BREACH NOTIFICATION POLICY

1. **POLICY.** Christian Community Homes and Services, Inc. ("CCHS") complies with the regulations for Breach Notification for Unsecured Protected Health Information published in the Federal Register on January 25, 2013 as part of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This Policy sets forth the procedures CCHS will use to determine if an impermissible or unauthorized access, acquisition, use or disclosure of CCHS's protected health information ("PHI") is a breach for which notification to the affected individual(s) is required under HIPAA.

2. **SCOPE OF APPLICATION.** This Policy applies to CCHS and all of its subsidiaries and affiliates. For purposes of this Policy, references to CCHS shall be deemed to include Christian Community Home of Hudson, Christian Community Home of Osceola, Hearthside Assisted Living, WinterGreen Senior Apartments, and Pine Ridge Assisted Living.

3. **DEFINITIONS.** Capitalized terms not otherwise defined in this Policy shall have the meanings given to them in HIPAA.

   (a) "Access" means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.

   (b) "Breach" means the acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the Unsecured PHI. Breach excludes:

      (i) Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of a CCHS or its business associate 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.

      (ii) Any inadvertent disclosure by a person who is authorized to access CCHS's PHI (whether a Workforce member, business associate, business associate workforce member or other authorized party) to another person authorized to access CCHS's PHI, 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.

      (iii) A disclosure of PHI where CCHS or its business associate has a good faith belief that the unauthorized person or entity to whom the disclosure was made would not reasonably have been able to retain such information.

   (c) "Disclosure" means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

(d) "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. parts 160 and 164, Subparts A and E, as currently in effect.

(e) "Unsecured PHI" means that PHI of CCHS which is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the Department of Health & Human Services ("HHS") in the guidance issued under section 13402(h)(2) of Pub. L.111-5 and available on the HHS website: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

(f) "Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for CCHS or a business associate of CCHS, is under the direct control of CCHS, whether or not they are paid by the CCHS or its business associate.

4. PROCEDURES.

(a) Discovery of Impermissible or Unauthorized Acquisition, Access, Use or Disclosure of Unsecured PHI. All Workforce members and business associates are required to report immediately the discovery of any potentially impermissible or unauthorized acquisition, access, use or disclosure of Unsecured PHI. Reports shall be made to: (1) the Director of Operations for CCHS' Hudson campus (for issues relating to the Hudson campus) or (2) the Administrator of CCHS' Osceola campus (for issues relating to the Osceola campus) (both the Director of Operations and the Administrator shall be referred to herein as the "Privacy Officer" for his or her respective campus). Upon receipt of such report, the Privacy Officer shall begin an investigation, and conduct a risk assessment, to determine whether a Breach has occurred.

(b) Investigation. The Privacy Officer shall act as the investigator of the Breach and shall be responsible for the management of the Breach investigation, completion of a risk assessment and coordinating with others at CCHS, as appropriate (*e.g.,* administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.). The Privacy Officer shall be the key facilitator for all Breach notification processes to the appropriate entities or individuals (*e.g.,* HHS, media, law enforcement officials, etc.).

(c) Risk Assessment. For acquisition, access, use or disclosure of Unsecured PHI to constitute a Breach, it must constitute a violation of the Privacy Rule. A use or disclosure of Unsecured 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. An impermissible or unauthorized acquisition, access, use, or disclosure of Unsecured PHI is presumed to be a Breach unless CCHS (or its business associate, as applicable) demonstrates that there is a low

probability that the Unsecured PHI has been compromised based on an assessment of at least the following factors:

(i) The nature and extent of the Unsecured PHI involved, including the types of identifiers and the likelihood of re-identification (*e.g.,* there is a high probability that the Unsecured PHI has been compromised when detailed clinical information such as treatment plans or diagnosis are involved);

(ii) The unauthorized person who used the Unsecured PHI or to the disclosure was made (*e.g.,* there is a low probability that the Unsecured PHI has been compromised when the person who received the Unsecured PHI has an obligation to protect its privacy under HIPAA, such as another covered entity);

(iii) Whether the Unsecured PHI was actually acquired or viewed (*e.g.,* there is a low probability that the Unsecured PHI has been compromised when forensic analysis indicates that Unsecured PHI on a stolen laptop was never accessed, viewed, acquired, transferred or otherwise compromised); and

(iv) The extent to which the risk to the Unsecured PHI has been mitigated (*e.g.,* there may be a low probability that the Unsecured PHI has been compromised when an employee, affiliated entity or business associate provides reasonable assurances that Unsecured PHI received in error was immediately destroyed, but reasonable assurances from certain third parties may not be sufficient).

(d) Documentation.

(i) The Privacy Officer shall document the risk assessment as part of the investigation and note the outcome of the risk assessment process. Based on the outcome of the risk assessment, CCHS will determine if there has been a Breach and, if so, provide the appropriate notification to the affected individual(s). CCHS may make Breach notifications without completing a risk assessment.

(ii) The Privacy Officer, or his or her designee, shall maintain a log of all Breaches. The log shall include the date of the Breach, a description of the impermissible use or disclosure, the date of discovery and the number of individuals affected, if known. The log will also include a description of the types of PHI involved, actions taken to notify individuals, mitigate the Breach and prevent future Breaches, and any other information required by HHS.

(iii) All documentation related to the Breach investigation, including the risk assessment and notifications made, shall be retained for a minimum of six years following the date of the incident.

(e) Notification Timing. If, based on the results of the investigation and the risk assessment, CCHS determines a Breach has occurred, CCHS shall begin the process of notifying each individual whose Unsecured PHI has been, or is reasonably believed by CCHS to have been, accessed, acquired, used or disclosed as a result of the Breach. CCHS also shall begin the process of determining what external notifications are required or should be made (*e.g.,* Secretary of Department of HHS, media outlets, law enforcement officials, etc.). Upon determination that Breach notification is required, the affected individual(s) shall be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach by CCHS. A Breach shall be treated as "discovered" as of the first day on which an incident that may have resulted in a Breach is known to CCHS or, by exercising reasonable diligence would have been known to CCHS (or by CCHS's business associate). CCHS shall be deemed to have "known" of a Breach if such Breach is known or, if 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 (*e.g.* a business associate acting as an agent of CCHS) of CCHS.

(f) Delay of Notification Authorized for Law Enforcement Purposes. If a law enforcement official states to CCHS that a notification, notice or posting would impede a criminal investigation or cause damage to national security, CCHS shall delay notification notice or posting:

(i) For the time period specified by the official, if the statement is in writing and specifies the time for which a delay is required; or

(ii) No longer than 30 days from the date of a verbal statement, unless a written statement as described above is submitted during that time. If the statement is made verbally, CCHS shall document the statement, including the identity of the official making the statement.

(g) Content of the Notice. The notice of Breach shall be written in plain language and must contain the following information:

(i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

(ii) A description of the types of Unsecured PHI that were 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).

(iii) Any steps the individual should take to protect him or herself from potential harm resulting from the Breach.

(iv) A brief description of what CCHS is doing to investigate the Breach, to mitigate harm to the individual and to protect against further Breaches.

(v) Contact procedures for an individual to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.

(h) Methods of Notification. The method of notification will depend on the individuals or entities to be notified. The following methods must be utilized accordingly:

(i) Notice to Individual(s). Notice shall be provided promptly and in the following form:

[a] 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 CCHS knows that 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 personal representative shall be carried out.

[b] Substitute Notice. In the case where there is insufficient or out-of-date contact information (including phone number, e-mail 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.

[i] In a case in which there is insufficient or out-of-date contact information for fewer than ten individuals, then CCHS will provide the substitute notice by an alternative form of written notice, telephone or other means.

[ii] In the case in which there is insufficient or out-of-date contact information for ten 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 CCHS's website, or a conspicuous notice in a major print or broadcast media in CCHS'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.

[c] If CCHS determines that 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.

(ii) Notice to Media. Notice shall be provided to prominent media outlets serving the state and regional area (of the Breached individuals) when the Breach of Unsecured PHI affects 500 or more of CCHS's individuals of a State or jurisdiction.

[a] The notice shall be provided in the form of a press release.

[b] CCHS will consider what constitutes a prominent media outlet based upon the State or jurisdiction where CCHS's affected individuals reside. For a Breach affecting more than 500 individuals across a particular state, CCHS will consider a prominent media outlet to be a major, general interest newspaper with a daily circulation throughout the entire state. CCHS will not consider a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics), as a prominent media outlet. Where a Breach affects more than 500 individuals in a limited jurisdiction, such as a city, then CCHS will consider a major, general interest newspaper with daily circulation throughout the city to be a prominent media outlet, even though the newspaper does not serve the whole State.

(iii) Notice to the Secretary. Notice shall be provided to the Secretary of HHS as follows:

[a] For Breaches involving 500 or more individuals, CCHS shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

[b] For Breaches involving less than 500 individual, CCHS will maintain a log of the Breaches. CCHS may report the Breaches during the calendar year or no later than 60 days after the end of that calendar year in which the Breaches were discovered (*e.g.,* 2012 Breaches were to be submitted by 3/1/2013). Instructions for submitting the logged Breaches are provided at www.hhs.gov.

(i) Maintenance of Breach Information/Log. As described above and in addition to the reports created for each incident, the Privacy Officer shall maintain a process to record or log all Breaches regardless of the number of individuals affected. The following information should be documented for each Breach:

(i) 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.

(ii) A description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, etc.).

(iii) A description of the action taken with regard to notification of individuals, the media and the Secretary of HHS regarding the Breach.

(iv) The results of the risk assessment.

(v) Resolution steps taken to mitigate the Breach and prevent future occurrences.

(j) Business Associate Responsibilities. Any business associate of CCHS that accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys or otherwise holds, uses or discloses Unsecured PHI shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach, notify the Privacy Officer of such Breach. This notice shall include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired or disclosed during such Breach. The business associate shall provide the Privacy Officer with any other available information that 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 business associate of discovery of a Breach, CCHS will be responsible for notifying affected individual(s), unless otherwise agreed upon by CCHS.

(k) Workforce Training. CCHS trains all members of its Workforce on its HIPAA policies and procedures as necessary and appropriate for such persons to carry out their job responsibilities. Workforce members also are trained as to how to identify and promptly report any impermissible or unauthorized acquisition, access, use or disclose of Unsecured PHI. Workforce members that assist in investigating, documenting and resolving Breaches are trained on how to complete these activities.

(l) Non-Retaliation. It is the Policy of CCHS not to retaliate against any Workforce member that makes a good faith report regarding a suspected or actual impermissible or unauthorized acquisition, access, use or disclose of Unsecured PHI, or who assists in investigating, documenting or resolving suspected or actual Breaches.

(m) Sanctions. Compliance with these policies and procedures is a requirement of employment by, or doing business with, CCHS. Workforce members who fail to comply with this policy may be subject to sanctions. Business associates who violate this Policy may be subject to termination.