Care1st Health Plan

POLICY & PROCEDURE

CORPORATE COMPLIANCE DEPARTMENT

Policy Title: Privacy and Security Breach Notification Procedures		
Policy No: 70.17.6	Orig. Date: September 2009	
Effective Date: 7/2010	Revision Date: 7/2010;12/2012; 2/2014	Revision No: 3
P&P Subcommittee Approval: Date: 3/27/14		
Board Approval Date: 3-27-14	Scope of Coverage: ALL DEPARTMENTS and/or All Lines of Business	

PURPOSE:
The purpose of this policy is to outline the internal processes, procedures, and time frames for reporting breaches of members/individuals' individually identifiable health information / personally identifiable information (PII) / protected health information (PHI) by Care1st Health Plan ("Care1st") and/or Care1st's contracted vendors and other related/contracted entities pursuant to the Final Omnibus Rule (effective 9/23/2013) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

POLICY:
(A) Following a breach of unsecured PHI, covered entities (CEs), or Care1st, and/or Care1st's Business Associates (BAs) and the BA's downstream subcontractors, must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. Care1st and/or its BAs and the BAs' downstream subcontractors will conduct a PHI/PII risk assessment to determine whether or not PHI was compromised and/or if a breach notification will be required. This risk assessment must include consideration of the following four (4) factors, at a minimum:

1. The nature and extent of the PHI/PII involved, including the types of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the PHI/PII or to whom the disclosure was made.
3. Whether the PHI/PII was actually acquired or viewed.
4. The extent to which the risk to the PHI has been mitigated.

(B) Care1st's Breach Notification (Internal) Risk Assessment includes all four factors above.

(C) Care1st's first-tier, downstream, and other related entities (FDRs) and other business associates are notified of any changes in Privacy and/or Security reporting/notification requirements through distribution of training materials and required training attestations.

DEFINITIONS:

The HIPAA Omnibus Final Rule - implements the Health Information Technology for Economic and Clinical Health (HITECH) Act provision making Business Associates (BAs), and the BAs' downstream subcontractors, directly accountable for compliance

with Health Insurance Portability and Accountability Act's (HIPAA) Security Rule and certain Privacy Rule requirements.

American Recovery & Reinvestment Act of 2009 (ARRA) – New HIPAA Notification Requirements on Breach of PHI. Section 13402 of ARRA requires HIPAA Covered Entities (CEs) to notify an individual if the CE discovers a breach of individual's unsecured PHI. Additionally, ARRA requires Business Associates (BAs) of CEs to notify the CEs of any discovered breaches of unsecured PHI. This requirement is only applicable in cases where the breach relates to "unsecured protected health information." If the breached PHI is secured, the notification requirements do not apply. *(*Refer to Section 10 *"Guidance to Render Unsecured PHI Unuseable, Unreadable, or Indecipherable to Unauthorized Individuals"* beginning on page 4 of this document.)

Breach – is, generally, an impermissible use of disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. c. A privacy/security violation involving PHI must be presumed to be a breach unless and until a risk assessment is performed and it indicates only a low probability that PHI is compromised. The Final Omnibus Rule retains the three (3) exceptions of a breach.

- Three (3) Exceptions to the definition of "breach".
    - The first one applies to the unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or Business Associate;
    - The second one applies to the inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or Business Associate to another person authorized to access PHI at the covered entity or Business Associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule; and
    - The final exception to breach applies if the covered entity or Business Associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

CMS – the Centers for Medicare & Medicaid Services is the Federal agency that administers Medicare, Medicaid and the State Children's Health Insurance Program (SCHIP).

Personally Identifiable Information (PII) – any information about an individual including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information, which is linked or linkable to an individual.

Protected Health Information (PHI) – any individual identifiable health information. Identifiable refers not only to the data that is explicitly linked to a particular individual (that's identified information). It also includes health information with data items which reasonably could be expected to allow individual identification.

PROCEDURES:

Internal Reporting:

1. When/if an/a attempted, suspected or successful breach incident is identified or committed by Care1st's staff and/or its first-tier and downstream entities; the incident is reported, **immediately,** to Care1st's Compliance and Management Information System (MIS) Departments. The following individuals are immediately notified:
   The Corporate Compliance Officer (CCO)/Privacy Officer;
   The Chief Information Officer (CIO);
   The VP of MIS & Security Officer;
   Legal and Regulatory Services Department; and
   Other Identified Individuals Involved in the breach, as deemed appropriate.
2. **Log/Enter in the Special Investigations Unit (SIU) Database:**
   The SIU Compliance Department is also informed of the incident. The incident is logged in the SIU database and is processed in accordance with Care1st's Policy and Procedure **70.17.2 and 70.17.2.1 – *Processing of Potential and Non-Compliant Activities.***

3. **Coordination with Legal and Regulatory Services ("Legal") and Other Departments Involved:**
   The CCO, CIO, and the VP of MIS & Security Officer will convene and will obtain advice from Care1st's Legal Department and statements from appropriate individuals and departments involved in the breach incident.

   The CCO, CIO, and the Security Officer and/or their designated representatives/staff may/will assist, as appropriate, in reporting the incident to regulatory agencies following the steps, criteria, and time frames describe below.

Individual Notices:

4. Care1st (and/or its FDRs) notifies affected individuals following the discovery of a breach of unsecured PHI. Care1st will provide this notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notice electronically.

- If Care1st has insufficient or out-of-date contact information for 10 or more individuals, Care1st provides substitute individual notice by either posting the notice on the home page of Care1st's web site or by providing the notice in major print or broadcast media where the affected individuals likely reside.
- If Care1st has insufficient or out-of-date contact information for fewer than 10 individuals, Care1st will provide substitute notice by alternative form of written, telephone, or other means.

Time Frames for Notifications:

5. Notifications will be provided without unreasonable delay and in no case later than 60 calendar days following the discovery of a breach and will include, to the extent possible:

- A description of the breach;
- A description of the types of information that were involved in the breach;
- The steps affected individuals should take to protect themselves from potential harm;
- A brief description of what Care1st is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as Care1st's contact information; and
- For substitute notice provided via web posting or major print or broadcast media, the notification includes a toll-free number for individuals to

contact Care1st to determine if members/individuals' PHI was involved in the breach.

Media Notice:

6. For a breach affecting more than 500 residents of a State or jurisdiction area, in addition to notifying affected individuals, Care1st (and/or its FDRs) provides notice to prominent media outlets serving the State or jurisdiction (e.g., in the form of a press release). Similar to Individual Notice, this media notification is provided without unreasonable delay and in no case later than 60 calendar days following the discovery of a breach and includes the same information required for the Individual Notice.

Notice to the Secretary of Department of Health & Human Services (DHHS):

7. In addition to notifying affected individuals and the media (where appropriate), Care1st (and/or its FDRs) notifies the Secretary of breaches of unsecured PHI. Care1st will notify the Secretary by visiting the DHHS web site and filling out and electronically submitting a breach report form (Appendix B) at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html or http://ocrnotifications.hhs.gov/

- If a breach affects 500 or more individuals, Care1st notifies the Secretary without unreasonable delay and in no case later than 60 calendar days following a breach.
- If, however, a breach affects fewer than 500 individuals, Care1st notifies the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 calendar days after the end of the calendar year in which the breach occurred.

Notification by Care1st's Business Associates (BAs) and their downstream subcontractors:

8. If a breach of unsecured PHI occurs at or by a Business Associate, or the BA's downstream subcontractor, the Business Associate notifies the appropriate regulatory agencies and Care1st following the discovery of the breach as required by the DHHS' Privacy and Security HIPAA rules.
  - The Business Associate must provide notice to the appropriate regulatory agencies and Care1st without unreasonable delay and no later that 60 calendar days from the discovery of the breach as required by the DHHS' Privacy and Security HIPAA rules.
  - To the extent possible, the Business Associate should also provide Care1st with the identification of each individual affected by the breach as well as any information required to be provided by Care1st in its notification to affected individuals (if Care1st also decides to notify affected individuals).

Burden of Proof:

9. Care1st and its Business Associates have the burden of proof to demonstrate that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach.
- Care1st applies all its existing Policies and Procedures related to Privacy Rule with respect to breach notification including, but not limited to:
  - Reporting breach incidents to other regulatory agencies (e.g., Centers for Medicare & Medicaid Services (CMS)), as deemed required and/or appropriate;

- Sanctions against workforce members and/or contracted entities/vendors who do not comply with Care1st's procedures, as deemed appropriate; and
- Training of employees and/or contracted entities/vendors on Privacy and Security Rules.

DHHS' Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals:

10. PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without cause of a confidential process or key" (CFR 164.304 definition of encryption) and such confidential process or key that might enable the decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.
    a. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.[1]
    b. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to Internet Protocol Security (IPsec) Virtual Private Networks (VPNs); or 800-113, Guide to Secure Socket Layer (SSL) VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.
2. The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
    a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
    b. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

11. Breach for Medi-Cal population/membership:

a. Care1st will inform L.A. Care on any breaches affecting the Medi-Cal membership within three (3) business days from the date of discovery (per Plan Partner's Service Agreement).

12. Breach Notification to the Department of HealthCare Services (DHCS):

a. Care1st will notify DHCS in accordance with Care1st's Policies and Procedures 70.17.36 *Notification to DHCS; P&P* 70.17.2 and 70.17.2.1

[1] NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates of this guidance, when available.

(Processing of Suspected/Potential Non-Compliant Activities for Medi-Cal (L.A. Care and San Diego, respectively).

Authority / References:

- The HIPAA Omnibus Rule, Code of Federal Regulation (CFR) 160.408
- Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act
- Care1st's Policy and Procedure 70.17.36 – *Breach Notification to DHCS*
- Care1st's Policy and Procedure 70.17.2 – *Processing Potential and Non-Compliant Activities*
- Care1st's Policy and Procedure 50.17.4 – *Reporting of Security Incidents to CMS*
- CMS Memorandum dated December 16, 2008 – *Security and Privacy Reminders and Clarification of Reporting Procedures*
- CMS Memorandum dated September 28, 2010 – *Update on Security and Privacy Breach Reporting Procedures*
- *CMS Information Security Incident Handling and Breach Analysis/Notification Procedure*, Version 2.1, October 28, 2008
- ***http://ocrnotifications.hhs.gov/***
- *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.*
- Breach Notification (Internal) Risk Assessment – Revised (Compliant with Omnibus Final Rule)
- Care1st HIPAA Omnibus Final Rule Training Materials for FDRs / Business Associates.

APPENDIX B