10

CITY AT THE CENTER
WEST ALLIS

City of West Allis
Matter Summary

7525 W. Greenfield Ave.
West Allis, WI 53214

File Number	Title	Status
R-2010-0068	Resolution	Introduced

Resolution Relative to Adopting a HIPAA Notification of Breach of Unsecured Protected Health Information Policy.

Introduced: 3/2/2010

Controlling Body: Administration & Finance Committee

COMMITTEE RECOMMENDATION adopt

ACTION DATE: MAR 0 2 2010

	MOVER	SECONDER	AYE	NO	PRESENT	EXCUSED
Barczak						
Czaplewski						
Kopplin			✓			
Lajsic	X		✓			
Narlock			✓			
Reinke						✓
Roadt						
Sengstock						
Vitale		X	✓			
Weigel						
TOTAL			4			1

SIGNATURE OF COMMITTEE MEMBER

Kurt E Kopplin
Chair

Vice-Chair

Member

COMMON COUNCIL ACTION ADOPT

ACTION DATE: MAR 0 2 2010

	MOVER	SECONDER	AYE	NO	PRESENT	EXCUSED
Barczak			✓			
Czaplewski			✓			
Kopplin	✓		✓			
Lajsic			✓			
Narlock		✓	✓			
Reinke						✓
Roadt			✓			
Sengstock			✓			
Vitale			✓			
Weigel			✓			
TOTAL			9	—		1

CITY AT THE CENTER
WEST ALLIS

City of West Allis

Resolution

7525 W. Greenfield Ave.
West Allis, WI 53214

File Number: R-2010-0068

Final Action: MAR 0 2 2010

Resolution Relative to Adopting a HIPAA Notification of Breach of Unsecured Protected Health Information Policy.

WHEREAS, the Health Information Technology for Economic and Clinical Health Act (HITECH), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA), mandated breach notification requirements for covered entities when impermissive or unauthorized access, acquisition, use and/or disclosure of unsecured protected health information occurs under the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA).

WHEREAS, the above-referenced regulations require the City of West Allis, as a covered entity, to implement a policy governing discovery, internal reporting and notification when a breach of unsecured protected health information occurs.

NOW, THEREFORE, BE IT RESOLVED by the Common Council of the City of West Allis that the attached HIPAA - Notification of Breach of Unsecured Protected Health Information Policy, with its attachments, be and is hereby approved for inclusion in the City's Policies & Procedures Manual.

BE IT FURTHER RESOLVED that the City Administrative Officer is authorized and directed to include the policy in the City of West Allis Policies & Procedures Manual and to distribute said policies to all departments, divisions, and offices.

ATTR-Resolution-HIPAA Notification of Breach of Unsecured PHI

ADOPTED MAR 0 2 2010

Paul M. Ziehler, City Admin. Officer, Clerk/Treas.

APPROVED 3/9/10

Dan Devine, Mayor

HIPAA –Notification of Breach of Unsecured Protected Health Information Policy | Personnel | 1400

1.0 PURPOSE:

To provide guidance for breach notification by the City of West Allis ("City") when impermissive or unauthorized access, acquisition, use and/or disclosure of unsecured protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

2.0 THE CITYS AFFECTED:

This policy applies to all City of West Allis departments, boards, commissions, officials and employees.

3.0 DEFINITIONS:

Access: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.

Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI. For purpose of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at 45 CFR §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

Breach excludes:

1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.

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

Individually Identifiable Health Information: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Protected Health Information (PHI): Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium, relating to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for health care provided to an individual. Protected health information does not include employment records held by the City in its role as employer.

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals by encryption or destruction.

Workforce: Workforce means employees, officials, board and commission members, volunteers, trainees, and other persons whose conduct, in the performance of work for the City, is under the direct control of the City, whether or not they are paid by the City.

4.0 POLICY:

4.1 Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the City, or, by exercising reasonable diligence would have been known to the City (includes breaches by the City's business associates). The City shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of the City (see attachment for examples of breach of unsecured protected heath information). Following the discovery of a potential breach, the City shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed by the City to have been, accessed, acquired, used, or disclosed as a result of the breach. The City shall also begin the process of determining what external

notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

4.2 Breach Investigation: The City shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the City as appropriate (e.g., administration, information technology, human resources, risk management, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

4.3 Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the City will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The City shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The City has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the City will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
B. The type and amount of PHI involved.
C. The potential for significant risk of financial, reputational, or other harm.

(*See attached Risk Assessment Analysis Tool*)

4.4 Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the City or the business associate involved. It is the responsibility of the City to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

4.5 Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the City that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the City shall:

A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
B. If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

4.6 Content of the Notice: The notice shall be written in plain language and must contain the following information:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
B. A description of the type of unsecured protected health information that was involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the City is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

4.7 Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

A. Notice to Individual(s): Notice shall be provided promptly and in the following form:
   1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the City knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.
   2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
      a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
      b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the City's website, or a conspicuous notice in a major print or broadcast media in the City's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.
   3. If the City determines notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 individuals. The Notice shall be provided in the form of a press release.
C. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list

identifying covered entities involved in all breaches in which the **unsecured** PHI of more than 500 individuals is accessed, acquired, used, or disclosed.

1. For breaches involving 500 or more individuals, the City shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
2. For breaches involving less than 500 individuals, the City will maintain a log of the breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

4.8 Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the City shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of individuals affected. The following information should be collected/logged for each breach (*See attached Sample Breach Notification Log*):

A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.
B. A description of the type of unsecured protected health information that was involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
C. A description of the action taken with regard to notification of individuals regarding the breach.
D. Resolution steps taken to mitigate the breach and prevent future occurrences.

4.9 Business Associate Responsibilities: Any business associate (BA) of the City that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the City of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the City with any other available information that the City is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the City will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity/City to document this notification).

5.0 TRAINING:

The City shall train all members of its workforce having access to PHI on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the City.

6.0 COMPLAINTS:

Individuals have the right to complain about the City's breach notification processes. Said complaints shall be made in accordance with the procedure set forth in Section 1473 of the City's Policies & Procedures Manual (Complaint Procedure Under the HIPAA Privacy Rules).

7.0 SANCTIONS:

Members of the workforce who fail to comply with privacy policies and procedures shall be subject to disciplinary action, up to and including termination.

8.0 RETALIATION/WAIVER:

The City may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for their exercise of any privacy right. The City may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Sample Breach Notification Log

The City shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of individuals affected. A record of the complete investigation of the potential breach as well as the risk assessment carried out to determine notification requirements should be created. The risk assessment and the record/incident report should be cross-referenced so that should the Secretary of HHS require more information, it is easy to locate and provide.

Note: Reconfigure Width of Data Fields for Landscape Document or Spreadsheet

Incident #	Date of Discovery	Date of Breach	Location	Brief Description of Breach*	Number of Individuals Involved	Notification Dates			Actions Taken Resolution Steps
						Individuals	Media	HHS	

- A description of what happened, including a description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).

Risk Assessment Analysis Tool

Note: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule

Q#	Question	Yes - Next Steps	No - Next Steps
	Unsecured PHI		
1	Was the impermissible use/disclosure unsecured PHI (e.g.. not rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary)?	Notifications not required. Document decision.	Continue to next question
	Minimum Necessary		
2	Was more than the minimum necessary for the purpose accessed, used or disclosed?	Continue to next question	May determine low risk and not provide notifications. Document decision.
	Was there a significant risk of harm to the individual as a result of the impermissible use or disclosure?		
3	Was it received and/or used by another entity governed by the HIPAA Privacy & Security Rules or a Federal Agency obligated to comply with the Privacy Act of 1974 & FISA of 2002?	May determine low risk and not provide notifications. Document decision.	Continue to next question
4	Were immediate steps taken to mitigate an impermissible use/disclosure (e.g. Obtain the recipients' assurances the information will not be further used/disclosed or will be destroyed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
5	Was the PHI returned prior to being accessed for an improper purpose (e.g., A laptop is lost/stolen, then recovered & forensic analysis shows the PHI was not accessed, altered, transferred or otherwise compromised)?	May determine low risk and not provide notifications. Document decision. Note: don't delay notification based on a hope it will be recovered.	Continue to next question

What type and amount of PHI was involved in the impermissible use or disclosure?			
6	Does it pose a significant risk of financial, reputational, or other harm?	Higher risk - should report	May determine low risk and not provide notifications. Document decision.
7	Did the improper use/disclosure only include the name and the fact services were received?	May determine low risk and not provide notifications. Document decision.	Continue to next question
8	Did the improper use/disclosure include the name and type of services received, services were from a specialized facility (such as a substance abuse facility), ***or*** the information increases the risk of ID Theft (such as SS#, account#, mother's maiden name)?	High risk - should provide notifications	Continue to next question
9	Did the improper use/disclosure ***not*** include the 16 limited data set identifiers in 164.514(e)(2) ***nor*** the zip codes or dates of birth? Note: take into consideration the risk of re-identification (the higher the risk, the more likely notifications should be made).	High risk - should provide notifications	May determine low risk and not provide notifications. Document decision.
10	Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals (ex. Limited data set included zip codes that based on population features doesn't create a significant risk an individual can be identified)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
Specific Breach Definition Exclusions			
11	Was it an unintentional access/use/disclosure by a workforce member acting under the organization's authority, made in good faith, within his/her scope of authority (workforce member was acting on the organization's behalf at the time), and didn't result in further use/disclosure (ex. billing employee receives an e-mail containing PHI about a patient mistakenly sent by a nurse (co-worker). The billing employee alerts the nurse of the misdirected e-mail & deletes it)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
12	Was access unrelated to the workforce member's duties (ex. did a receptionist look through a patient's records to learn of their treatment)?	High risk - should provide notifications	Continue to next question

13	Was it an inadvertent disclosure by a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same organization, or its OHCA, ***and*** the information was not further used or disclosed (ex. A workforce member who has the authority to use/disclose PHI in that organization/OHCA discloses PHI to another individual in that same organization/OHCA and the PHI is not further used/disclosed)?	May determine low risk and not provide notifications. Document decision.	Continue to next question
14	Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (e.g. EOBs were mistakenly sent to wrong individuals and were returned by the post office, unopened, as undeliverable)?	May determine low risk and not provide notifications. Document decision.	Continue to next question. Note: if the EOBs were not returned as undeliverable, these should be treated as breaches.
15	Was a disclosure of PHI made, but there is a good faith belief than the unauthorized recipient would not have reasonably been able to retain it (ex. A nurse mistakenly hands a patient discharge papers belonging to a different patient, but quickly realized the mistake and recovers the PHI from the patient, and the nurse reasonable concludes the patient could not have read or otherwise retained the information)?	May determine low risk and not provide notifications. Document decision.	Document findings.
Burden of Proof: Required to document whether the impermissible use or disclosure compromises the security or privacy of the PHI (significant risk of financial, reputational, or other harm to the individual).			