Updated FY15 Dignity Health General Compliance Education for Staff Module 2

This course will provide you with important information about the laws and regulations that affect the healthcare industry, our organization and you.

Dignity Health

Course Objectives

Upon completion of this course, you should be able to understand and describe:

- Understand what data elements make up PHI
- Patient's rights under HIPAA
- Appropriate use of the Dignity Health network
- Appropriate use of Social Media
- Your disclosure and reporting obligations

Health Insurance Portability and Accountability Act (HIPAA)

Dignity Health

3

HIPAA Regulations

The Health Insurance Portability & Accountability Act (HIPAA) is managed by the Office of Civil Rights (OCR)

- HIPAA regulations include controls for the use and disclosure of Protected Health Information (PHI).
  - **Use**: when PHI is used internally for Treatment, Payment or other Healthcare Operations (audits, training, customer service, internal analysis, etc.).
  - **Disclosure**: to release or provide access to a patient's PHI to someone like a physician, an attorney, insurance company, etc., outside of Dignity Health.

Dignity Health

4

Protected Health Information (PHI)

- HIPAA regulations include controls for the use and disclosure of PHI.
- PHI comes in many forms and does not need to include the patient's name to be considered PHI:
  - Paper records of all types
  - Labels on patient care items
  - Photos and graphics
  - Electronic & computer-based records
  - Biomedical equipment
  - Portable storage media
  - Video recordings
  - Verbal communications

Dignity Health

5

Patient's Rights under HIPAA

All Patients have a right to:

- Inspect and/or get a copy of their medical record
- Request a restriction on disclosure of their PHI.
- An Accounting of Disclosures - Patients at any time can ask us to provide them with a list of everyone we have released their health records to, for a period of 6 years.
- Request an alternative means of communication.
- Request an amendment to their PHI.
- All inpatients have the right to Opt-Out of the facility directory

Dignity Health

6

Notice of Privacy Practices

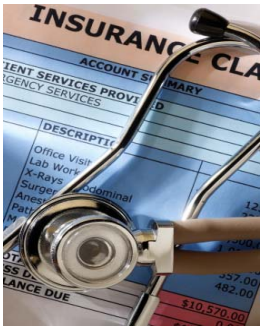
- Dignity Health must provide a Notice of Privacy Practices (NPP) to patients at the time of their visit to the facility. The NPP explains:
  - How we use and disclose PHI
  - What we do to protect privacy
  - Patients' rights with regard to privacy
  - Who to contact to file a complaint

Dignity Health

7

Treatment, Payment and Operations (TPO)

- A patient's written authorization is required for most uses or disclosures of PHI except for Treatment, Payment and healthcare Operations (TPO).
  - Treatment: Disclosing necessary information to other providers who are involved in treating the patient.
  - Payment: Disclosing necessary information to health plans, insurers, or others for the payment of health care provided to the patient.
  - Operations: Use of health information for quality improvement, care management, patient satisfaction studies, accreditation, and education.



Dignity Health

8

Minimum Necessary

- HIPAA's Privacy Rule requires that you make a reasonable effort to limit the use, disclosure or release of PHI to only the Minimum Necessary amount of data that is necessary to accomplish the intended purpose.
  - Only share PHI with authorized individuals who have a need to know.
  - Dignity Health workforce members must apply Minimum Necessary standards when PHI must be disclosed to someone outside of Dignity Health. (for example, an attorney, contractor, business associate, auditor, etc.)

Reference Policy 70.8.015 Minimum Necessary Standards

Dignity Health

9

Patient's Family and Friends

- You may disclose PHI to members of the patient's family, friends, or any other person identified by the patient as being involved in their care or payment, if the patient has agreed to the disclosure.
- Disclose only PHI that is directly relevant to the involvement of the family member or friend.
- Use professional judgment about disclosing PHI in an emergency or if patient is unable to express agreement.
- You may disclose a patient's location, general condition, or death in order to notify, identify or locate a family member or personal representative of the patient.

Reference Policy 70.8.013 Patient's Friends and Family

"For your privacy, is it okay to discuss the test results for your incontinence problem in front of your visitors?"

Dignity Health

10

HITECH Act

Effective January 1, 2009 the HITECH Act is the privacy and data security component of the American Recovery and Rehabilitation Act (ARRA)

Health

Information

Technology for

Economic and

Clinical

Health

- HITECH applies HIPAA standards and penalties to Business Associates.
- Increases penalties for HIPAA Violations
  - Maximum penalty per violation increases from $100 per violation to $50,000 maximum.
  - The cap on penalties for all similar violations increased from $100,000 to $1,500,000.
  - **Makes individuals subject to penalties**.

Dignity Health

11

HITECH Impact to the Individual Healthcare Worker

Doctor and Two Employees Plead Guilty to HIPAA Violation

- Little Rock - The United States Attorney's Office, issued a press release providing details of the guilty pleas by a physician and two hospital employees for HIPAA violations. Each pled to a violation of HIPAA based on their accessing a patient's record without any legitimate purpose.

Ex-UCLA Healthcare Employee Sentenced to Federal Prison for Illegally Peeking at Patient Records

- Los Angeles - A former UCLA Healthcare System employee, who admitted to illegally reading confidential medical records, mostly celebrities and other high profile patients, was sentenced to four months in federal prison.

Dignity Health

Safeguarding PHI & Sensitive Information

- Protecting patient privacy and confidential information means practicing some basic safeguards in your work area.
  - Do not leave documents with PHI or confidential information unattended on fax machines, printers or copiers.
  - Never allow removal of PHI or other confidential information from the facility without authorization and appropriate security measures.
  - Store portable media that contains PHI or Confidential information in a locked drawer or cabinet.

Safeguarding Faxes and U.S. Mail

- Misdirected faxes are the #1 reported privacy incident across Dignity Health.
- Everyone must use a Dignity Health fax coversheet when faxing PHI or other confidential information.
- Always verify the recipient's fax number before sending (including preprogrammed number).
- Report any misdirected fax or U.S. mail to your local FCP.

Reference Policy 70.8.014 Safeguarding PHI and Sensitive Information

Safe Disposal of PHI and Confidential Information

PHI must be kept confidential even when it is thrown away.

- Paper records with PHI should be shredded or disposed of in a manner that the PHI can not be read or reconstructed (shredded or put in a locked shredder bin).
- Pill bottles or patient care items with labels that contain patient information should be destroyed and never put in a recycle bin or garbage can.
- Electronic media (CDs, DVDs, backup tapes, etc.) that contain PHI or confidential information must be cleared, overwritten or destroyed so that the information can not be retrieved.

Dignity Health

15

Data Security

Dignity Health

16

Data Security

- Dignity Health is required to monitor and detect any potential privacy or data security breach, including regularly monitoring user network activity.
- Attempts to bypass or override any privacy or data security safeguards to access PHI is a violation of Dignity Health's policies.
- It is the responsibility of all Dignity Health network users to safeguard and protect ePHI.

Information is a valuable Dignity Health asset.

Dignity Health

17

Network Usage Policy 110.2.006 (NUP)

- Dignity Health Network access is a privilege that is granted to users to assist with the performance of Dignity Health business.
- User responsibilities are covered in the Network Usage Policy (110.2.006) that every network user must read and sign.
- Dignity Health regularly monitors user activity.
  - The contents and history of a user's network activity are Dignity Health's property.
  - Any content a user creates or receives via the network is not private nor personal.

Dignity Health

18

Inappropriate Access & Snooping

- PHI may not be accessed without a legitimate business purpose.
- In order to ensure compliance with regulations, Dignity Health requires employees to follow the same authorization procedures as patients.
- It is a violation of Dignity Health policy to use your network access to review your own medical record, PHI of a family member or other individual without the proper authorization.
- Inappropriate access of PHI will result in disciplinary action per HR policy 120.1.006.

Protecting PHI is everyone's job.
PHI is not everyone's business.

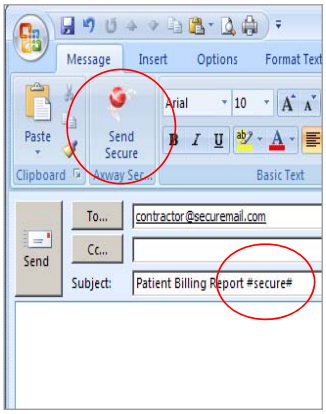
Being Snoopy Can Get You In The Doghouse

Dignity Health

19

110.2.013 Email Policy and Sending Secure Email

- Any PHI or confidential information sent outside of the Dignity Health network requires encryption.
  - Insert a space after the subject, then type #secure# (lower case).
  - If a message is sent without the #secure# tag it will not be encrypted and this may be a reportable incident.
  - You may use the "Send Secure" button if available in your Outlook version.



Dignity Health

20

SharePoint

- SharePoint sites are a great tool for sharing information, but are **not authorized** for posting, sharing, or storing documents with PHI or sensitive information.
- If it is discovered that a document with PHI or sensitive information is posted in a SharePoint site, the site administrator should:
  - Contact the individual user who posted the document and/or their supervisor to alert them that PHI or sensitive documents should not be posted.
  - Site administrator should promptly notify the Facility Compliance Professional.

What Should You Do?

- Dr. Aragon wants to access work information stored on the Dignity Health network from his home, using a laptop provided and supported by Dignity Health.
- Which of the following is a safe way to work remotely?
- (click on a response below)

A. Copy the information to a thumb/flash drive.

B. Use a Virtual Private Network (VPN) or other secure application that is approved by Dignity

C. You should never access the Dignity Health network remotely.

Incorrect Response

This is not the best choice.
Click button to return to question and try again.

Dignity Health

23

Correct Answer

- B. Use a Virtual Private Network (VPN) or other secure application that is approved by Dignity Health.

VPN or other secure method provided by Dignity Health IT should always be used. Bringing data home on portable devices (like thumb drive) or in other physical form can be quite risky. A secure remote access system is the most secure way to access sensitive work data at home.

Click button to continue 

Dignity Health

24

Portable Devices and Social Media

Dignity Health

25

110.2.015 - Portable Device & Media Security Policy

- Electronic information is portable and ePHI can be compromised by lost or stolen laptops, cell phones, CDs, thumb drives, etc.
- Only Dignity Health approved smart phones and tablets may be used to access the Dignity Health network.
- Limit the storage of PHI or other sensitive information on portable computers and media to the minimum necessary to perform the required tasks.
- When PHI or confidential information is stored on a laptop or other portable media, maintain a record, mirror copy or backup on the Network.
- Use appropriate safeguards when using, transporting or storing laptops or removable media.

Dignity Health

26

Removable Media Encryption

- Password protection is NOT the same as encryption!
- You are responsible to ensure all PHI or sensitive data on removable media like memory sticks, CDs or DVDs is properly encrypted and stored in safe location.
- Never save PHI or Sensitive Information to a hard drive or removable media that is not properly encrypted.
- Do NOT use the encryption software to encrypt devices like cell phones, cameras, music players or memory cards as they may be damaged or rendered unusable and/or unrecoverable.

Dignity Health

27

Personal Cell Phone Use

- The use of personal cell phones or other camera-equipped devices must comply with the Network Usage Policy (110.2.006). The scope of this Policy includes smart phones, pagers, tablets and any handheld device.
- All employees, physicians, and contractors are responsible for following policies and procedures to restrict the creating of or use of unauthorized digital images with a cell phone or other camera-capable device.

Dignity Health

28

Texting ePHI and Image Transmission

- PHI sent via unsecured texting represents both a privacy and data security incident that may require patient notification and reporting to regulatory agencies.
- Images sent via text leave a copy of the image on the server of the cellular carrier (i.e. AT & T, Verizon, etc.), the sender's cell phone, and the recipient's cell phone indefinitely.
- Cell phone and data carriers are not business associates of Dignity Health and have no authorization to receive confidential data, and have no obligation to keep messages confidential.

Dignity Health

29

Lost or Stolen Portable Media

- Call the IT Help Desk immediately to report the theft or loss of CD, flash drive, laptop or other portable device that contains PHI or sensitive information.
- Call the IT Help Desk immediately to report theft or loss of your tablet or smart phone that you use to connect to the network.
- The IT Security Team can send a "wipe" command to clear the memory on the device.
- Do not cancel phone service with your provider before notifying the IT Help Desk because the "wipe" command cannot be sent.

Dignity Health

30

Social Media Guidelines

- All employees are expected to conduct themselves in a manner that reflects integrity, as well as shows respect and concern for others, including the use of Social Media.
- Never post confidential information or photo of a patient on the internet, even if it does not include a patient's name.
- Never discuss confidential information in public forums, chat room, text message or news group.
- Inappropriate posts of confidential information or photos can seriously damage Dignity Health's reputation, and result in individual liability for the responsible person(s)

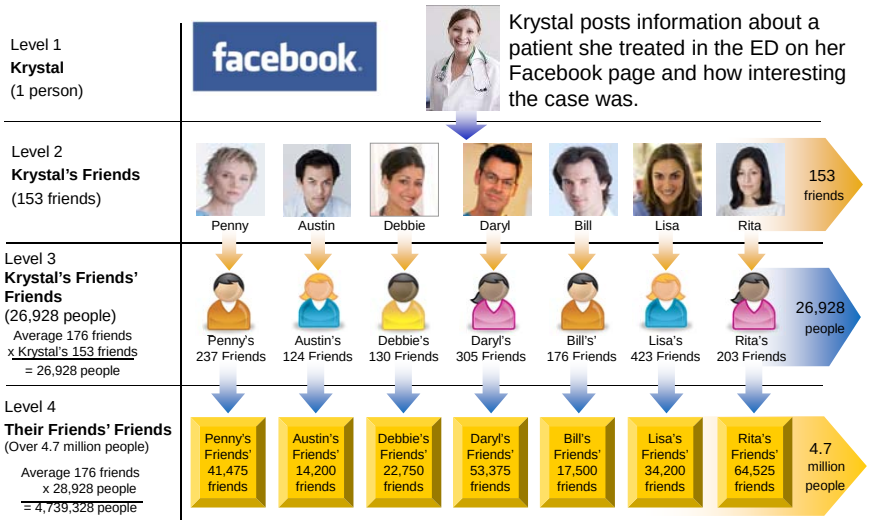
Max was shocked and outraged to find cell phone photos of his recent neuter procedure posted on his veterinarian's FaceBook page.

Think about the consequences that may result from your communications.

Dignity Health

31

The Reality of Social Networks



One person's post grows exponentially based on "friending".

32

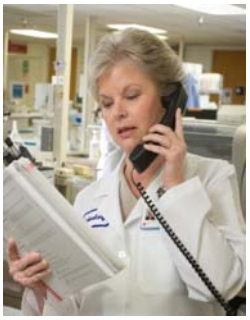
Reporting and Investigations

Dignity Health

33

Reporting Systems

- It is the right and responsibility of every member of Dignity Health's workforce to immediately report any known or suspected violations of laws and regulations, the Standards of Conduct, Dignity Health policies and procedures and any unethical or other improper acts.
- If corrective action is called for, Dignity Health will make appropriate corrections. All reports are taken seriously, reviewed and investigated promptly and employees are provided the option of anonymous reporting.
- In some instances, the facility must report breaches to the Department of Health and Human Services (HHS) and notify the individuals affected.



Dignity Health will not permit retaliation against any employee who reports his or her concerns in good faith.

Dignity Health

34

Reporting Systems (cont'd)

- Dignity Health has maintained a Disclosure Program (Hotline) pre-dating the CIA and it is required by the CIA.
- Per the CIA, any report must be recorded in a disclosure log within 48 hours of receipt and shall include a summary of the report, the status of the respective internal review, and any corrective action taken.
- You should report known or suspected violations of the law, policies or procedures to:
  - Your immediate supervisor / manager
  - Facility Compliance Professional (FCP)
  - Facility IT Site Director
  - Human Resources (for HR related issues)
  - Dignity Health Hotline (anonymous and confidential): 1-800-938-0031
  - Privacy.office@dignityhealth.org (for privacy and data security incidents)

Dignity Health

35

Privacy Considerations for California

Dignity Health

California Privacy Laws

Effective January 1, 2009, California Health & Safety Code 1280.15 (SB541) impacts all Dignity Health facilities.

- Prohibits unauthorized viewing, use or disclosure of medical records without direct need for diagnosis, treatment or other lawful use.
- Requires healthcare organizations to prevent, detect, and investigate unlawful or unauthorized access, use or disclosure of patient medical information.
- Requires that breaches be reported to the California Department of Public Health (CDPH) and affected patient(s) within 5 business days of discovery.
- The alleged violator's name is required as part of reporting.
- Authorizes penalties:
  - $25,000 per patient up to $250,000
  - $100 per day for failure to report.

Dignity Health

37

California Privacy Laws

- Health & Safety Code 130200 (AB211) impacts both Healthcare providers & individuals.
  - Provides private right of action for patients to seek damages as a result of privacy incidents.
  - Places liability directly on the individual who knowingly, willfully or negligently obtains, discloses or uses medical information inappropriately with penalties from $2,500 to $250,000 per violation.

Dignity Health

38

Thank You

- If you have any questions, please contact your local Service Area Compliance Director or Facility Compliance Professional.
- This completes module 2. You will now take the module test.