Mcvh case study data governance

Business

The mall goal Is to have a high quality health care, cost containment, and expansion Into new services, such as Dry.

Brownie’s anticipated Geriatric Medicine department (Hoofer : Rammers, 2011 The team, composed of Heeler, Lopez, Jefferson, and a consultant, has been evaluating various options for integrating the hospital’s operational, clinical, and financial information. An EMMER system would allow physicians to access all medical information for a patient, even though that information is from deferent systems and locations, including various physician, hospital, laboratory, and Insurance records.

As part of a translation from the paper chart to Emirs, and as a way of addressing medical errors, hospitals, including MOVE, are also beginning to take a closer look at computerized physician order entry (COPE) systems. However, COPE may not be a best choice because Physicians have a difficult time to adopt into it like for example; it takes ample time to make changes on a prescription if the requirement does not fall on default values. Traditional ways of writing a prescription is much faster and more invention according to Dry.

Z.

Other Issues they need to address are HAIFA security rules and requirements to protect patient Information. Data governance Is a major concern they need to ensure the quality, availability, integrity, security, and usability of data within an organization. EMMER will be a good pick aside from compliance government gives incentives to use it. President Barack Obama goal in health care program is to have a secure electronic medical record for every American by 2014.

That was part of his administration’s “ first wave” of health reform In the American Recovery and Reinvestment Act, passed by Congress In February 2009.

Starting 2013, health care professionals who effectively use electronic records can receive up to $44, 000 over five years through Medicare or up to $63, 750 over six years through Medicaid. Beginning in 201 5, facilities that don not have the system fully in place will be penalized by lower payments from Medicare and Medicaid. (“ Report: Push For Electronic Medical Records Overlooks Security Gaps”, 2011). Data quality is a big Issue at MOVE. Not knowing where all the documents are, who used It last, who made en recent update Is crucial to ten organizations goal AT Dulling null equal and eliminates errors in the process.

Compared to paper charts EMMER will allow sharing of the data, it is complete, it has audit trail who did what and when did they do it. It will never be misplaced or lost. It can be reproduced in case of major disaster. Data will be easy to locate to consolidate and analyze when needed. With EMMER, providers can track patient data, they can identify patients due for preventive visits, monitor the patient conditions like blood pressure readings, blood sugar level, scores of vaccinations and schedule for regular checkup. It thus improves quality of care in a practice.

Paper chart on the other hand is disorganized, fragmented, and incomplete making it difficult to view overtime. It is manually filed on folders that oftentimes get misplaced or lost, parts of the charts get misplaced or missing or never returned to proper folder. Paper chart cannot be shared to another user or physician unless they make photo copies, which cause redundancies and uncertainness of records. Despite the benefits of Emirs ease of accessibility to data and automation process, it has some vulnerability. Primary concern is security and privacy.

It includes incidents of hacking on EMMER systems that led to altering of patient records or alteration or destruction of clinical systems, improper use of health information records by authorized users of EMMER systems, long-term data management concerns surrounding EMMER systems, and government, and other authority intrusion into private health care matters (Ninja, 2009).

To implement a successful EMMER it will requires a viable, engaged, dynamic, and ongoing security culture. The culture needs constant attention, care, and feeding to maintain the recess.

To make the security culture successful, it must be a high priority at all levels of the organization. The necessary resources and training shall be provided to its entirety. To be effective, a holistic security approach that converges, law, organization policy, professional ethics is the only possible way to mitigate or eliminate threats in healthcare organizations (Snowshoeing).

To accomplish security objectives, upper management should be involved. Getting upper management support sometimes is difficult but very important to obtain.

To get started with selling per management support for a security culture, the following tips may prove to be very useful, adopt a business perspective of the healthcare organization; understand the initiatives and how the business operates. Find a way to educate upper management regarding risks and promote the cost-benefit Justifications of directly addressing them with action. Set metrics that show information security are providing value to the organization.

Provide news stories about healthcare breaches, show the damage they cause why it is important to apply and prevent this from occurring.

Due diligence will go a long way even if a breach does occur. Although there is no proven and true method to sell a security culture to upper management, it is certainly advisable not to ignore the risk. It is important to have a strategy to earn the culture. There is no better fit governance should start from higher level or the executive stakeholders.

After getting an upper management security culture buy-in, next will be a security cultures for users. Users should understand what behaviors are expected in the organization. They should be aware that aside from safety, security is very important when providing healthcare services.

These actions are accomplished by defining policy and procedures. These help guide the organization toward a securely culture Ana addresses responsibility Ana now everyone T also very important that these are not only communicated well throughout the enterprise but also well understood. (Cole).

The Health Information for Economic and Clinical Health Act (HITCH) was released as part of the American Recovery and Reinvestment Act of 2009. Not only does this act build upon existing HAIFA security initiatives, it also provides incentives for the healthcare industry to adopt an information security culture.

HITCH is also the first example of national breach notification legislation. In addition, HITCH provides financial incentives for healthcare facilities to transition toward a secure EMMER infrastructure by the 2014 (Thompson, 2012). Conclusion Protecting health information security is essential for providers and healthcare facilities.

This paper gives an insight the importance of managing the data within an organization’s objectives such as availability, integrity, and compliance with isolations.