

**DIGNITY HEALTH
ADMINISTRATIVE POLICY AND PROCEDURE**

FROM: Dignity Health Compliance Oversight Committee

SUBJECT: HIPAA Workforce Data Security Education

EFFECTIVE DATE: June 12, 2015

REVISED:

ORIGINAL EFFECTIVE DATE: June 12, 2015

REPLACES: New

APPLIES TO:	System Offices:	<u> X </u>
	Acute Care Entities:	<u> X </u>
	Non-acute Care Entities:	<u> X </u>

I. POLICY:

It is the policy of Dignity Health to provide its HIPAA Workforce with training and education concerning confidentiality, privacy¹ and data security² as may be reasonably necessary and appropriate to ensure material compliance with applicable laws and Dignity Health policies relating to the protection of Protected Healthcare Information (“**PHI**”).

In addition, where Dignity Health offers practice management services (which include physicians and their office staff), the practice management services contract will determine the responsibility for education and training for Dignity Health’s compliance purposes.

Third parties having a contractual relationship with Dignity Health that spend substantial amounts of time working within Dignity Health Facilities are welcome to participate in Dignity Health data security training activities, but are not required to participate. These third party contractors are separately required to comply with Dignity Health Facility policies and procedures, applicable laws, and contractual terms related to privacy and data security education.

¹ 45 CFR 164.530(b)

² 45 CFR 164.308(a)(5)

II. PURPOSE:

The purpose of this policy is to implement certain aspects of Dignity Health's Privacy Principles policy #70.8.001 in order to comply with the Health Insurance Portability and Accountability Act ("HIPAA") and other federal and state laws governing protection of confidential health information. The Dignity Health Board has delegated certain aspects of its authority to the Dignity Health Chief Information Security Officer (CISO) 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 as defined in the Dignity Health Data Security Administrative Policy Definitions policy #110.2.003.

HIPAA Workforce:³

A Dignity Health Facility's HIPAA Workforce includes Dignity Health Facility employees (including employed physicians). It also includes residents, volunteers (including Chaplaincy Volunteers), and students, whose conduct, in the performance of their work for the Dignity Health Facility, is under direct control of the Dignity Health Facility. Students are those people participating in Dignity Health Facility-sponsored medical training programs. Personnel from external programs, including, but not limited to, residents, registry staff, interns and students from such programs are third party entities, and accordingly, shall not be deemed members of the HIPAA Workforce. (See **Business Associate and Other Classified Information** policy # 70.8.011).

IV. PRINCIPALLY AFFECTED DEPARTMENTS:

This policy applies to all system offices, hospitals, ambulatory surgery centers, home health agencies, physician practices and sites with Users of the Dignity Health Network, and each shall receive required education as applicable.

V. PROCEDURES FOR ALL FACILITIES:

It is the responsibility of each Dignity Health Facility or system office to develop the necessary procedures to implement this policy in a uniform manner in order to meet the requirements of this policy. At a minimum, the Dignity Health Facility or system office will adhere to the following:

³ 45 C.F.R. 160.103

- A. All members of the HIPAA Workforce shall be provided with initial general data security awareness training as follows:
 - 1. New Hire Training: All newly hired members of the HIPAA Workforce will be provided with general data security awareness training within 30 days from the date of hire or initial date of service⁴. Per Diem and casual employees must be trained within 60 working hours of commencing employment. This training shall be incorporated into the orientation program at each facility or system office.
- B. Additional training:
 - 1. Any member of the HIPAA Workforce whose job function requires substantial or regular Use or Disclosure of PHI or Sensitive Information, is a Business Owner of a facility non-IT managed system or is involved with handling and/or processing credit card information shall be provided additional function-specific training based on the requirements of the job.
 - 2. Additional training will be required whenever new policies are issued or there are material changes in Dignity Health policies and procedures concerning Use and Disclosure of PHI⁵, Sensitive Information or data security.
 - 3. The HIPAA Workforce will be provided with appropriate data security training prior to the compliance date for new or revised federal and state data security regulations.
- C. All HIPAA Workforce members will be required to complete Data Security awareness training on a periodic basis.
- D. Each Dignity Health Facility shall be required to maintain documentation of Data Security training for each member of the HIPAA Workforce member as required above⁶ for a minimum of six years.

VI. STATUTORY/REGULATORY AUTHORITIES:

Noted in footnotes in policy if applicable.

(end of policy)

⁴ 45 CFR 164.530(b)(2)(i)(B)

⁵ 45 CFR 164.530 (b)(2)(i)(C)

⁶ 45 CFR 164.530 (b)(2)(ii)