Module 6 dq1 and 2

Technology, Information Technology

Module 6 DQ1 and 2 John Jones DQ1 One only has to listen to the news to realize that security should be of the utmost importance inmanaging a healthcare facility. There are three separate areas of that subject that will be discussed here; physical, technical and data redundancy. Physical security concerns the safety of the material aspects of the entity, buildings, equipment and people. Such preventive measures as security guards, passkeys and identification tags, locked equipment, and keeping an eye out for unauthorized people are all facets of physical security. Technical security would be those measures taken to protect computers and the like from attacks, viruses, worms, etc. Such things as antivirus software and password or smart card logons help facilitate this.

Data redundancy is backing up necessary computerized information so that it is available elsewhere in the event of a disaster. Most use what is known as a COOP site, an offsite storage area that is reasonably safe from fire, flood, and a myriad of other problems. Because mechanical items fail, data redundancy also can refer to having extra servers and computer equipment available so that the facility can continue to operate (IAHSS 2012). After the devastating effects on healthcare caused by Hurricanes Sandy and Katrina, those administrators would probably agree with this author that redundancy is the most important of the three areas discussed in this paper.

HIPAA 1996 and its successor, PPACA 2009 (Obama Care) do tend to place what appears to be a rather large burden on healthcare providers concerning privacy (HHS 2013). However, as described above, the laws as written attempt to help keep providers

and patients alike comfortable in the knowledge that necessary personal

information (such as social security numbers) is not released to the public, as was the case with the VA employee who lost thousands of SSN’s.

DQ2

The Health Insurance Portability and Accountability Act (HIPAA) provides a list of what it refers to as " identifiable patient information”. Although the law allows the use of the information for clinical use, the Act entails strict privacy rules that must be adhered to (HHS 2013). It specifically disallows release of such information, except in those particular circumstances as outlined. This includes what HIPAA refers to as “ demographic” information as that is defined as those statistics or characteristics that define a certain segment of the population. Such items as name, address, Social Security Number, and date of birth are specified, as well as any state of the patient’s health; physical as well as mental, past, present, and future. In addition, the patient’s monetary status is included, either payments he or she made or monies paid to said patient.

The “ Administrative Requirements” section does indeed list detailed responsibilities for those clinics (entities) receiving Federal money. This is basically all healthcare facilities operating in the country, for all treat some form of Federal patient, either Medicare, Medicaid, or the military Tricare system (Vormetric 2013). As far as strictly adhering to those policies, it is probably true that entities do have written policies. After all, it is easy enough to publish rules and procedures. However, human nature is what it is and it is doubtful that clinics follow all of the policies to the letter. For example, one would doubt a busy employee shreds all of the paperwork containing privacy information. Moreover, the whistleblower protection

against retaliation looks good on paper but one can read many times how that provision did not work.

References

IAHSS (2012), Security Design Guidelines for Healthcare Facilities, Retrieved from:

http://www. iahss. org/REF-MATERIALS/guidelines/designguidelines2012. pdf.

HHS (2013), Summary of the HIPAA Privacy Rule, Retrieved from:

http://www. hhs. gov/ocr/privacy/hipaa/understanding/summary/index. html

HHS (2013), What Information is Protected, Retrieved from:

http://www. hhs. gov/ocr/privacy/hipaa/understanding/summary/index. html

Vormetric (2013), HIPAA Requirements, Retrieved from:

http://www. hipaasurvivalguide. com/hipaa-requirements. php.