**DIGNITY HEALTH**
**ADMINISTRATIVE POLICY AND PROCEDURE**

**FROM:** Compliance Oversight Committee

**SUBJECT:** Investigation, Response and Notification of Data Security Incidents

**EFFECTIVE DATE:** June 12, 2015

**REVISED:**

**ORIGINAL EFFECTIVE DATE:** June 12, 2015

**REPLACES:** New

| **APPLIES TO:** | | |
|---|---|---|
| | System Offices: | X |
| | Acute Care Entities: | X |
| | Non-acute Care Entities: | X |

## I. POLICY:

It is the policy of Dignity Health to promptly respond to, investigate and document all reports, complaints and inquiries relating to Data Security Incidents. As part of its investigation the Dignity Health Facility shall evaluate and promptly report and/or notify[1], as required by this policy, and Mitigate, to the extent practicable, any harmful effects of such Incidents.[2]

A. The CISO and Director of Security or designated delegate(s) will identify the reporting structure and staffing for the incident response team.

B. Every Data Security Incident will designate an individual from the incident response team to be the investigator or incident owner who will be responsible for coordinating the investigation, documentation, and timely communications to all relevant stakeholders.

C. All investigations shall follow the IT Security Incident Response Standard #001.009.00001 guidelines that define the criteria of incidents that are and are not to be investigated.

[1] California Civil Code 1798.82, Title 52 Nevada 603A; Arizona Revised Statutes § 44-7501
[2] 45 CFR 164.530(f) and 45 CFR 164.308(a)(6)

D. For Data Security Incidents involving PHI, PII or any other Sensitive information, unless otherwise directed by the Corporate Compliance Officer or Chief Information Security Officer (CISO), the investigator will notify all relevant Facility Compliance Professionals (FCPs) and add them to the list of stakeholders.

E. For Incidents involving possible misconduct by members of the Dignity Health Facility's HIPAA Workforce, the investigator shall follow the procedures of the **Corrective Process for Breach of Patient Privacy or Confidentiality** policy #120.1.006.

F. For Incidents involving Business Associates, the investigator shall follow the procedures of the **Investigation, Response and Notification of Privacy and Data Security Incidents** policy #70.8.028.

G. For Incidents involving trading partners or other third parties, the investigator shall contact the appropriate Legal Services representative for guidance.

H. For Incidents involving members of the Dignity Health Facility's Organized Health Care Arrangement (OHCA), the incident response team investigator shall investigate the Incident, with the assistance of the Medical Director or the Dignity Health Facility Administrator and local legal counsel.

I. For any Incident involving a known or suspected criminal act, the investigator shall report the incident to the Dignity Health Facility's public safety official.

J. The investigator and the Dignity Health Facility shall take necessary and reasonable timely actions to restore the integrity, confidentiality, and availability of the Network and to correct or minimize any known Breach of Privacy or Confidentiality or any Breach of Security.

K. For any Breach requiring regulatory and/or patient notification, the incident response team investigator shall coordinate with the appropriate FCP. The FCP, in conjunction with the Corporate Compliance Officer, Legal Services representative, and a representative of Corporate Communications, shall follow the procedures of the Dignity Health **Investigation, Response and Notification of Privacy Incidents** policy #70.8.028, and promptly notify the applicable Covered Entity[3], state or federal agency, as well as the affected patient(s) whose personal information has, or is reasonably believed to have been, the subject of the Breach.

[3] 45 CFR § 164.410 Notification by a business associate

## II. PURPOSE:

The purpose of this policy is to define requirements for the notification, investigation, and response of Data Security Incidents in accordance with Dignity Health's **Investigation, Response and Notification of Privacy and Data Security Incidents** policy #70.8.028, the Health Insurance Portability and Accountability Act ("HIPAA") and other federal and state laws governing protection of confidential information. The Dignity Health Board has delegated certain aspects of its authority to the Dignity Health Corporate Compliance Officer and Chief Information Security Officer to ensure that necessary policy and procedures are written and implemented to comply with federal and state Privacy and Data Security regulations.

## III. DEFINITIONS:

Capitalized terms not defined herein shall be defined in the **Data Security Administrative Policy Definitions** policy #110.2.003.

- "**Data Asset**" – means any of the following:
  - Hardware: computer, server, network, network device, router, switch, workstation, personal computer (PC), personal digital assistant (PDA), tablet computer, mainframe computer, tape, compact disk (CD), floppy, flash memory device, etc;
  - Software: operating system, application, database, program, script, etc;
  - Electronic data or information: entered into, received by, transmitted over or through, processed by, stored on, or in any way involved with an electronic information asset, regardless of media;

- "**Breach**" – means the unauthorized viewing, acquisition, access, use, or disclosure of PHI, Personal Information, or credit card information in oral, paper or electronic form which compromises the confidentiality of such information. Exceptions, such as good faith exceptions, may apply depending on the specific circumstances associated with the breach.

- **"Business Owner"** – see section I.E.6 of the **Data Security policy** #110.2.001.

- "**Encrypted**" – means a technology or algorithmic process which renders the data unreadable, unusable, or indecipherable to unauthorized individuals and which satisfies the requirements for Secured PHI as defined under Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act and consistent with guidance published by the Secretary of the Department of Health and Human Services.

- **"Incident"** – means a Privacy Incident or Data Security Incident.

- **"Mitigate"** or **"Mitigation" –** means the act of minimizing any harmful effect that is known to the Dignity Health Facility and that is a Use or Disclosure in violation of the Dignity Health Facility's privacy and security policies and procedures or a violation of the terms of a Business Associate Agreement.

- "**Personal Information**" – means an individual's first name or first initial and last name in combination with any one or more of the following data elements:[4]
  1) Social security number
  2) Driver's license number or state issued non-operating identification card or license number
  3) Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
  4) Medical Information

- **"Data Security Incident**" – means any negligent, intentional or natural act that impacts the confidentiality, integrity, or availability of electronic data. For example, but not limited to any occurrence that
  1) results in a Breach of any Dignity Health non-public data;
  2) permits unauthorized access to the Dignity Health Network;
  3) results in the unauthorized creation, deletion or change of data
  4) adversely impacts the functionality of the Dignity Health Network; or
  5) involves the loss or loss of control of a Dignity Health owned or managed information technology resource; or
  6) results in non-compliant action or configuration related to a data asset.
  7) involves the use of Dignity Health information technology resources for illegal purposes or to launch attacks against other individuals or organizations.

- **"User(s)" –** means all employees, non-employee providers, Business Associates, contractors, and other third parties that have been given access to the Dignity Health Network, including information systems, and portals.

## IV. PRINCIPALLY AFFECTED DEPARTMENTS:

This policy applies to all facilities and departments with Users of the Dignity Health Network, and each shall receive required education as applicable.

[4] California Civil Code 1798.82(e), Title 52 Nevada 603A.040; Arizona Revised Statutes § 44-7501

## V. PROCEDURES FOR ALL FACILITIES:

### A. Reporting Incidents.

Timely reporting of all Data Security Incidents is critical to Dignity Health's ability to promptly investigate the Incident, mitigate any potential harm, and to comply with its legal obligations under federal and state regulations.

1. Any individual that has agreed to comply with Dignity policy by having signed or is in scope of a Network Usage Policy Agreement (such as, but not limited to a member of the Dignity Health Facility's HIPAA Workforce, member of a Dignity Health Organized Health Care Arrangement (OHCA), Business Associate, Business Owner, technical owner, or other person having authorized access to Dignity Health's records or Network), shall promptly report any Incident known to them that involves events or actions representing significant threat to the security and/or integrity of the Dignity Health Network or which may involve unauthorized access to Sensitive or Confidential Information.

2. Any member of the Dignity Health HIPAA Workforce, Business Associate, trading partner or other User that becomes aware of a Data Security Incident shall promptly report the Incident to one of the following:
   a. The local facility Dignity Health IT Site Director. If the Site Director determines the report is a Data Security Incident, it must be reported to the incident response team or IT Helpdesk;
   b. Directly to the IT incident response team.
   c. Directly to the IT Helpdesk

3. The person receiving the complaint shall assist with determining whether a Security Incident is merited and submit the information to the incident response team.

### B. Investigation of Security Incidents.

The Security Incident Response Standard will list the requirements for the investigation and reporting of Data Security Incidents and complaints, and include a Standard Operating Procedure (SOP) for the incident response team.

1. All investigations shall be completed without unreasonable delay and within sixty (60) days of notification of the Incident.
2. For Incidents involving PHI, the investigator will promptly notify the appropriate Facility Compliance Professional.
3. For Incidents representing significant or serious risk to the Dignity Health Network, including incidents involving known or suspected unauthorized

access to PHI or other Sensitive Information, the incident response team shall include in the SOP the following:

a. Methods to secure all evidence such that it can be used effectively by law enforcement or in a court of law.

b. Assessment of the risk of continuing operations, consulting with Business Owners, technical owners, and IT operations managers as appropriate.

c. Requirements for password changes on affected systems and networks as necessary.

d. Review of plans to restore affected systems using the last uncompromised backup.

e. Coordination of activity with other command centers or disaster recovery efforts.

f. Prompt notification to the IT Site Director, and CISO of all such Incidents, and shall provide timely status reports on the progress of investigation and management of the Incident.

g. Dignity Health Legal Counsel shall be consulted to advise on any special considerations that are to be taken relating to the investigation.

C. **Notification by Dignity Health as a Business Associate.** When Dignity Health is a business associate of a Covered Entity, Dignity Health shall, following the discovery of a Breach involving another Covered Entity's Unsecured PHI, seek guidance from the appropriate Legal Services representative, and notify the Covered Entity without unreasonable delay and no later than 60 calendar days after discovery of a breach or in accordance with the agreement between the parties, per the Dignity Health Investigation, Response and Notification of Privacy and Data Security Incidents policy #70.8.028. The notification shall include, to the extent possible the identification of each individual whose unsecured PHI has been or is reasonably believed by Dignity Health to have been subject to the breach.

**D. Sanctions**. Individuals that fail to comply with Dignity Health's privacy and security policies, interfere with the effectiveness of Dignity Health's data security controls or are responsible for a Breach of Privacy or Security shall be sanctioned in accordance with Dignity Health policy and as follows:

1. Members of the Dignity Health Facility's workforce shall be referred to Human Resources for disciplinary action as provided in the **Corrective Process for Breaches of Patient Privacy and Confidentiality** policy #120.1.006;

2. Independent members of the Dignity Health Facility's credentialed medical staff shall be referred to the Vice President of Medical Affairs or other applicable executive responsible for the Dignity Health Facility's medical staff for consideration of re-education, loss of Network privileges, or other appropriate medical staff action.

3. A Business Associate or other third party Users will be referred to the applicable Dignity Health Business Sponsor for consideration of re-education, loss of Network privileges, or other appropriate sanctions or notices under the provisions of the applicable written agreements, per the Dignity Health **Investigation, Response and Notification of Privacy and Data Security Incidents** policy #70.8.028.

**E. Documentation**. The incident response team Investigator shall complete and retain all documentation of the incident investigation for a minimum of six years from the date of completion of all required remediation.

## VI. STATUTORY/REGULATORY AUTHORITIES:

Noted in footnotes in policy if applicable.

## VII. EXHIBITS: