Responsibilities of the director of health information

As a Director of Health Information, the scope of expectations covers extensive knowledge and ability in overseeing the integrity of all clinical and financial data and ensuring that providers can access accurate and complete health information at their convenience. A collateral duty associated with ensuring access to critical data is establishing security systems, quality control, and audit programs. It is the responsibility of a Health Information Management (HIM) Director to establish vital auditing programs in order to systematically check the integrity of the organization’s information system. Auditing has been proven to ensure accurate and truthful evaluations of an entity’s operational fidelity; by utilizing a disinterested third party, with nothing to gain or lose by identifying critical vulnerabilities or unethical business practices, outside agencies can rely on these reports to reflect an accurate assessment of the organization’s adherence to the regulations and directives they’re mandated to abide by.

In the case of health information management, a HIM Director could use the results of the audit to ensure that any critical vulnerabilities of their system are identified as soon as possible before a potential breach or spillage of patient data occurs. Historical data will reflect that major organizations will often contract the conception and development of their information delivery system to smaller businesses who often over promise and under develop in order to meet the contract’s requirements in the time provided. This practice is not uncommon, and if not held accountable, the organizations who accept this quality of work often jeopardize the sensitive information they are being charged with protecting. A potential improvement to the auditing process is to establish a procedure of cycling through different outside agencies to

conduct annual audits. By ensuring that the same inspector isn’t performing the inspection every time, HIM Directors will mitigate tantamount results often discovered when the same person or group performs the same function. Different agencies may inspect functional areas differently, which increases the likelihood of the discovery of discrepancies and adverse trends. Through this type of regular auditing, a HIM Director can also determine if the implemented cybersecurity procedures (or e-security) are abiding by the standards outlined in the Company’s policy. Any deviation from the established standards compromises the security of information and adversely affects the Health Organization’s reputation as well as the reputation of the HIM Director.

Breaches and spillages of sensitive patient information is not entirely preventable, there is always a chance for unforeseen circumstances to create the unstable conditions that ultimately lead to the breach in cybersecurity or inaccurate audits. A possible improvement to this functional area of a HIM Director’s scope of responsibility is to ensure they’re vigorously updating their cybersecurity systems to match the rapidly mutating threats. It is another collateral duty for the HIM Director to ensure they are implementing business continuity planning to ensure they are actively responding to deficiencies and ensuring that the proper measures are taken to prepare for the inevitable failure of any part of their health information system; whether it be the tangible items such as additional servers to serve as back-ups or the more intangible function such performing drills to ensure that the staff is aware of and proficient in the implemented damage control procedures. Business continuity planning is critical to

ensuring the longevity of a company in a rapidly evolving environment. If leadership roles ensure they’re properly addressing the significance that continuity planning plays for their subordinate employees, it introduces fresh minds into the conversation and permits for the discovery of innovative ideas to further improve said process.

Commonly, a signature is not obligatory for many healthcare transactions that divulge personal health information for treatment or payment, therefore, the inquiry of e-signatures being used under HIPAA rules becomes superfluous. Yet, when a signed authorization is necessary for a disclosure of personal health information not permitted by the HIPAA Privacy Rule. According to HIPAA, “ not only should the contract, document, agreement, or authorization comply with the federal rules for e-signatures, they should also clearly demonstrate the terms, clearly demonstrate the intent of the signatory, and the option should exist for the signatory to receive a printed or emailed copy of the contract. Covered entities are also advised to seek legal advice about any state or local laws that might also determine can e-signatures be used under HIPAA rules” (HIPAA, 2015).

The Office for Civil Rights (ORC) has created an audit program to ensure HIPAA regulations are being observed and security protocols are being followed. Audits act as compliance improvement to guarantee HIPAA regulations are being observed. Matters regarding compliance discovered and amended through an audit will assist in improving the privacy and security of health records. These audits will inspect compliance with explicit requirements of the Privacy, Security, or Breach Notification Rules and auditees will be informed of the subjects of their audit (HHS Office of the

Secretary, Office for Civil Rights, & Ocr, 2016). These audits will enhance the systems capabilities to meet regulatory requirements and protect information by grading security risks.

Additionally, the use of dashboards as a benchmarking tool will also ensure that regulations are being met. There are multiple dashboards that each service specific tasks when benchmarking that improve performance as well as comply with regulation. According to Eckerson, Operational dashboards observe operational processes, proceedings, and accomplishments as they occur. Tactical dashboards measure and examine the presentation of departmental accomplishments, procedures, and objectives. And Strategic dashboards track development on the way to attaining strategic objectives in a top-down manner (Eckerson, 2011). Each of these dashboards serve as useful tools, some organizations use more than one at a time or even all three. Tactical dashboards support specific departmental objectives that are channeled through IT applications. According to Eckerson, " strategic dashboards often run into political issues that bog down projects, especially when they are deployed top down on an enterprise, as many are. In addition, many strategic dashboards never make the transition from Excel or PowerPoint to a more robust data infrastructure that is needed to deliver clean, timely, integrated data on an ongoing basis with minimal manual effort" (Eckerson, 2011). Operational dashboards are predominantly used by front-line staff to regulate procedures using the greatest up-to-date data imaginable. Eckerson explains that theoretically operational and tactical dashboards observe the function of business procedures, strategic dashboards monitor growth in the direction of attaining

strategy. Operational and tactical dashboards warn users when a process surpasses a stated threshold of operation, while strategic dashboards monitor whether essential actions to progress new or outstanding procedures have been observed and are operating as intended (Eckerson, 2011). These dashboards allow for progress tracking in real time which ensures that the organization will always be within compliance. The moment something goes off track the dashboards will be alerted and will correct any issues to remain in compliance.

Another functional area of a HIM Director’s scope of expectation is to identify the best equipment their team needs that is ergonomic to the user and meets the demands of the workflow. In addition to determining the best equipment for the job, a Director is also expected to recognize human factors that may influence the design of the user interface of health information technologies. By understanding the necessary features of an electronic interface that create an efficient work environment for the user, HIM Directors can determine which product is best suited for the employees as well as the organization. Utilizing systems that are compatible unilaterally between the different departments of a Health Organization and that operate with a common user interface allow the organization to train multiple team members, whom are assigned to different functions of health information systems management, with the same instructional materials. This method allows for one user to operate different roles without any further required training on the interface itself. By programming the user interface with simple visuals

Although standardization isn’t typically synonymous with ergonomics, the way one standardizes an interface that is user-friendly across all departments is the most cost effective means of achieving ergonomics for both the employees and the organization. Simple measures can be taken in order to create a better work environment for the staff. For instance, sit and stand work stations, giving time for periodic breaks, proper lighting, and a peaceful work environment. According to “ cognitive HFE issues include interactions between people and the rest of the system such as perception, memory, attention, mental workload, and support for decision making. At the organizational level, HFE focuses on communication and coordination, teamwork, job design, sociotechnical system, and system design, and change” (Carayon, 2013). By adjusting the work place to meet the needs of both the patients and staff the overall satisfaction and productivity are increased.

There are multiple levels of health IT that all work in conjunction with one and other to create a system. An enterprise data warehouse (EDW) permits all data from an organization with multiple inpatient and outpatient facilities to be combined and evaluated. Enterprise wide information assets that are common to large health care organizations include billing systems, EHR/EMR, master patient index, clinical automation systems, patient portals, personal health records, telemedicine, health information exchange (HIE), clinical applications (lab, pharmacy), etc. The enterprise data warehouse (EDW) is a source of valuable data from diverse information assets and corporate systems/applications. The data enclosed in an EDW can be combined for many strategic uses throughout the enterprise. Strategic purposes may

comprise of undertakings and proposals intended to enhance quality, safety, cost, and efficiency.

Benefits of an EDW include additional support for data, the design capability to track, manage, and examine information, in order to provide a more productive resource. Additionally, EDW’s work alongside other analytics programs to encourage company growth. EWD’s are able to track and adjust marketing campaigns, for expedited, and offer a more precise examination of campaign efficiency. EDW’s enhance data, removing unusable superfluous information, and enhancing total data quality. The user also has the ability to look at information within the platform itself which maintains data integrity. Lastly, costs are often reduced saving the organization money (Salesforce, n. d.).

Data Warehousing could be used in obtaining the strategic objective of growing an organization to become more profitable and cutting out unnecessary spending. By using EWD to remove unnecessary information the quality is improved and the organization runs smoother without any road blocks. This saves the organization money and allows for the profit margin to expand. Through a data warehouse from data mining and also CAC could be used to accomplish the strategic objective. Data warehousing could be implemented when examining the business necessities by collecting and keeping data in a meaningful form. In the use of data mining, the requirements of the organization can be forecasted. Data warehouse can act as a foundation of this.

In order to improve the quality of healthcare an effective strategic plan is paramount to the success of the training program implemented by the organization. A strategic plan is the detailed map that explains how an organization will implement its selected strategy. A good strategic plan reflects the values held within the organization. It clearly states what is most important for achieving success. It assists everyone in their decision making. It allows for everyone to be on the same page, and is focused on pulling everyone in the same direction. If effective, a culture of strategic thinking will be created and practiced in daily decision making. By using strategic planning to evaluate a training program an organization is able to asses and fine tune the program periodically.

Most improvement strategies entail some reworking of the culture within the organization. Patient-focused improvement strategies must consider the needs of patients, as well as the staff. According to the Agency for Healthcare Research and Quality, “ The team also needs to detect factors that could facilitate their work. Facilitators can include financial or non-financial incentives, such as gain sharing for staff if a specific target is met or better quality of life for the staff when a problem is fixed. Other facilitators include picking an aim that is part of the organization’s strategic plan or one that will improve other goals the staff care about, such as clinical outcomes” (AHRQ, p. 4. b, 2015). The key to implementing an effective training plan all depends on the communication within the team. Keeping the team on track and evaluating progress throughout, in addition to rewarding accomplishments, leads the team in the direction of success while reinforcing the culture being implemented through proper training.

Data storage is the practice of keeping the contents of data maintained on a computer and storing it. Off-site storage is storage of data away from the user’s location. An example of this is the cloud. An advantage to off-site storage is the ability to access data from any location via internet access. And the data stored can be dispersed to multiple locations. On-site storage is the practice of storing data at the location of the user on devices such as hard drives. This method is less expensive but requires manual back up and does not require internet access. Removable data storage is able to be removed and taken away from computer. Examples of this storage include USB drives and external hard disk drive. In the case of disaster recovery purposes off site storage is the safest solution. Because the data can be accessed anywhere there is no risk of damage or losing the information.

Spear phishing is quite possibly one of the easiest methods a cyber-attacker can use to gain access into an electronic database, organization’s internal server, or cloud. It is most commonly achieved through the use of emails constructed in a manner that would appear official in its nature and compel the recipient to click on a link that directs the user to a website. Now whether the website appears to official any capacity or simply a spoof webpage is immaterial, by simply clicking on the link the user has inadvertently allowed the cyber-attacker to discreetly download malicious software (also referred to as ‘ malware) onto the targeted employee’s computer. Once the malware has successfully installed, the cyber-attacker is virtually granted all the permissions required to extract whatever data that resides within that server or network. This type of breach is most

problematic for any organization that maintains their data on secure or encrypted networks.

An effective control that can be implemented to reduce the number of breaches by spear phishing is training; it all starts with educating the individual employee on the threat of spear phishing and its catastrophic effects on secure data infrastructure. The more training a company mandates for employees at all levels has a direct correlation with the mitigation of these type of breaches. Furthermore, in addition to establishing annual training procedures, not only can an organization ensure the widest dissemination of vital education but also ensure that its own security team is exercising awareness and maintaining their vigilance against cyber-attacks through systematic internal inspections and audits.

The System Development Life Cycle (SDLC) is a five step process that encompasses theorizing, constructing, applying, and refining hardware, software, or both. When effective, the SDLC must take into consideration any possible security concerns, as well as user requirements throughout the entire process of the life cycle (Broad, 2013).

During the Initiation phase of the SDLC Issues within the organization are identified which then leads to the formation of a plan to address them, in this case the ultimate solution would be implementing an EHR. The same could be done within an REC or HIE when addressing an issue. The design and structure of said system must align with the mission of the organization. Financial considerations must be taken to be sure the new system is a feasible option within the organizations budget. Security is a top priority

because of the risk involved during the initiation phase to insure that private patient information is secured (Broad, 2013).

During the development phase requirements are evaluated that were created in the initiation phase. Based on these evaluations and functional as well as security requirements. One of the biggest challenges that could occurred during implantation with in an REC is integration issues. While still trying to be functional numerous issues could pop up creating tension in the system and delays. Next, in the implementation phase the system is assessed by professionals and any necessary adjustments are made and risk assessments are done. During this phase there could start to be an excessive overhead issue if staff does not properly carry over information gathered from the previous steps. In the operations and maintenance phase the system is fully functional. Periodic reviews are still completed as well as maintenance. The last phase is disposal when changes of technology, systems become obsolete which indicate a limited life expectancy. During this phase the information that was previously being processed by the system must be managed with security being the highest priority (Broad, 2013).

As a Director of Health Information, the scope of expectations covers widespread information and aptitude to oversee the integrity of all clinical and financial data and ensuring that providers can access correct and comprehensive health information at their convenience. By addressing any issues and taking appropriate action to abide by regulations the organization will be more successful and better serve patients.

References

- Agency for Healthcare Research and Quality. (2015, November 16). Section 4: Ways to Approach the Quality Improvement Process. Retrieved from https://www. ahrq. gov/cahps/quality-improvement/improvement-guide/4-approach-qi-process/index. html
- Broad, J., & Mitchneck, A. J. (2013). *Risk management framework a lab-based approach to securing information systems* . Amsterdam: Syngress.
- Carayon. (2013). *Making Health Care Safer II: An Updated Critical Analysis of the Evidence for Patient Safety Practices.* (Vol. 211). Rockville, MD: Agency for Healthcare Research and Quality. doi: https://www. ncbi. nlm. nih. gov/books/NBK133393/
- Eckerson, W. W. (2011). *“ Performance dashboards: Measuring, monitoring, and managing your business, second edition”* .
- HHS Office of the Secretary, Office for Civil Rights, & Ocr. (2016). HIPAA Privacy, Security, and Breach Notification Audit Program. Retrieved fromhttps://www. hhs. gov/hipaa/for-professionals/compliance-enforcement/audit/index. html
- HIPAA. (2015). Can E-Signatures Be Used Under HIPAA Rules? Retrieved from https://www. hipaajournal. com/can-e-signatures-be-used-under-hipaa-rules-2345/
- Salesforce. (n. d.). Advantages of Implementing an Enterprise Data Warehouse. Retrieved from https://www. salesforce. com/hub/analytics/advantages-of-entreprise-data-warehouse/