



**RESOLUTION NO. 2017-07**

**A RESOLUTION OF THE CITY COMMISSION OF THE CITY OF SWEETWATER, TEXAS, ADOPTING HIPAA PRIVACY AND SECURITY POLICY AND PROCEDURES AND DESIGNATING A HIPAA OFFICER AND AN INCIDENT RESPONSE TEAM.**

**WHEREAS**, The City of Sweetwater is considered a covered entity under the Federal Government's Health Insurance Portability and Accountability Act of 1996, codified at 42 U.S.C. § 300gg, 1181 et. seq. and 1320d et. seq.; and

**WHEREAS**, The City Commission adopts the City of Sweetwater HIPAA Privacy and Security Policy and Procedures which establishes basic provisions for implementation of the HIPAA rules within the City of Sweetwater; and

**WHEREAS**, pursuant to 45 CFR § 164.308(a)(2) the City Commission of the City of Sweetwater is required to "identify a security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associates" and those responsibilities relate directly to electronic information security. ; and

**WHEREAS**, the City Commission of the City of Sweetwater believe that it is necessary to designate the Human Resources Director of the City of Sweetwater as HIPAA Privacy Officer and the Information Technology Director as HIPAA Security Officer and vest in these positions the authority to appoint an Incident Response Team that will have the authority to make administrative policies related to the security of information systems in all forms as required by law.

**NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF SWEETWATER, TEXAS, THAT:**

**SECTION 1.** The City Commission hereby approves the City of Sweetwater HIPAA Privacy and Security Policy and Procedures to identify and implement safeguards that comply with and carry out the standards and implementation specifications in the HIPAA Security Rule.


**SECTION 2.** The City Commission designates the Human Resources Director of the City of Sweetwater as HIPAA Privacy Officer and the Information Technology Director as HIPAA Security Officer in accordance with 45 CFR § 164.308(a)(2).

**SECTION 3.** The City Commission gives authority to the HIPAA Privacy and Security Officers to appoint the Incident Response Team to be comprised no less of themselves and Directors of Emergency Medical Services and Senior Nutrition Activities Program, and any staff deemed necessary; and,

**SECTION 4.** That this Incident Response Team is the delegated authority to create, maintain and implement policies, procedures and standards applicable to the City of Sweetwater's information systems, for the purpose of safeguarding electronic information and other forms of protected information, in a manner consistent with all applicable laws and regulations.

**DULY PASSED AND APPROVED** by the City Commission of the City of Sweetwater, Texas, this 11th day of April 2017.

**APPROVED:**

  
\_\_\_\_\_  
Jim McKenzie, Mayor

**ATTEST:**

  
\_\_\_\_\_  
Patty Torres, City Secretary

# **City of Sweetwater**

## **Emergency Medical Service (EMS) and Senior Nutrition Activities Program (SNAP)**

### **HIPAA Privacy and Security Policy and Procedures**

#### **I. Assignment of HIPAA Privacy/Security Officers**

The City Commission of the City of Sweetwater has designated The Human Resources Director as the HIPAA Privacy Officer along with the Director of Information Technology as HIPAA Security Officer, and Directors of Emergency Medical Services and Senior Nutrition Activities Program as key decision makers of the City of Sweetwater's HIPAA Incident Response Team, and has authority to establish, implement, and enforce these policies and procedures for the security and privacy of our patient, client, employee, and volunteer protected health information and personal identification information (PHI/PII).

#### **II. Risk Assessment**

HIPAA Officers are responsible for conducting annual HIPAA privacy and security risk assessment. The assessment will be completed with the assistance of the entire HIPAA Incident Response Team.

Additional risk assessments and notification to HHS within 60 days may be necessary each time (1) new software or hardware is acquired and placed in service; (2) when a new service or procedure is initiated; (3) when there is a significant change in an existing service or procedure; or (4) when there is a change or addition to the physical layout of the offices concerned.

The HIPAA Officers will periodically but at least quarterly review the DHHS's HIPAA website to determine if there have been any changes in the HIPAA rules and regulations and to determine if any changes or modifications to this policy and its procedures are necessary due to changes in HIPAA rules, regulations or regulatory interpretations.

#### **III. Policy regarding physical access to building**

##### ***Senior Nutrition Activities Program:***

Employees access the building via main entrance or employee entrance. All full-time employees, the part-time office clerk, and the janitor have a key to the front door. Only full-time employees and the janitor have personal codes to disarm the security system to enter the building. Only the Director, secretary, and office clerk have the keys to the Director's office containing the patient, client, employee, and volunteer PHI and PII. Security system activity is tracked and a record made showing which employee disarmed the system each day and the time the system is armed at the end of the day. The main

entrance and all exit doors are locked after hours and unlocked each morning at 8:00 a.m. when office staff arrives. Other part-time kitchen staff enter through the kitchen door after 8:00 a.m.

***Emergency Medical Services:***

Employees access the fire station building via secured entrances using an electronic key fob. Visitors are only allowed in by employees after identification. Security system activity is tracked and a record made identifying the employee unlocking the door each time. Eight security cameras monitor and record all entries into building and administration office entrances. The fire station is open twenty-four hours a day, seven days a week. Only the officers and insurance administrative staff have access to the patient PHI/PII. Administrative offices are never left unattended and computers containing access to patient PHI/PII are locked and secure using HIPAA compliant passwords. The computer serving the administrative system is securely locked. The only keys to the server are in possession of the Emergency Medical Services Director and the Information Technology Director. Both are members of the HIPAA Incident Response Team.

**IV. Policy regarding confidentiality of all forms of Protected Health Information (PHI) and Personal Identifying Information (PII)**

All PHI or PII regardless of its form, mechanism of transmission, or storage is to be kept confidential and use is kept to the minimum necessary to fulfill the authorized purposes. Only individuals with a business need to know are allowed to view, read, or discuss any part of a patient, client, employee, or volunteer's PHI/PII. During initial new hire or volunteer orientation and at annual HIPAA training, employees and volunteers are reminded that any viewing, reading, or discussions of PHI/PII that is not for authorized business purposes is prohibited. An employee or volunteer who violates this confidentiality policy will be subject to sanctions up to immediate termination or dismissal. All employees and volunteers are required to verify in writing that they have read and will comply with City policy regarding confidentiality of all forms of PHI/PII.

Access to office where HIPAA files and computer systems are kept secure. Director, secretary, or authorized office personnel are required to close and lock office door upon exiting. These offices are never to be left unattended.

To further limit unauthorized access, Director and any authorized personnel are to lock computers before exiting their workspace.

**V. Policy regarding security of oral, written or electronic PHI/PII (e-PHI/PII)**

Authorized Purpose means the specific organization's mission and purpose or purposes described in the Scope of Work of the SNAP Base Contract with HHS.

Authorized User means a person:

1. Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential information pursuant to the DUA;
2. For whom the City warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and
3. Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the confidential information as required by this Data Use Agreement (DUA).

Only employees, whose job functions require access to City computer systems with PHI/PII located on them, will be given a secure, unique password to access the system. Volunteers do not have access to computer systems, files or unattended offices. Volunteers have only bare minimum personal identification information required to complete the necessary organization's tasks.

Access to any information in any form will be immediately terminated for employees or volunteers who leave City of Sweetwater employment or workforce.

All PHI/PII transmitted to third parties will be transmitted on secured lines. The security of transmission lines will be verified via contract with third party responsible for transmitting our patient or client's PHI/PII.

No digitally stored PHI/PII shall leave this facility without being first encrypted; this includes laptops, flash drive devices, CDs, and e-mail.

It is strictly prohibited for anyone to use, disclose, create, maintain, store or transmit HHS Confidential Information outside of the United States of America.

#### **VI. Cooperation with Federal or State Agencies**

The City requires cooperation with HHS agencies or federal and state regulatory inspections, audits or investigations related to compliance with the DUA or applicable law.

#### **VII. Patient/Client request for accounting of all disclosures made by the City of Sweetwater to authorized service providers**

Patients and clients, only after positive identification, have a right to request their own personal information and an accounting of all disclosures of their PHI/PII made by the City of Sweetwater to any authorized service provider or agency. When a patient or client makes such a request, it must be in writing

and addressed to the appropriate City Director who then will process the request in a timely manner. The patient or client will then be told when the information will be available and given the option of waiting for information by mail or returning to pick-up the data.

### **VIII. Patient or client request for restriction of PHI/PII paid for “out of pocket”**

#### *Emergency Medical Services*

Patients who pay for ambulance service out of pocket (fully paid for by patient with no reimbursement or additional payment by a third party), have a right to have all information regarding such services held confidentially and not released to third parties. To exercise this right the patient must (1) pay for EMS service and (2) make known to the City of Sweetwater their desire to have information regarding the EMS service held in confidence and not released to third parties. Any employee who receives such a request must immediately inform the Insurance Administrator in writing who will flag the information as being restricted.<sup>1</sup> HIPAA allows for the release of restricted PHI/PII (1) in compliance to a subpoena; (2) in compliance to statutory reporting requirement; or (3) upon receiving an unrestricted, HIPAA compliant authorization for release of medical records from the patient, patient’s legal representative, or executor of deceased patient’s estate.

#### *Senior Nutrition Activities Program*

Although some clients do pay for nutrition services, no one fully pays for the service and the additional expense is covered by grant funding and the City of Sweetwater general operating funds.

### **IX. Policy regarding charges for copies of personal client or patient records**

The Privacy Rule permits the Covered Entity (a healthcare or service provider) to impose reasonable, cost-based fees for paper copies.

According to HITECH the covered entity may charge for the labor cost of making the copies or e-copy. This does not include the cost for searching the data base to find appropriate medical record(s).

### **X. Business continuity**

The City of Sweetwater has an approved Emergency Management Plan in place in the event of a disaster. Departments within the City also maintain their own Disaster Preparedness Recovery Plans for their concerned patients and participants.

#### *Overview:*

The City is to ensure that in the event of a disaster, the City as an organization will survive and be able to resume operations and ongoing

---

<sup>1</sup> This contemplates development and implementation of appropriate software programming with your electronic medical records (EMR) vendor.

services to its citizens including but not exclusive to water, sanitation, public safety, ambulance, and SNAP nutrition services to its clients as soon after the occurrence as possible.

*Purpose of the Plan:*

- Outline procedures for employees to use as a guide as they respond to a disaster.
- Ensure employees, volunteers, and citizens are not in “harm’s way”.
- Minimize or eliminate loss of resources.
- Minimize disruption in operations and provide for an orderly resumption of “business as usual”.
- Necessary supplies of medical, nutrition, and structure resources are maintained in amounts to sustain operations for up to two weeks.

**XI. HIPAA Incident/Breach Investigation**

Any incident in which the privacy/security of an EMS patient’s or SNAP client’s PHI/PII may have been compromised will be immediately reported to appropriate director and the HIPAA Privacy and Security Officers. An incident investigation will be initiated without unreasonable delay. The HIPAA Officers will establish an Incident Response Team (IRT) to investigate incidents and determine if the incident rises to the level of a breach. Refer to definition of IRT in Addendum II, page 10. The procedure for conducting HIPAA incident/breach investigation is located in Addendum II, page 13.

**XII. Sanction Policy**

Staff and volunteers exposed to confidential information regarding those we serve or supervise or with whom we work will receive training regarding the City of Sweetwater’s policy for sanctioning employees and volunteers who violate our HIPAA privacy/security policy. Training will be prior to assuming work duties and annually thereafter.<sup>2</sup>

Employees or volunteers through course of business who gain confidential information regarding those we serve or supervise may not take advantage of such information for personal gain nor may such information be disclosed to anyone, except as required by the employee’s position. Confidential information will not be disclosed to third parties without staff, patient, or client written consent and management approval.

Disciplinary action may include any or all of the following four steps: 1) Verbal reprimand, 2) Written reprimand, 3) Suspension with or without pay, or 4) Termination of employment. Taken into consideration will be the seriousness of the problem and the frequency and or length of time it has been a problem when deciding which steps are most appropriate. There may be

---

<sup>2</sup> Note: HIPAA requires “periodic” training but does not specify the time frame—annually is recommended by most HIPAA Officers.

circumstances when one or more steps are bypassed. In long term or very serious situations, some types of employee problems may justify either an immediate suspension, or in extreme situations, termination of employment, without going through the usual progressive disciplinary steps.

### **XIII.Document Retention Policy**

- a. All HIPAA documentation of terminated patient, client, employee, or volunteer such as policy and procedures, risk assessment, incident investigation, breach notification, and training records will be maintained for at least seven (7) years<sup>3</sup> according to the HIPAA records and documentation section of this policy.
- b. Such records, as described above, are maintained in a secure locked City compartment or storage area with access limited to Director or responsible authorized person. After seven year retention period, documentation is shredded by Director or responsible authorized person.
- c. As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI/PII before it is stored or exchanged. De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members.
- d. Re-identification of confidential information is when a cross reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

---

<sup>3</sup> City of Sweetwater Standard (Documentation) (Time Limit)



e. PHI or PII includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual such as dates of birth, marriage, death, etc.
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

## **Addendum I**

### **HIPAA FAQs**

[www.hhs.gov/ocr/privacy/hipaa/faq](http://www.hhs.gov/ocr/privacy/hipaa/faq)

**If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?**

**Answer:**

The Privacy Rule permits the covered entity to impose reasonable, cost-based fees. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive a summary or explanation of his or her protected health information, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information. See 45 CFR 164.524.

Date Created: 12/20/2002

Last Updated: 03/14/2006

[Accessed 9/22/2010 RK]

---

## Addendum II

# City of Sweetwater Emergency Medical Service (EMS) and Senior Nutrition Activities Program (SNAP)

## HIPAA Incident/Breach Investigation Procedure

### I. Purpose

To distinguish between (1) cases in which the City of Sweetwater HIPAA policy was not correctly followed but such violation did not result in the unauthorized release of protected health information (PHI/PII) (referred to as a HIPAA incident) and (2) cases involving the unauthorized release of PHI/PII and said release resulted in or is reasonably expected to result in financial, reputational or other harm to the patient or client. This investigation procedure outlines the process for contacting the patient or client and identifying risk management measures to mitigate identified risks.

### II. Definitions

Breach is the unauthorized acquisition, access, use or disclosure of PHI/PII in a manner not permitted by HIPAA regulations which compromises the security or privacy of the PHI/PII and poses a significant risk of financial, reputational, or other harm to the patient or client except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. (Also see definition of incident and reportable breach).

Breach Notification is a HIPAA requirement in which the Covered Entity (CE) that has experienced a breach must notify the patient or client that the privacy or security of their PHI/PII has been compromised.

Business Associate (BA) is a business organization but not an employee of the CE that performs or assists in the performance of activity involving the use or disclosure of individually identifiable health information; for example, claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management or practice management.

Commercial Supplier (CS) is a business organization that provides services to a CE. While said services do not require CS to directly handle or impact PHI/PII, their presence in the CE's facility may cause or allow them to come in contact with PHI/PII. A janitorial service is an example of a commercial supplier.

Commercial Supplier agreement is a signed contract or memo of understanding between the CE and commercial supplier explaining the CS's duty to avoid PHI/PII and provides assurances that the CS will instruct their employees regarding their duty to

avoid viewing, reading, copying or otherwise obtaining information relating to patients and clients PHI/PII.

Covered Entity (CE) is a healthcare provider, a health plan, or a healthcare clearinghouse.

e-PHI/PII is individually identifiable patient healthcare information created, stored or transmitted in electronic format.

Health Information is any information, whether oral or recorded in any form or medium, that: (1) is created or received by a healthcare provider, health plan, public health authority, employer, and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

HIPAA Officer is the individual formally assigned the duty to establish, implement, and monitor the CE's HIPAA policy and procedures. In small CEs both the Privacy and Security regulations could be handled by one individual, whereas in a large CE one individual may be assigned as the CE's HIPAA Privacy Officer and a second individual assigned as the CE's HIPAA Security Officer.

Incident is an actual or suspected unauthorized release, loss, or destruction of PHI/PII but upon complete investigation it is determined by the Incident Response Team that the incident does not represent a significant risk of financial, reputational, or other harm to the individual.

Incident Response Team (IRT) is composed of members of the CE's staff including at least one key individual with decision making authority. The team is responsible for investigating the actual or suspected unauthorized access, release, or destruction of PHI/PII; making the determination as to whether or not (1) the incident did in fact occur, (2) whether or not the incident rises to the level of a breach, (3) identifying appropriate Risk Management interventions to prevent similar re-occurrence, (4) assuring appropriate individuals are notified, and (5) assuring appropriate reports are made to Department of Health and Human Services (DHHS) when breach occurs.

Individually Identifiable Health Information is any protected health information about an individual that can possibly be used to identify that individual and connect him/her to the health information.

Notification the contacting of individual(s) (or if deceased-next of kin or executor of estate) who is the subject of the unauthorized disclosure, release, loss or destruction of their PHI/PII. Notification is required when the incident is determined to rise to the level of a breach.

Office of Civil Rights (OCR) is the Federal agency authorized by DHHS to investigate claims of HIPAA Privacy or Security breaches.

Protected Health Information (PHI/PII) individually identifiable health information created, transmitted or maintained by CE or BA that (1) identifies the individual or offers

a reasonable basis for reconstructing said identity, (2) is created, received, maintained or transmitted by the CE or BA, and (3) refers to a past, present or future physical or mental condition, healthcare treatment, or payment for healthcare.

Reportable Breach is a HIPAA incident that rises to the level of a breach. A HIPAA breach requires the CE to notify the patient or client, log the breach and report all such breaches to DHHS annually—If 500 or more individuals are involved in a given breach then special notification/reporting requirements apply.

Risk Analysis is the process by which the CE attempts to (1) identify all ways in which an unauthorized release, loss, access, or destruction of PHI/PII could occur; (2) determine what risk management protections are currently in place to minimize the likelihood of the identified risk occurring; (3) assess the current level of risk management protections for each identified risk; (4) recommend additional privacy or security safeguards as needed; (5) review DHHS's website for breach events at other CEs that might suggest weaknesses in CE's privacy/security safeguards; and (6) assess adequacy of HIPAA training for CE's staff.

Sanction Policy is CE's written employee disciplinary policy that outlines the consequences of an employee's violation of the CE's HIPAA Privacy and Security policy and procedures. The sanction policy clearly states that the CE retains the right to immediately terminate an employee for what the CE determines to be an egregious violation of the CE's HIPAA Privacy or Security policy/procedures.

Unsecured PHI/PII is PHI/PII that is not secured through the use of a technology or methodology specified by HIPAA/HITECH rules or regulations. Generally it would be e-PHI/PII not secured by encryption, paper or other media containing PHI/PII that has not been shredded or destroyed in a manner that would prevent it from being reassembled.

### **III. Acquiring Knowledge of Actual or Suspected Breach:**

There are many ways in which we may become aware of an actual or suspected breach.

1. HIPAA training is a major key to the early discovery of a suspected or actual breach. Early detection will often prevent an incident from becoming a reportable/notifiable breach. As part of HIPAA training all staff will be instructed to report any actual or suspected breach to the appropriate department head or HIPAA Officer as soon as it is discovered or suspected.
2. Business Associate may cause or become aware of a breach and inform us.
3. Another CE may become aware of an actual or suspected breach and inform us.
4. The patient or client may become aware of an actual or suspected breach and inform us.

5. We may discover an actual or suspected breach while performing an audit of our HIPAA privacy/security policy and procedures.
6. We may be informed by the Office of Civil Rights that a complaint has been filed against us.

The City of Sweetwater will investigate all incidents we become aware of to determine if a breach did in fact occur; to determine steps necessary to mitigate possible damage to patient; to determine risk management interventions necessary to prevent such incidents from reoccurring; and, to provide appropriate notification to patient and report to Department of Health and Human Services (DHHS).

#### **IV. Unsecured PHI/PII—Exceptions & Safe Harbors**

HIPAA allows for two **exceptions** and three **safe harbors** for the unauthorized release of PHI/PII in which breach notification is not required. The following **exceptions** are allowed:

(1) when unauthorized access or use of PHI/PII is unintentional and is made by an employee working within the scope of their job in which they would normally be expected to access or use PHI/PII and such access is not continued, enlarged or disclosed by said employee; and

(2) an unintended or accidental disclosure is caused by an employee who is authorized to access, use or disclose PHI/PII at the facility in which they work (our employee) who sends or causes to be sent PHI/PII to another individual of another program and/ facility who is also authorized to access, acquire or use PHI/PII at their facility (an employee of another facility or other CE) provided the second employee agrees to return or destroy PHI/PII and agrees not to disclose or further access PHI/PII.

The three **safe harbors** are:

(1) The unauthorized release of e-PHI/PII but the e-PHI/PII is protected by encryption;

(2) The media on which the PHI/PII was stored has been destroyed: (a) paper, film or hard copy media destroyed via shredding, incineration or, for digital/video media, destroyed in such a manner that the PHI/PII cannot be reconstructed (For example; cutting CD into small parts), (b) electronic media destroyed or rendered un-retrievable in a manner consistent with NIST Special Publication 800-88, Guide to Media Sanitization; or,

(3) The unauthorized release consisted of health information that was completely de-identified—removal of all names, addresses down to zip code, social security numbers, date of birth, phone numbers, case numbers or any other data that might be used to trace back and identify the individual.

Unauthorized releases that fall under these exceptions or safe harbors are not considered as a breach and do not require notification of patient or reporting to DHHS.

## **V. Incident Response Team (IRT):**

City of Sweetwater has established an Incident Response Team and charged it with the responsibility of investigating HIPAA incidents. The team is composed of at least one key decision maker, i.e., an individual who is authorized by the organization to make key decisions relative to organizational policy and expenditure of organizational funds, and at least two employees one of whom has line (as opposed to management) responsibility. The following individuals are members of the City of Sweetwater Incident Response Team:

1. Human Resource Director [HIPAA Privacy Officer]
2. Information Technology Director [HIPAA Security Officer]
3. Emergency Services Director [Key Decision Maker]
4. Director of Senior Nutrition Activities Program [Key Decision Maker]

## **VI. Procedure**

Distinguish between a HIPAA incident and a breach. Breaches of PHI/PII would require notification of patient and client and inclusion in the annual report to DHHS. If breach involves 500 or more individual patients then DHHS must be immediately notified and public news media must be advised.

1. First determine if the incident/breach falls within one of the exceptions or safe harbors allowed by HIPAA
  - i. If Yes, document and close file
  - ii. If No, move to # 2.
2. Second determine if there has been an impermissible use or disclosure of PHI/PII under HIPAA rules.
  - i. If No (there has not been an impermissible use or disclosure of PHI/PII), document rationale and close file. For example, the incident falls under the "Oops!" category or a case in which the individual would not reasonably be able to retain the PHI/PII, such as a visitor glancing at a computer screen containing PHI/PII.
    1. Documentation should include date, time and names of Incident Response Team members as well as a brief description of the incident and the reason it was determined the incident was not an impermissible use or disclosure of PHI/PII under HIPAA rules. Include any FAQ from DHHS's website that was used to support final decision as well as citation to any HIPAA rules or regulations used to make the determination.

2. Refer to XI, page 16, Note Regarding Determination of Incident vs. Breach
  - ii. If Yes, move to 3.
3. Third, determine if the impermissible use or disclosure compromises the security or privacy of the PHI/PII, i.e., there is a significant risk of financial, reputational, or other harm to the individual.
  - i. If No (this was an incident that did not rise to the level of a breach), document your rationale, record this as a HIPAA incident, and close file.
    1. Documentation should include date, time and names of Incident Response Team members as well as a brief description of the incident and the reason it was determined the incident was not an impermissible use or disclosure of PHI/PII under HIPAA rules. Include any FAQ from DHHS's website that was used to support final decision as well as citation to any HIPAA rules or regulations used to make the determination.
    2. Determine and document why our policy, procedures, or training failed to prevent this incident and what risk management intervention(s) was taken to prevent similar occurrences.
    3. Include this incident in our annual risk assessment for ongoing review and monitoring.
    4. If changes were made to office policies or procedures as part of risk management intervention subsequent to incident, train all employees, owners, and business associates as needed and document training.
    5. Refer to XI, page 16, Note Regarding Determination of Incident vs. Breach
  - ii. If Yes (Breach did occur)
    1. Complete investigation as soon as possible
    2. Determine cause of breach—why our HIPAA policy and procedures failed to prevent the breach from occurring, not just who caused the breach. For example: Breach occurred due to failure to follow procedure arising from failure to train employee before assigning her to job; failure of BA to follow BA agreement; or failure of computer firewall due to outdated technology.



3. Identify corrective action(s) (risk management interventions) to be taken to address failure(s) including sanction for employee(s) if appropriate.
4. Notify patient or client as per VII below
5. Log breach for end of year reporting to DHHS
6. Include failure in annual risk assessment

## **VII. Notification of Patient or Client**

When the Incident Response Team determines that there has been an unauthorized disclosure of a patient's or client's PHI/PII, and it rises to the level of a breach, then the patient or client must be notified. Notification will be made as soon as the determination of an unauthorized disclosure is made and appropriate investigation has been completed, but no later than 60 days from discovery. It is expected that the notification will be completed as soon as possible - once discovery and appropriate investigation is completed the notification will be made at that time without waiting for the running of the sixty day maximum limit. In addition, if the situation is deemed urgent by the Incident Response Team, notification to the patient or client will be made immediately without waiting for full investigation. Urgent notification will be made, if possible, via phone. Non-urgent notification will be provided as follows:

1. Written notification provided via first class mail with copy of letter placed in patient's medical record. Said notification mailed to last known address. If patient or client has given prior approval for communication via e-mail then notification may be made via e-mail. Additional mailings may be required as additional information is obtained.
2. If individual is deceased then notification will be mailed to next of kin or executor of estate.

## **VIII. Business Associate Notification**

If a Business Associate (BA) becomes aware of a breach caused by the BA, our written BA agreement requires the BA to notify us immediately. Our Incident Response Team will conduct the investigation to determine if impermissible disclosure occurred, how to notify the patient or client, and what steps should be taken to prevent similar incident/breach from reoccurring.

## **IX. Delay of Notification Requested by Law Enforcement**

Notification may be delayed if law enforcement official determine that notification would impede a criminal investigation or endanger national security. The delay request must be in written form and identifies the law enforcement official making the request. The delay can be for no more than 30 days unless a written request for a specific extension is made within the initial 30 day extension by a law enforcement official.

## **X. Elements of the Written Notification**

The patient's or client's written notification of a breach involving their PHI/PII will contain:

1. A short description of how the breach occurred; when it occurred; when we discovered the breach
2. An explanation of the type of PHI/PII involved in the breach such as patient or client name (full or partial), diagnosis, treatment, lab/test results, social security number, date of birth, patient's address, account or case number and/or financial data such as credit card numbers
3. Our recommendation(s) to the patient or client as to the steps he/she should take to protect themselves from identity theft or the unauthorized use of their medical insurance accounts
4. An explanation of what we are doing to prevent re-occurrence of such breaches
5. Information the patient or client may use to contact us if they have further questions

## **XI. Note Regarding Determination of Incident vs. Breach**

If, after an appropriate investigation has been conducted, it is determined that the incident did not rise to the level of a breach, we have the burden of proof, i.e., we must be able, if required at a later time, to demonstrate to DHHS or OCR that the impermissible use or disclosure did not constitute a breach, and therefore we were not required to notify the patient or client and include incident in our annual report of breaches to DHHS. Appropriate documentation of the investigation and the rationale used to make our non-breach (incident) determination will be maintained for at least six years after the initial non-breach finding. To demonstrate due diligence regarding our desire to comply with HIPAA requirement, we will document all changes in policies/procedures and/or additional staff training that resulted from our investigation into the incident. We will also include the incident in our annual risk assessment.

# **Addendum III**

## **City of Sweetwater**

### **HIPAA Privacy and Security**

#### **SANCTION GUIDELINE**

##### **Legal and Ethical Duty**

Healthcare providers, employees, consultants, business associates and others who have a business reason to create, maintain, view, or transmit confidential data relative to patient or client's medical care have a legal and ethical duty to maintain the privacy, security and confidentiality of such medical information. Violation of this duty will result in sanctions being imposed on the responsible party.

##### **Federal Privacy and Security Legal Requirements**

City of Sweetwater requires all employees, as a condition of employment, to receive training regarding their responsibility relative to HIPAA privacy and security standards. All staff must follow established privacy and security policies to ensure the confidentiality, integrity, and availability of all protected health information. All individuals having access to protected health information (PHI/PII) are required to read, sign, and comply with this organization's privacy and security policy. By signing the privacy and security policy staff acknowledges that both the City of Sweetwater and the staff member have a legal duty to comply to the best of their ability with the privacy and security policy.

##### **Sanctions for Breach of Privacy and Security Policy**

Staff who, without a business "need to know," unintentionally or carelessly views or accesses PHI/PII is subject to an initial verbal warning. This warning is given with an additional warning that repeat of this or similar offense will result in further disciplinary action not to exclude suspension without pay or immediate termination of employment.

Staff who, without a business "need to know," unintentionally or carelessly views or accesses PHI/PII and then relates portions of the PHI/PII to another individual is subject to an initial written warning. This warning is given with an additional warning that repeat of this or similar offense will result in further disciplinary action not to exclude suspension without pay or immediate termination of employment.

Staff who, without a business need to know, intentionally views or accesses PHI/PII to satisfy personal desire to learn details regarding a patient or client's PHI/PII is subject to immediate termination of employment.

Staff who views or access PHI/PII with malicious intent or desire for personal gain is subject to immediate termination of employment.

**Non Retaliation Policy**

Staff who, in good faith and belief that a privacy or security policy has been violated, reports such concern to the appropriate department head or City of Sweetwater HIPAA Privacy/Security officer shall not be subject to retaliation, harassment, or intimidation as a result of such communication to said officials. Should staff believe he/she is being harassed by the individuals serving as HIPAA Officials, the staff should report situation to the City Manager.

Date Policy Created/Approved 4-11-17

Date Policy Reviewed/Revised \_\_\_\_\_

Date Policy Reviewed/Revised \_\_\_\_\_

Date Policy Reviewed/Revised \_\_\_\_\_

Date Policy Reviewed/Revised \_\_\_\_\_

Date Policy Reviewed/Revised \_\_\_\_\_

## Addendum IV:

### **Risk Assessment Form (Example)**

#### Scoring:

0 = Probability – possible, but not likely

1 = Probability - could happen

2 = Probability - likely to happen, but not guaranteed to happen

	<b>Risk</b>	<b>Probability of Occurrence</b>
1	Lost laptop (MD takes unencrypted laptop home)	1
2	Lost paper medical record (Nurse puts lab reports in pocket and waits until end of day to file reports)	2
3	Hacker getting into our system and obtaining e-PHI/PII	1
4	Lost CD or flash drive (MD takes unencrypted flash drives home)	2
5	Break-in and patient or client records stolen (Facility specializes in pain management and is located in a high crime area)	2
6	Patient or client's HIV prescription accidentally broadcast to dozens of fax numbers in the system	0

1. Begin with blank spreadsheet or flip chart and have Risk Assessment Team brainstorm all the possible ways in which the confidentiality of PHI/PII might be breached.
2. List each risk under the risk column, and then as a group assign the probability of the risk occurring at our facility. The brainstorming session should be free-flowing, no bad ideas, be careful that an authority figure does not repress the free flowing of ideas.
3. Take all the "2s" and develop risk interventions that will eliminate or reduce the possibility of the risk occurring. For example; under risk number 2 a policy could be established that all lab reports are filed as soon as they are received; risk number 4 could be reduced to a "0" with the adoption of encryption technology for CDs and flash drives used in the facility; and, risk number 5 could be lowered to a "1" with the addition of better lighting and a monitored security service.
4. Risk number 6 was scored a "0" because the Office Manager had the broadcast function removed prior to putting the software into service.

5. Keep documentation of the meeting to use as a beginning point for next years session; check DHHS's HIPAA web site to determine if other facilities have had breaches that might occur in our facility; perform risk assessment each time new or updated electronic medical records software/hardware is adopted; perform risk assessment any time a new procedure or new clinical technology is adopted; and maintain documentation for at least six years.
6. Keep in mind that the purpose of Risk Assessment is to (1) identify potential risk to PHI/PII, (2) set the priority for addressing identified risks, (3) establish risk management interventions to minimize or eliminate identified risks, (4) test our current risk management interventions to make sure they are still appropriate, and (5) gauge the effectiveness of our HIPAA training.