such data automatically, per Name of Backup Solution's programmed standards, nightly at 2300 hours.
- The Name of Responsible Party or Person or his or her designee will, no later than 0900 the next day, place the backup media into the media vault located in Location of Backup Vault or Facility.

- The media vault meets fire and disaster standards for media and will be kept locked at all times. Only the Name of Responsible Party or Person, the system administrator, and their designees have access to the media vault.
- In the event that the secured media vault is not available or properly functioning, the Name of Responsible Party or Person, the system administrator, or their designees will remove backup media to a secured offsite location until the media vault becomes available.
- The Name Responsible Party or Person, the system administrator, or their designees will use Name of Backup Solution's reporting utilities at the start of each business day to validate the accuracy, completeness, and integrity of the backup performed the previous night.
- Individuals so validating the backup will generate daily repots and log them in the network log in the system administrator's office. The system administrator will maintain such reports for a minimum of 30 days, or specify other number of days, weeks, or months.
- Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- Responsible personnel will clean the tape or other backup unit(s) according to the manufacturer's recommended guidelines, currently once per week, or specify other period.
- A rotation of four, or specify other number weekly data tapes must be maintained at all times.
- The Name of Responsible Party or Person will ensure replacement of backup tapes or media according to manufacturer's recommended guidelines currently annually, or specify other media replacement timeframe(s).
- The Name of Responsible Party or Person is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least monthly and more often if necessary to ensure data integrity, availability, and confidentiality.
- Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensue the validity of backup data.
- All personnel who detect or suspect a data backup problem should immediately report the same to the Name of Responsible Party or Person. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    - Narrative of the data backup problem.
    - How long the problem has existed.
    - Suggested solutions.

Compliance and Enforcement

All information technology managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 32
Effective Date: 09-11-13
Last Revised: _____

Disaster Recovery Plan

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Disaster Recovery Plan in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This plan and policy governs disaster recovery operations for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to disaster recovery, in accordance with the requirements at § 164.308(a)(7).
- A disaster may occur at any time, not necessarily during work hours.
- CITY must remain operational with as little disruption of business operations and patient care as possible.
- Continuity of patient care requires uninterrupted access to patient information.
- In a dangerous emergency, evacuating personnel has priority over preserving information assets.
- The following conditions can destroy or disrupt [name of facility]'s information systems:
    - Power interruption.
    - Fire.
    - Water.
    - Weather and other natural phenomena, such as earthquakes.
    - Sabotage and vandalism.
    - Terrorism.
- List other assumptions in this section.

Preventive Measures

- The Name of Responsible Party or Person and/or designee must ensure that all personnel must take the following preventive measures:
    - Retain dictation on disk for three months.
    - Back up computerized files according to our Data Backup Plan.
    - Store backup media tape in the off-site media vault, according to our Data Backup Plan.
    - Maintain and replace backup tapes according to our Data Backup Plans.

- Test integrity of backup system no less than monthly, according to our Data Backup Plan.
- Store media properly. For example, laser discs must be stored in sleeves of plastic, paper, or combination of the two, placed in cardboard jackets or boxes, and stored on edge on metal shelving, properly labeled.
- Color-code all media as to priority of evacuation: red is first priority; yellow is second priority; green is third priority.
- Protect by uninterruptible power supplies all servers and other critical equipment from damage in the event of an electrical outage.
- Locate file servers and other critical hardware in rooms with Halon fire protection systems which limit damage to the immediate area of the fire. In the event of a catastrophic fire, backup data must be installed on other/replacement hardware.
- In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent.
- In the event of a fire or flood, seal room(s) to contain fire or water and/or use strategies to protect information and equipment from fire or from water falling from above as appropriate.
- Receive training in disaster preparation and recovery and know responsibilities in the event of a disaster.

- ☐ The Name of Responsible Party or Person **must take the following measures:**
  - Ensure that major hardware is covered under CITYS' property and casualty, and/or other appropriate insurance policy or policies.
  - Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.

High Priority Tasks During Emergencies

All workforce members should:

- ☐ Remain calm.
- ☐ Give the alarm. That is, pull the fire alarm or call 911 as appropriate.
- ☐ Evacuate if necessary. If personnel are injured, ensure their evacuation and call emergency assistance as necessary.
- ☐ If a fire occurs that you believe you can fight, use the nearest fire extinguisher.
- ☐ If safe, close all doors as you leave.
- ☐ Obtain portable phone(s) to communicate.
- ☐ Notify concerned fire, police, security, administration, and others as necessary.
- ☐ Notify other departments of situation and emergency protocols.
- ☐ If computers have not automatically powered down, initiate procedures to orderly shut down systems, when possible.
- ☐ If a fire or flood occurs, disconnect power if possible.
- ☐ If a fire or flood occurs, try to prevent further damage from water by covering areas with plastic sheets with adequate drainage.
- ☐ Move records/equipment/storage media away from area being flooded. Organize health information logically and label clearly for continued access.
- ☐ Arrange for transportation of paper records to a salvage, restoration, or reconstruction company.
- ☐ Respond to requests for records via potable phone rather than computer.
- ☐ Continue to provide patient charts as requested by physicians or other parties.

High Priority Disaster Recovery Tasks

All workforce members should:

- ❑ Prevent personnel from entering the area until officials or building inspectors have determined that the area is safe to reenter.
- ❑ Not permit unauthorized personnel to enter the affected area.
- ❑ Determine the extent of the damage and whether additional equipment/supplies are needed.
- ❑ Determine how long it will be before service can be restored, and notify departments.
- ❑ Replace hardware as necessary to restore service.
- ❑ Work with vendors as necessary to ensure that support is given to restore service.
- ❑ Notify insurance carriers.
- ❑ Retrieve and upload backup files if necessary to restore service.
- ❑ Air-dry floppy disks, if any, using a hair dryer on "air," not "heat." When dry, copy disk.
- ❑ For water damage, wipe off CD-ROMs and laser discs with distilled water, working out from the center in a straight line, and then wipe off water or dirt with a soft, dry, lint-free cloth. Air-dry. Do not use a hairdryer. For dirt or smoke damage, wipe out from the center with a clean, soft cloth. Then wash off any remaining dirt with distilled water.
- ❑ Remove water-damaged paper records by the wettest first. Freeze wet items to stabilize.
- ❑ Wrap paper records to prevent them from sticking together. Label the wrapped records.
- ❑ Contact fire, water, and storm damage restoration company. Contact for services as needed.
- ❑ Reconstruct/reacquire documents from the following:
    - o Dictation system.
    - o Word processing system.
    - o Computer system.
    - o Holders of document copies.
- ❑ Move records and equipment back to home location.
- ❑ Catch up on filing.
- ❑ Ensure that backup procedures are followed.
- ❑ Document data that cannot be recovered in patient record.
- ❑ Meet with management and staff to identify opportunities for improvement.

Additional Disaster Recovery Tasks

The following tasks must be assigned to specific persons or positions:

- ❑ Determine whether additional equipment and supplies are needed.
- ❑ Notify vendors or service representatives if there is need for immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- ❑ If necessary, check with other vendors to see whether they can provide faster delivery.
- ❑ Rush order any supplies and equipment necessary.
- ❑ Notify personnel that an alternate site will be necessary and where it is located.
- ❑ Coordinate moving equipment and support personnel to the alternate site.
- ❑ Bring recovery materials from offsite storage to the alternate site.
- ❑ As soon as hardware is up to specifications to run the operating system, load software and run necessary tests.
- ❑ Determine priorities of software that must be available and load those packages in order. Post these priorities in a conspicuous location.
- ❑ Prepare backup materials and return them to the offsite storage area.
- ❑ Set up operations at the alternate site if necessary.
- ❑ Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed.
- ❑ Ensure that periodic backup procedures are followed according to our Data Backup Plan.

- ❑ Plan to phase in all critical support.
- ❑ Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations.
- ❑ Coordinate with administration and others for continuing support and ultimate restoration of normal operations.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 33
Effective Date: 09-11-13
Last Revised: 09-10-13

Emergency Mode Operations Plan

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Emergency Mode Operations Plan in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs emergency mode operations for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency mode operations planning, in accordance with the requirements at § 164.308(a)(7).
- Individually identifiable health information must be protected during emergencies, even as it is protected during normal operations. This Emergency Mode Operations Plan is designed to ensure the protection of individually identifiable health information during emergencies requiring CITY to operate in "emergency mode".
- This Emergency Mode Operations Plan must be implemented and executed in coordination with other emergency and/or disaster plans and procedures, as appropriate and necessary.

Policy

- It is the Policy of CITY to establish this Emergency Mode Operations Plan to implement procedures to enable continuation of critical business processes for the protection of individually identifiable health information while operating in emergency mode.
- It is the Policy of CITY to fully document all emergency planning and preparedness activities and efforts, in accordance with our Documentation Policy.
- This Emergency Mode Operations Plan shall b executed whenever CITY must operate in "emergency mode".
- "Emergency Mode" shall be in effect and activated whenever one or more of the following conditions applies:
    - Electrical power is unavailable for more than eight, or other number hours.
    - Fire, flood, storm or other natural disaster renders our normal business facility unavailable or unusable for more than eight, or other number hours.
    - Any other condition renders our normal business facility unavailable or unusable for more than eight, or other number hours.

Plan Details

The following personnel are hereby assigned to lead the functions listed below during emergency mode operations...

Function	Team Lead
Telephones Outbound	
Telephones Inbound	
Computing Resources	
U.S. Mail	
Couriers (FedEx, etc.)	
Internet and Email	
Customer/Patient Contact	
Medical Records	
Other Business Records	
Legal Issues	
U.S. Mail	
Couriers (FedEx, etc.)	
Internet and Email	
Transportation	
Internal Communications	
Physical Security	
Utilities Restoration	
Remediation & Restoration	
Vendor/Partner Relations	
Media Relations	
Event/Activity Chronicler	
other function here	

other function here	
other function here	

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 34
Effective Date: 09-11-13
Last Revised: _____

Policy on Testing and Revision of Contingency and Emergency Plans and Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Policy on Testing and Revision of Contingency and Emergency Plans and Procedures in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the periodic testing and revision of emergency and contingency plans and procedures for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the testing and revision of emergency and contingency plans and procedures, in accordance with the requirements at § 164.308(a)(7).
- Emergency and contingency plans, and the procedures associated with them, must be periodically tested and revised to ensure that they meet the emergency preparedness needs of CITY.
- Individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) must be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Policy

- It is the Policy of CITY to periodically test, and revise as necessary, all emergency preparedness plans, including emergency and contingency plans.
- Such emergency and contingency plans are the responsibility of the designated HIPAA Official or HIPAA Officer, who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements.
- All emergency and contingency plans shall be reviewed, and revised if necessary, at least annually, or specify other time period. Copies of all such plans shall remain on file and be available to all personnel.
- All emergency and contingency plans shall be rehearsed, with all team members participating in such rehearsals, at least twice annually, or specify other time period.

- It is the Policy of CITY that all individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) shall be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.
- It is the Policy of CITY to fully document all emergency preparedness plans, including emergency and contingency plans, and all the revisions thereto, in accordance with our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 35
Effective Date: 09-11-13
Last Revised: _____

Policy on Data and Applications Criticality Analyses

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Policy on Data and Applications Criticality Analyses in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the periodic analyses of the relative criticality of both data and applications for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the analysis of the relative criticality of both data and applications, in accordance with the requirements at § 164.308(a)(7).
- A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies and during normal business operations.

Policy

- It is the Policy of CITY to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations.
- The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in the place for data and applications at each level of risk.
- Data to be subject to criticality analysis shall include individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Criticality analysis shall be the responsibility of Name of Responsible Party or Person, who shall work in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
- Criticality analyses shall determine and document the relative criticality of each type or category of data and applications that CITY possesses and/or uses to the continuity and success of our operations.

- The most critical data and applications shall be given the highest priority in terms of investment and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
- In conducting data and applications analyses, Name of Responsible Party or Persons shall employ the technical guidance and recommendations of the National Institute of Standards and Technology ("NIST"), or other information technology "best practices", as appropriate.
- It is the Policy of CITY to fully document all analyses of the relative criticality of both data and applications, in accordance with our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 36
Effective Date: 09-11-13
Last Revised: _____

Policy on Determining the Effectiveness of Emergency and Contingency Plans and Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Policy on Determining the Effectiveness of Emergency and Contingency Plans and Procedures in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the use of periodic technical and nontechnical evaluations to determine the effectiveness of emergency and contingency plans and procedures for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the periodic evaluation of the effectiveness of emergency and contingency plans and procedures, in accordance with the requirements at § 164.308(a)(8).
- Emergency and contingency plans and procedures must be evaluated periodically to determine their potential effectiveness in genuine emergencies.

Policy

- It is the Policy of CITY to periodically evaluate emergency and contingency plans and procedures, in order to improve their effectiveness.
- It shall be the responsibility of Name of Responsible Party or Person to periodically conduct such technical and nontechnical evaluations. Name of Responsible Party or Person shall work in coordination with legal counsel, information technology, senior management, and any other persons, departments or parties necessary in order to conduct such evaluations.
- Such technical and nontechnical evaluations shall be conducted at least every six months, or specify another timeframe.
- The results of such technical and nontechnical evaluations shall be internally published and shall be available to senior management and to all parties with responsibility for emergency preparedness.

- The purpose of such evaluations is to improve the effectiveness of our emergency and contingency plans and procedures, so that they best protect our business, our assets, our personnel, and the individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) that we possess or use.
- It is the Policy of CITY to fully document our periodic technical and nontechnical evaluations to determine the effectiveness of emergency and contingency plans and procedures, in accordance with our Documentation Policy.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 37
Effective Date: 09-11-13
Last Revised: _____

Business Associates Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted the Business Associates Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs our relations and work with Business Associates (as defined by HIPAA at § 160.103 and as amended by the HITECH Act) for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to Business Associates, in accordance with the requirements at § 164.308(b)(1), § 164.410, § 164.502(e), § 164.504(e), and HITECH Act § 13401.
- In cooperation with our organization, Business Associates work with, use, transmit, and/or receive individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), which be afforded reasonable protections under HIPAA law.
- CITY has the primary responsibility in all Business Associate relationships to ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded.

Policy

- It is the Policy of CITY to establish and maintain business and working relationships with Business Associates that are in full compliance with all the requirements of HIPAA.
- Responsibility for maintaining appropriate and lawful relationships with Business Associates shall reside with the HIPAA Privacy/Security Officer, who shall ensure that all aspects of our Business Associate relationships are appropriate and lawful, and who shall ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
- With regard to Business Associates, the duties and responsibilities of the HIPAA Privacy/Security Officer shall include, but are not limited to the following:

- Ensure that all Business Associate contracts meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, and any requirements of State laws in the state(s) where we operate.
- Ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
- Ensure that Business Associates understand the importance and necessity of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), whether in electronic form ("ePHI") or hardcopy form.
- Ensure that Business Associates have proper and appropriate safeguards in place for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before entrusting such information to them.
- Ensure that Business Associates understand and are properly prepared to detect and respond to breaches of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

❑ It is the Policy of CITY to fully document all Business Associate-related contracts and activities, in accordance with our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 38
Effective Date: 09-11-13
Last Revised: _____

Contingency Operations Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted these Contingency Operations Procedures in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

These contingency operations procedures, in combination with our other emergency preparedness plan and procedures, govern contingency operations for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to Contingency Operations Procedures, in accordance with the requirements at § 164.310(a)(1-2).
- Contingency Operations Procedures, for purposes of this document, are defined as procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- These contingency operations procedures, in combination with our other emergency preparedness plans and procedures, shall be documented, analyzed, revised and updated periodically in accordance with other established emergency preparedness and documentation policies and procedures.

Policy

- It is the Policy of CITY to be fully prepared to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), during contingency operations.
- Responsibility for planning and executing contingency operations shall reside with Name of Responsible Party or Person, who shall prepare, analyze, test, and update plans for contingency operations on a periodic basis.
- The primary purpose of our contingency operations procedures is to allow our organization to restore lost data in the event of an emergency.

- ❑ It is the Policy of CITY to fully document all contingency operations plans and procedures, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Contingency Operations Procedures

- ❑ List specific contingency operations procedures in this section.
- ❑ List specific contingency operations procedures in this section.
- ❑ List specific contingency operations procedures in this section.
- ❑ List specific contingency operations procedures in this section.
- ❑ List specific contingency operations procedures in this section.
- ❑ List specific contingency operations procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 39
Effective Date: 09-11-13
Last Revised: _____

Facility Security Plan and Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Facility Security Plan and Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This plan and Policy governs facility security for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of the CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security, in accordance with the requirements at § 164.310(a)(1-2).
- In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to provide strong facility security, in addition to other technical and administrative safeguards, in order to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Primary responsibility for facility security is hereby assigned to HIPAA Privacy/Security Officer, who shall analyze the security of our facility and implement devices, tools and techniques to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- The analyses of our facility security should include, but are not limited to, the following factors:
    - Windows and doors
    - Roofs and the potential for roof access
    - Locks and keys
    - Electronic access control systems
    - Video cameras and video surveillance systems
    - Electronic alarms and related systems

  - Employee, partner, vendor and guest access
  - Vehicle parking security
  - Routine and non-routine deliveries
- ❑ It is the Policy of CITY to fully document all facility security-related activities and efforts, in accordance with our Documentation Policy [See Policy No. 3] and our Maintenance Records Policy. [See Policy No. ___]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 40
Effective Date: 09-11-13
Last Revised: _____

Information Access Control and Validation Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted these Information Access Control and Validation Procedures in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs information access control for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of the CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to information access control and validation, in accordance with the requirements at § 164.310(a)(1-2).
- Information access control and validation procedures are designed to control and validate individual access to facilities based on role or function; including visitor control, and access control for software testing and revision.
- Strong information access control and validation procedures are an essential element of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to implement and support strong information access control and validation procedures, in full compliance with all the requirements of HIPAA.
- Responsibility for developing, testing, analyzing, and periodically updating information access control and validation procedures shall reside with Name of Responsible Party or Person.
- The development and implementation of specific information access control and validation procedures shall be conducted in accordance with guidance and information provided by the National Institute of Standards and Technology ("NIST"), or other information technology "best practices".
- It is the Policy of CITY to fully document information access control and validation procedures, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Information Access Control and Validation Procedures

- ❑ List specific information access control and validation procedures in this section.
- ❑ List specific information access control and validation procedures in this section.
- ❑ List specific information access control and validation procedures in this section.
- ❑ List specific information access control and validation procedures in this section.
- ❑ List specific information access control and validation procedures in this section.
- ❑ List specific information access control and validation procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 41
Effective Date: 09-11-13
Last Revised: _____

Facility Security Maintenance Records Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Facility Security Maintenance Records Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the creation and use of facility security-related maintenance records for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to facility security maintenance records, in accordance with the requirements at § 164.310(a)(1-2).

Policy

- It is the Policy of CITY to create and maintain complete facility security maintenance records, in full compliance with all the requirements of HIPAA.
- Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security, as detailed in our Facility Security Plan.
- Responsibility for the creation and updating of facility security maintenance records is hereby assigned to Name of Responsible Party or Person, who shall establish procedures for maintaining such records in appropriate form.
- It is the Policy of CITY to fully document facility security maintenance records-related activities and efforts, in accordance with our Documentation Policy.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 42
Effective Date: 09-11-13
Last Revised: _____

Workstation Use Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Workstation Use Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs workstation use for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers and volunteers must read, understand and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
- The establishment and implementation of an effective workstation use policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and maintain this workstation use policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this workstation use policy, and any procedures associated with it, shall reside with HIPAA Privacy/Security Officer, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper functions, procedures, and appropriate environments of workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of CITY to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Workstation Use Procedures

- ❑ List specific workstation use procedures in this section.
- ❑ List specific workstation use procedures in this section.
- ❑ List specific workstation use procedures in this section.
- ❑ List specific workstation use procedures in this section.
- ❑ List specific workstation use procedures in this section.
- ❑

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with CITY'S Sanction Policy. [See Policy No. 18]

Policy Number: 43
Effective Date: 09-11-13
Last Revised: _____

Workstation Security Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Workstation Security Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs workstation security for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
- The establishment and implementation of an effective workstation security policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and maintain this workstation security policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this workstation security policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), to restrict access to authorized users only.
- It is the Policy of CITY to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Workstation Use Procedures

- ❑ List specific workstation security procedures in this section.
- ❑ List specific workstation security procedures in this section.
- ❑ List specific workstation security procedures in this section.
- ❑ List specific workstation security procedures in this section.
- ❑ List specific workstation security procedures in this section.
- ❑

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 44
Effective Date: 09-11-13
Last Revised: _____

Media Disposal Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Media Disposal Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs media disposal and disposition for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- Electronic media means 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 transmission media used to exchange information already in electronic storage media.]
- Media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.

Policy

- It is the Policy of CITY to dispose of all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in full compliance with all the requirements of HIPAA.
- Responsibility for proper media disposal and disposition shall reside with Name of Responsible Party or Person, who shall develop procedures to ensure the proper disposition of all such media.
- It is the Policy of CITY to fully document all media disposal-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Media Disposal and Disposition Procedures

- ❑ Identify the types of hardware and electronic media and track them.
- ❑ Disposal of any electronic media that contains ePHI must be rendered unusable and/or inaccessible.
- ❑ Develop methods of disposal of electronic media, including degaussing, to ensure all ePHI is fully erased or to use other methods to dispose of the electronic media is to physically damage it beyond repair, making the data inaccessible.
- ❑ Specify the use of technology, such as, software or a specialized piece of hardware, to make ePHI, and/or the hardware or electronic media, unusable and inaccessible.
- ❑ List specific media disposal and disposition procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 45
Effective Date: 09-11-13
Last Revised: _____

Media Re-Use Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Media Re-Use Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs media re-use for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- Electronic media means 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 transmission media used to exchange information already in electronic storage media.]
- Media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased or sanitized ("wiped") before any re-use of such media may take place, or the data residing on such media is subject to corruption, compromise, or loss.

Policy

- It is the Policy of CITY to properly erase and/or sanitize ("wipe") all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before any media may be re-used.
- Responsibility for proper media re-use shall reside with Name of Responsible Party or Person, who shall develop procedures to ensure the proper disposition of all such media before any re-use.
- It is the Policy of CITY to fully document all media re-use and disposition-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Media Re-Use and Disposition Procedures

- ❑ All workforce members must appropriately reuse electronic media, whether for internal or external use.
- ❑ All ePHI previously stored on the media must be removed to prevent unauthorized access to information.
- ❑ List specific media re-use procedures in this section.
- ❑ List specific media re-use procedures in this section.
- ❑ List specific media re-use procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 46
Effective Date: 09-11-13
Last Revised: _____

Hardware and Media Accountability Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Hardware and Media Accountability Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs hardware and media accountability for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at § 164.310(d)(1-2).
- Electronic media means 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.
- Proper protection of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), requires that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.

Policy

- It is the Policy of CITY to maintain records of the movements of hardware and electronic media, and any person responsible therefore, in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this hardware and media accountability policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person [Security Officer], who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to ensure that the CITY maintains records of the movements of hardware and electronic media, and any person responsible therefore.
- It is the Policy of CITY to fully document all hardware and media accountability-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Hardware and Media Accountability Procedures

- ❑ The Security Officer is required to identify all types of hardware and electronic media and person responsible for the hardware and electronic media containing ePHI.
- ❑ The movement of all hardware and electronic media containing ePHI must be tracked.
- ❑ The Security Officer must maintain a log documenting the movement of the hardware and electronic media from one location to another and must maintain a log documenting the person who is responsible for the hardware and electronic media.
- ❑ Where there are multiple devices of the same type, identify the individual devices, and log or record them separately using serial numbers or other tracking mechanism.
- ❑ List specific hardware and media accountability procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 47
Effective Date: 09-11-13
Last Revised: _____

Data Backup and Storage Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Data Backup and Storage Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs data backup and storage for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to data backup and storage, in accordance with the requirements at § 164.310(d)(1-2) and § 164.308(a)(7).
- Electronic media means 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 transmission media used to exchange information already in electronic storage media.]
- The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and electronic protected health information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- Timely access to health information is crucial to providing high quality health care, and to our business operations.
- Physicians and others must have immediate, around-the-clock access to patient information.
- No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy

- The Name of Responsible Party or Person is responsible for performing daily backups on network of the CITY, including shared drives containing application data, patient information, financial data, and crucial system information.

- Name of Responsible Party or Person will back up all such data automatically, per Name of Backup Solution's programmed standards, nightly at 2300 hours.
- The Name of Responsible Party or Person or his or her designee will, no later than 0900 the next day, place the backup media into the media vault located in Location of Backup Vault or Facility.
- The media vault meets fire and disaster standards for media and will be kept locked at all times. Only the Name of Responsible Party or Person, the system administrator, and their designees have access to the media vault.
- In the event that the secured media vault is not available or properly functioning, the Name of Responsible Party or Person, the system administrator, or their designees will remove backup media to a secured offsite location until the media vault becomes available.
- The Name of Responsible Party or Person, the system administrator, or their designees will use Name of Backup Solution's reporting utilities at the start of each business day to validate the accuracy, completeness, and integrity of the backup performed the previous night.
- Individuals so validating the backup will generate daily reports and log them in the network log in the system administrator's office. The system administrator will maintain such reports for a minimum of 30 days, or specify other number of days, weeks, or months.
- Any errors will be acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- Responsible personnel will clean the tape or other backup unit(s) according to the manufacturer's recommended guidelines, currently once per week, or specify other period.
- A rotation of four, or specify other number weekly data tapes must be maintained at all times.
- The Name of Responsible Party or Person will ensure replacement of backup tapes or media according to manufacturer's recommended guidelines, currently annually, or specify other media replacement timeframe(s).
- The Name of Responsible Party or Person is responsible for testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least monthly and more often if necessary to ensure data integrity, availability, and confidentiality.
- Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- All personnel who detect or suspect a data backup problem should immediately report the same to the Name of Responsible Party or Person. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    - Narrative of the data backup problem.
    - How long the problem has existed.
    - Suggested solutions.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 48
Effective Date: 09-11-13
Last Revised: _____

Unique User I.D. Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Unique User I.D. Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the mandatory use of unique user identification [I.D.'s] for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of unique user I.D.'s, in accordance with the requirements at § 164.306 and § 164.312(a)(1).
- The use of unique user I.D.'s is an essential element in our overall effort to protect individually identifiable health information, including Protected Health Information ("PHI"), as defined by HIPAA.

Policy

- It is the Policy of CITY to exclusively use unique user I.D.'s for all information system access and activities, in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this unique user I.D. policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that access to all our information systems and data is accomplished exclusively through the use of unique user I.D.'s.
- Nothing in this policy shall limit the use of additional security measures, including login and access measures, that may further enhance the security and protection we provide to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of CITY to fully document all unique user I.D.-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 49
Effective Date: 09-11-13
Last Revised: _____

Emergency Access Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted these Emergency Access Procedures in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs procedures for emergency access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to emergency access procedures, in accordance with the requirements at § 164.104, § 164.306, and § 164.312(a)(1).
- The establishment of emergency access procedures further strengthens the protections we offer to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and implement emergency access procedures, in full compliance with all the requirements of HIPAA.
- These emergency access procedures apply to access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Responsibility for the development and implementation of our emergency access procedures shall reside with Name of Responsible Party or Person, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to ensure that authorized workforce members can access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies.
- These Emergency Access Procedures shall be developed and implemented in combination with our emergency preparedness and response plans.

- ❑ It is the Policy of CITY to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Emergency Access Procedures

- ❑ Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.
- ❑ Identify a method of supporting continuity of operations should the normal access procedures are disabled or unavailable due to system problems.
- ❑ List specific emergency access procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 50
Effective Date: 09-11-13
Last Revised: _____

Automatic Log-Off Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Automatic Log-Off Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the mandatory use of automatic system log-off application for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to the use of automatic log-off applications, in accordance with the requirements at § 164.306, and § 164.312(a)(1-2).
- The establishment and implementation of an effective automatic log-off policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to always use automatic log-off applications or systems on all workstations and computers, in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this automatic log-off policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper functions and procedures of our automatic log-off systems on all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of CITY to fully document automatic log-off-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Automatic Log-Off Procedures

- List specific automatic log-off procedures in this section.
- List specific automatic log-off procedures in this section.
- List specific automatic log-off procedures in this section.
- List specific automatic log-off procedures in this section.
- List specific automatic log-off procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 51
Effective Date: 09-11-13
Last Revised: _____

Encryption and Decryption Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Encryption and Decryption Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs the encryption and decryption of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to encryption and decryption, in accordance with the requirements at § 164.312(a)(1-2).
- The establishment and implementation of an effective encryption and decryption policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of CITY to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Encryption and Decryption Procedures

- List specific encryption and decryption procedures in this section.
- List specific encryption and decryption procedures in this section.
- List specific encryption and decryption procedures in this section.
- List specific encryption and decryption procedures in this section.
- List specific encryption and decryption procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 52
Effective Date: 09-11-13
Last Revised: _____

Audit Controls Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Audit Controls Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs audits and auditing controls for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to audit controls, in accordance with the requirements at § 164.312(b).
- The establishment and implementation of an effective audit controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and maintain this audit controls policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this audit controls policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper usage and application of audit controls for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of CITY to fully document all audit controls-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Encryption and Decryption Procedures

- List specific audit controls procedures in this section.
- List specific audit controls procedures in this section.
- List specific audit controls procedures in this section.
- List specific audit controls procedures in this section.
- List specific audit controls procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 53
Effective Date: 09-11-13
Last Revised: _____

Data Integrity Controls Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Data Integrity Controls Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs data integrity controls for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to data integrity controls, in accordance with the requirements at § 164.312(c)(1-2).
- The purpose of this Integrity Controls Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) has not been altered or destroyed in an unauthorized manner.
- The establishment and implementation of an effective data integrity controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and maintain this data integrity controls policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this data integrity policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of CITY to fully document all data integrity controls-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Integrity Control Procedures

- ❑ Identify all approved users with the ability to alter or destroy data, if reasonable and appropriate.
- ❑ Implement mechanism to identify all users who have been authorized to access ePHI in conjunction with the identity of any possible unauthorized sources that may be able to intercept the information and modify it.
- ❑ Identify scenarios that may result in modification to the ePHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors).
- ❑ Conduct this activity as part of your risk analysis.
- ❑ Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps.
- ❑ Identify and implement methods that will be used to protect the information from modification.
- ❑ Identify and implement tools and techniques to be developed or procured that support the assurance of integrity.
- ❑ Implement electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
- ❑ Consider possible electronic mechanisms for authentication such as: Error-correcting memory, Magnetic disk storage, Digital signatures and Check sum technology.
- ❑ Review existing processes to determine if objectives are being addressed.
- ❑ Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.
- ❑ List specific data integrity control procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 54
Effective Date: 09-11-13
Last Revised: _____

Person or Entity Authentication Policy

Introduction

CITY OF LOS ANGELES ("CITY") has adopted this Person or Entity Authentication Policy in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This Policy governs person and entity authentication for access to information systems and data, for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to person or entity authentication, in accordance with the requirements at § 164.312(d).
- The purpose of this Person or Entity Authentication Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) can only be accessed by persons or entities who are in fact who they claim to be, and not imposters.
- The establishment and implementation of an effective data Person or Entity Authentication Policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this Person or Entity Authentication Policy, and any procedures associated with it, shall reside with Name of Responsible Party or Person, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper authentication of persons and entities who access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) on our computers, workstations, and systems.
- It is the Policy of CITY to fully document all person or entity-related activities and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Person or Entity Authentication Procedures

- Identify methods available for authentication. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed. (45 CFR §164.304)
- Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that he or she has been authorized for specific access privileges to information and information systems.
- Weigh the relative advantages and disadvantages of commonly used authentication approaches available:
    - Something a person knows, such as a password,
    - Something a person has or is in possession of, such as a token (smart card, ATM card, etc.),
    - Some type of biometric identification a person provides, such as a fingerprint, or
    - A combination of two or more of the above approaches.
- Select the appropriate authentication method based on the analysis of the four commonly used authentication approaches.
- Implement the methods selected into the operation and activities of City.
- List specific person or entity authentication procedures in this section.
- List specific person or entity authentication procedures in this section.
- List specific person or entity authentication procedures in this section.
- List specific person or entity authentication procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]

Policy Number: 55
Effective Date: 09-11-13
Last Revised: _____

Data Integrity Controls Procedures

Introduction

CITY OF LOS ANGELES ("CITY") has adopted these Data Integrity Controls Procedures in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

These procedures govern data integrity controls for CITY, a Hybrid Entity, as well as each and every designated Health Care Component part of CITY.

All personnel of CITY must comply with this Policy. Demonstrated competence in the requirements of this Policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, trainees and volunteers must read, understand, and comply with this Policy.

Assumptions

- CITY hereby recognizes its status as a HYBRID ENTITY.
- The designated HEALTH CARE COMPONENTS of CITY hereby recognize their status as HEALTH CARE COMPONENTS of CITY under the definitions contained in the HIPAA regulations.
- CITY must comply with HIPAA and the HIPAA implementing regulations pertaining to data integrity controls, in accordance with the requirements at § 164.312(c)(1-2) and § 164.312(e)(1-2).
- The purpose of these Integrity Controls Procedures as with our Integrity Controls Policy, is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) has not been altered or destroyed in an unauthorized manner.
- The establishment and implementation of an effective data integrity controls procedures is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy

- It is the Policy of CITY to establish and maintain these data integrity controls procedures in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of these data integrity procedures, as with our Data Integrity Controls Policy, shall reside with Name of Responsible Party or Person, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- Specific integrity control procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of CITY to fully document all data integrity controls-related procedures, activities, and efforts, in accordance with our Documentation Policy. [See Policy No. 3]

Specific Integrity Control Procedures

- ❑ List specific data integrity control procedures in this section.
- ❑ List specific data integrity control procedures in this section.
- ❑ List specific data integrity control procedures in this section.
- ❑ List specific data integrity control procedures in this section.
- ❑ List specific data integrity control procedures in this section.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this Policy. Employees who violate this Policy are subject to discipline up to and including termination in accordance with the Sanction Policy of CITY. [See Policy No. 18]