WELLNESS CENTER OF MAINE

OPERATIONAL POLICY

Breach Notification Policy

Purpose:

To define the process and protocols for employees to take when a known or suspected breach of confidentiality hasoccurred.

Scope:

This policy applies to all employees (including full-time and part-time employees), contract providers, volunteers,students or interns, of Wellness Center of Maine (WELLCOME) and all consumers served.

Information:

1. On January 17th, 2013, the United States Department of Health and Human Services (HHS) released the Health Information Technology for Economic and Clinical Health (HITECH) Final Rule which further restricts health care providers, health plans, and other Covered Entities (CE) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (45 CFR) to notify individuals when their health information has been breached. These "breach notification" regulations implement provisions of the HITECH Act, passed as part of the American Recovery & Reinvestment Act of 2009 (ARRA).
2. The breach notification provisions of the HITECH Act apply to HIPAA-covered entities and their businessassociates who access, maintain, retain, modify, store, destroy, or otherwise hold, use, or disclose Protected Health Information (PHI) and Electronic Protected Health Information (EPHI).
3. These regulations, developed with the HHS Office for Civil Rights (OCR), require health care providers and otherHIPAA-covered entities to promptly notify affected individuals of a breach of confidentiality, as well as notifying the Health and Human Services (HHS) Secretary and the media in cases where a breach affects more than five hundred (500) individuals. Breaches affecting fewer than five-hundred (500) individuals are to be reported to the HHS Secretary on an annual basis. Since business associates are also covered under the provision of the HITECH Act, all Business Associates (BA) of WELLCOME are also required to notify WELLCOME of any known or suspected breaches of confidentiality.
4. Wellness Center of Maine (WELLCOME) is a covered entity and is required to comply with, including but not limited to, 45 CFR Sections 164.40 - 164.414 concerning breaches of Protected Health Information.
5. Specifically, and according to these provisions, following a discovery of a breach of unsecured PHI, WELLCOME is required to notify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach. (See "Definitions" section below for definition of"unsecured PHI".) Other notifications must also be made as detailed below.
6. All WELLCOME employees receive annual Recipient Rights and Corporate Compliance training which includes training on confidentiality, disclosure, privacy, and security practices, employee code of conduct, breach notification, and employee disciplinary actions/sanctions for non-compliance.
7. Encryption and destruction are technologies and methodologies for rendering PHI/EPHI unusable, unreadable, orindecipherable to unauthorized individuals.

Policy:

A. Safe Harbor from Breach Notification Reporting:

1. Regardless of whether or not something is considered a breach, the HIPAA/HITECH Final Rule establishes a safe harbor for any breach of PHI/EPHI that is encrypted according to federal guidelines. As long as the PHI/EPHI involved in the breach was encrypted, there is no requirement

to provide notification.

B. Individual Notification:

1. Following the discovery of a breach of unsecured PHI, WELLCOME is required to notify the affected consumers (or their next of kin if the consumer is deceased) whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, used, or disclosed in the breach. This notification must occur withoutunreasonable delay but no later than sixty (60) calendar days of the discovery of the breach. (Except when the delay is required by law enforcement officials who determine that a notification would impede a criminal investigation or cause damage to national security.) The notification shall be written in plain language and include, to the extent possible:
    - A brief description of what happened, date of the breach, and date of discovery of the breach, if known;
    - A description of the types of PHI/EPHI involved (e.g. full name, social security number, address, diagnosis,and other types of information involved);
    - Any steps that individuals should take to protect themselves from potential harm as a result of the breach;
    - A brief description of what WELLCOME is doing to investigate the breach, mitigate the cause of the breach, andmitigate harm, as well as to protect against future breaches;
    - Contact procedures for individuals to ask questions or learn additional information, which shall include atoll-free number, an e-mail address, website address, and/or postal address.
2. This notification must be provided in plain language. In general, the written notification should be provided by first-class mail to the last known address of the person (alternatively, written notice may be provided in the formof an e-mail if the individual has agreed to electronic notice and the agreement has not been withdrawn). In situations where WELLCOME believes the possibility exists for imminent misuse of the unsecured PHI, WELLCOME may providenotice of the breach to affected consumers by telephone in addition to the written notice. If the individual is a minor or legally incapacitated, notice to the parent or personal representative is acceptable.
3. If there is insufficient contact information for some or all of the affected individuals or if some of the notices are returned as undeliverable, substitute notice should be provided to the unreachable individuals in a manner reasonably calculated to reach them. For example, if WELLCOME does not have the individual's last known address, but has the individual's e-mail or telephone number, notice can be provided electronically or by phone without theindividual's consent. Posting a notice on WELLCOME's website may also be appropriate.
4. In the case where there is insufficient or out-of-date contact information, WELLCOME will provide substitute notice, including, when there are ten (10) or more individuals for whom there is insufficient contact information, a conspicuous posting on the WELLCOME website for at least ninety (90) days, or a notice in a major print (such as a stateor local newspaper or magazine) or using a broadcast media in the geographic area(s) where the affected individuals are likely reside. The notice must include a toll-free telephone number that remains active for at least ninety (90) days for individuals to call regarding the breach.

C. Media Notification:

1. In addition to notifying affected individuals of the breach, when a breach of unsecured PHI involves more than five-hundred (500) consumers, WELLCOME shall provide notice to appropriate prominent media outlets serving the stateor jurisdiction. This will be done without unreasonable delay following discovery of the breach (in no case later than sixty days after discovery). This would typically be in the form of a press release to appropriate media outlets such as a general interest newspaper with daily circulation covering the area where the affected individuals live. The information required for the notification is defined in B.1 above.

D. Government Notification:

1. **500 or more individuals:** For breaches of unsecured PHI involving five-hundred (500) or more individuals, WELLCOME shall also provide notice to the government within sixty (60) days of the breach, contemporaneously with the notifications to the individuals, in the manner specified on the HHS website. WELLCOME will utilize the HHS electronic report form and the reporting instructions/format specified by HHS @ http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

2. **Less than 500 individuals:** For breaches involving less than five-hundred (500) individuals, WELLCOME shall maintain a record-log and shall report this information to HHS on an annual basis (no later than 60 days after the end of each calendar year). WELLCOME will utilize the electronic report form and the reporting instructions/format specified by HHS @http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

E. Process for Employees when a Suspected or Known Breach of Confidentiality has Occurred:

1. If any WELLCOME employee becomes aware of any issue or matter that could possibly impact WELLCOME's breach notification obligations, the employee must immediately report the information to the WELLCOME CEO/ED using any of the following methods:

    - Phone reporting: Christopher McGary direct line at (207) 717 – 5627
    - In writing to: Wellness Center of Maine
      P.O. Box 29
      Dover Foxcroft, Maine 04426
      Attention:CEO/ED

2. Employees are not expected nor should they attempt to make a determination as to whether an actual breach (asdefined in the "Definitions" section below) has taken place. Rather, employees are expected to report any known or suspected instances where PHI may have been accessed or disclosed inconsistent with the HIPAA privacy and security regulations and WELLCOME's "Minimum Necessary Protocols for External Disclosures Policy" (ORI.1.13) Failure to report a known or suspected breach is a violation of this policy and can result in disciplinary action

3. No employee will be threatened, intimidated, coerced, discriminated against, or have any other retaliatory actiontaken against them for reporting a breach or possible breach.

3. Examples of issues that should be reported for further investigation include, but are not limited to:

    - Access of data/files/records by unauthorized individuals;
    - Access of data/files/records by authorized individuals but for improper/non-business purposes;
    - Disclosure of data/files/records to unauthorized individuals;
    - Disclosure of PHI without an authorization when an authorization is required; and
    - Disposing of PHI such as hardcopy reports or other paper containing PHI without following appropriate destruction protocols (e.g. failure to shred reports prior to disposal)

4. Upon receipt of a report, the Compliance Officer will notify the Executive Director and will conduct an investigation to determine whether WELLCOME has a notification obligation under the regulations.

5. It is also WELLCOME's policy and a requirement of our business associate agreements that all business associates, contract providers, or vendors must report (within forty-eight hours) any breach of confidentiality consistent with this policy.

F. Procedure for Investigating a Breach:

Upon receipt of a report or learning of an issue that may impact WELLCOME's breach notification obligations, the Compliance Officer (and additional staff, as appropriate) shall do the following:

1. **Investigate the Breach**: Conduct an investigation to determine if the matter involved unsecured PHI (as defined in the "Definitions" section below). If the matter involved unsecured PHI, the Compliance Officer, and other staff as appropriate, shall determine whether or not a breach has occurred. The following actions shall be taken by the Compliance Officer and/or other WELLCOME staff:

    a. Determine whether there has been an impermissible use or disclosure under the privacy regulations. The Compliance Officer shall gather and document all relevant facts and circumstances pertinent to the issue andconduct a risk assessment, which includes:

        - the nature and extent of PHI;
        - whether the PHI is individually identifiable;

- the types of identifiers and the likelihood of re-identification;
- the unauthorized person who accessed/obtained PHI or to who the disclosure was made (forexample if the person to whom the PHI was improperly disclosed is another HIPAA-covered entity who is also obligated to protect PHI. In this case there would be a determination that there is a low probability that PHI was compromised);
- whether the PHI was actually acquired or only viewed (for example, a laptop containing unencrypted PHI is lost, but later found and forensic analysis reveals that the PHI was never accessed, thiswould favor a determination that no notification is required), and;
- the extent to which any risk of PHI has been mitigated (if PHI is improperly used or disclosed, WELLCOMEor the business associate should immediately take steps to mitigate any potential risk to the PHI, which would favor a determination that there is a low probability that the PHI was compromised)

b. If there has been an impermissible use or disclosure, WELLCOME must determine and document whether the impermissible use or disclosure compromises the security or privacy of the PHI and is considered to be a reportable breach after conducting the risk analysis (i.e. WELLCOME has determined that there is a high probability that the PHI has been compromised based on a risk assessment) that it poses a significant risk of financial, reputational, or other harm to the individual. Legal counsel should be consulted at this stage. If the risk assessment indicates a low probability of compromise, no notification is required.

c. Determination must be made as to whether or not the breach is deemed excluded. A breach is excluded if:

   - There is an unintentional acquisition, access, or use of PHI by a workforce member or a person acting on behalf of WELLCOME. If such acquisition, access, or use was made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the privacy regulations; or
   - Any inadvertent disclosures by a person who is authorized to access PHI to another person authorizedto access PHI and the information is not further used or disclosed in a manner not permitted under the privacy regulations; or
   - A disclosure of PHI where WELLCOME 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.

     Note that under the regulations, WELLCOME retains the burden of proof to show why the matter falls under one of the above three (3) exceptions. Legal counsel should be consulted when making this determination.

     Note: The Compliance Officer may consult with legal counsel as part of the process to assist in analyzing the issues and in making determinations as to appropriate reporting requirements

d. Conduct post-breach evaluation and remediation.

2. Reporting the Breach:

a. If the results of the investigation reveal that a reportable breach has occurred, the Compliance Officer (and/or other appropriate administrative staff) is required to make notification without unreasonable delay but no laterthan sixty (60) calendar days of the discovery of the breach in accordance with items B, C, and D above.

b. WELLCOME will maintain documentation to demonstrate that all required notifications were made, or alternatively, documentation that notification was not required.

Definitions/Acronyms:

Acronyms:

ARRA – American Recovery and Reinvestment Act
BA – Business Associate
CE – Covered Entity

CFR – Code of Federal Regulations
ePHI – Electronic Protected Health Information
WELLCOME – Wellness Center of Maine
HHS – Health and Human Services
HIPAA – Health Insurance Portability & Accountability Act
HITECH – Health Information Technology for Economic and Clinical Health
PHI – Protected Health Information
PHR – Personal Health Record

Definitions:

Business Associate: A HIPAA business associate is any organization or person working in association with or providing servicesto a covered entity who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR).

Breach: means the unauthorized acquisition, access, use, or disclosure of PHI that compromises the privacy or security of the information. In order for a breach to occur, the acquisition, access, use, or disclosure must be in violation of the HIPAA Privacy Rules and which compromises the security or privacy of consumer's PHI (i.e. a risk assessment has been done to determine if there is a low or high probability of a compromise of the PHI). Note that a breach would not be considered to pose a significantrisk if the PHI at issue does not include certain identifiers. Identifiers in the Privacy Rule (45 CFR) include the following:

- Date of Birth
- Names
- Social Security Numbers
- Case Numbers
- Account Numbers
- Health Plan Numbers
- Addresses (other than town/city or state)
- Certificate/Licensure Numbers
- Vehicle Identifiers
- Telephone Numbers
- Telefax Numbers
- E-mail Addresses
- Full-face Images & comparable images
- Biometric Identifiers
- Internet Protocol Address Numbers
- URLs
- Device Identifiers & Serial Numbers
- Genetic Information

Covered Entity: A HIPAA covered entity is any organization or corporation that directly handles Protected Health Information (PHI) or Personal Health Records (PHR). The most common examples of covered entities include hospitals, doctors' offices, mental health agencies, and health insurance providers.

Encryption: Algorithms that encode plain text into non-readable form providing privacy. The receiver of the encrypted text must use a "key" to decrypt the message which then returns it to its original plain text form. Encryption technology is intended to make PHI private.

Exceptions/Excluded Breach: For the purpose of this policy, it is not considered a breach if:

(a) there is an unintentional acquisition, access or use of PHI by a workforce member or a person acting on behalf of WELLCOME or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the privacy regulations (example: an employee mistakenly sends an e-mail with PHI to another co-worker who opens it in the normal course of business but then deletes it and notifies the first employee); or

(b) an inadvertent disclosure by a person who is authorized to access PHI at WELLCOME or a business associate to another person authorized to access PHI at WELLCOME and the information is not further used or disclosed in a manner not permitted under the privacy regulation; or

(c) a disclosure of PHI where WELLCOME or a business associate 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. (An example would be if WELLCOME sent a record to an incorrect consumer. The document is returned to WELLCOME by the post-office as undeliverable and is unopened. In such a case, WELLCOME can conclude that the incorrect addressee could not have retained the PHI.)

Note that under the regulations, WELLCOME retains the burden of proof to show why the matter falls under one of the above three
(3) exceptions.

Genetic Information: relates to genetic tests of the person or peros family members, the manifestation of a disease or disorder in the person's family members, or any requests for receipt of genetic services, or participation in clinical research which includes genetic services, by the person or any family member of the person.

Intimidating or Retaliatory act: to demote, terminate, withhold pay, or suspend a person for filing a complaint, participating in an investigation, or opposing any unlawful act related to HIPAA privacy and security breach notification.