**Discussion: Week 7**

In Healthcare 4.0, the patient’s records are stored in electronic health records that are located either at centralized or distributed locations so that providers can access patient information from anywhere at any time. This data is accessed from the database repository via an open channel, such as the Internet, therefore security and privacy are major concerns when this information is assessed from any location.

In today’s world, maintaining patient data privacy is crucial to preserve the integrity of the stored data. Along with the financial setback, Data breaches will affect both individuals and organizations in many ways such as data pilferage that can destroy the image of an organization and brand value. Data breaches can be internal and external. External data breaches are caused by an external source and include hacking, ransomware attacks, phishing, and many more. (Hathaliya., 2019) The scenario presented falls under Internal, and it was done by the end-user and it happened because of the staff who publicly posted the death on social media.

Database design and end-user application affected the patient in this case, therefore ensuring data safety must be the priority in database design because cyberattacks and other threats can lead to data loss and corruption.To address this challenge, when developing a database design, developers must implement robust data backup and recovery strategies, data redundancy, and disaster recovery plans to ensure that if one system fails, another system takes over without loss of data or downtime. There can be issues while managing large amounts of data that can be solved by developing a database architecture called “Data Mesh” that enables to break down silos and distribute data ownership across the organization. This resulted in improved data quality, increased data access, and faster decision-making. (Shivangi, 2023)

**Causes of security breaches:**

**Security breaches can be caused by**cyber-attacks that are used to gain unauthorized access to confidential data. Approaches such as Ransomware and malware are used to expose protected health information. In the scenario presented exposure of confidential health data via the internal source of the organization was the cause of the breach that falls under abuse of privileges.  Other causes can be Improper disposal of unnecessary data leading to the disclosure of protected health information, lack of security awareness training, and poor Cybersecurity framework. (Chipeta, 2023)

**Strategies**

Strategies to prevent this type of circumstance in the future can be identifying all vulnerabilities, segmenting the Network, stopping data leaks, making an **Inventory of all data sets, identifying locations of sensitive information,**strictly limiting privileged access, Securing the network perimeter, limiting lateral movement and many more. Conducting cybersecurity training for employees, contractors, and partners will be an important strategy in the scenario presented because intentional and unintentional mistakes of staff, contractors, and partners represent the biggest threat to data security and the most significant challenge in data breach prevention. Proper training that covers data usage guidelines, password policies, and common threats, such as social engineering and phishing scams, should happen regularly.(Froehlich, 2022) Employee training sessions to familiarize employees with the organization’s policies on the release of information. Employees should be required to take two consecutive weeks of vacation at least once every two years so that if an employee is hacking the organization’s information systems and covering up the unauthorized access, an absence of two weeks is likely long enough to expose what is occurring and when an employee is going to be fired, disabling all the employee’s computer accounts before telling the employee about the termination. (Harrington, 2016)

**References:**

Chipeta, C. (2023, August 3). 5 ways tech companies can prevent data breaches: Upguard. RSS. https://www.upguard.com/blog/how-tech-companies-can-prevent-data-breaches

Froehlich, A. (2022, July 28). How to prevent a data breach: 10 best practices and Tactics. Security. [https://www.techtarget.com/searchsecurity/tip/How-to-prevent-a-data-breach-10-best-practices-and-tacticsLinks to an external site.](https://www.techtarget.com/searchsecurity/tip/How-to-prevent-a-data-breach-10-best-practices-and-tactics)

Harrington, J. (2016). Relational database design and implementation (4th ed.). Cambridge, MA: Morgan Kaufmann. Chapter 23, “Database Security” (pp. 471–494)

Hathaliya, J. J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). [Securing electronics healthcare records in Healthcare 4.0: A biometric-based approachLinks to an external site.Links to an external site.](https://go.openathens.net/redirector/waldenu.edu?url=https://www.sciencedirect.com/science/article/pii/S004579061930062X?via%3Dihub). Computers and Electrical Engineering, 76, 398–410.

Shivangi. (2023, October 13). How to overcome common database design challenges?. RootQuotient. <https://www.rootquotient.com/blog/designing-databases-that-work-overcoming-common-development-obstacles/>

**Response1:**

Thank you for the informative post. Free text can indeed be a challenge when it is used to assess the presence of specific components. Communication from EHR can be done through structured and unstructured pathways. Structured pathways are designed for highly specified and discrete information that can be checked against information elsewhere in the system which enables detecting information mismatch and mitigating medication errors such as incorrect doses, duplicate medications, and allergic reactions before the error reaches the patient.  On the other hand, Unstructured pathways such as free-text fields in medication orders, and free-text orders, have very few content restrictions. The nature of free-text content, the information entered in these orders is not checked against information in the system. There is a lack of safety checks making free-text orders a potentially risky method of entering medication information into the EHR. There can be unintended consequences via the use of free text if it contains unreliable and inconsistent information. (Kandaswamy et al., 2021)

Also, in the scenario sharing of the tragic health information was due to the result of poor end-user controls. Data security and patient privacy are non-negotiable in healthcare. with great power comes great responsibility, and one aspect that cannot be emphasized enough is data security and patient privacy. According to HIPPA security risk and role analysis, “Organizations must develop appropriate administrative, physical and technical safeguards required to protect the confidentiality, integrity, and availability of individually identifiable health information “. Therefore, appropriate training and education can be one way to prevent this type of occurrence in the future.

References:

Kandaswamy, S., Pruitt, Z., Kazi, S., Marquard, J., Owens, S., Hoffman, D. J., Ratwani, R. M., & Hettinger, A. Z. (2021, May). Clinician perceptions on the use of free-text communication orders. Applied clinical informatics. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8172259/

<https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis#:~:text=The%20HIPAA%20Security%20Rule%20requires,and%20security%20of%20this%20information>.

**Response2:**

Hello Emily,

Thank you for the post, you have mentioned in your post that poor database design can lead to improper data entry that makes it difficult to generate accurate reports. Incomplete data that comes from poor database design can lead to misdiagnosis and medical error when clinicians rely on the EHR while roundingand during hand-offs. One of the greatest challenges of EHRs is that they often have been designed without a recognition of the complex and ever-changing cognitive, collaborative, organizational, and structural aspects of interdisciplinary health care delivery. Such systems have traditionally been conceptualized through a billing or overall administrative lens which may not fully align with clinicians’ and patients’ perspectives or information needs. (Holmes et al., 2021) Therefore along with billing and overall administrative areas, when designing EHR health care personal needs should also be taken into consideration for better outcomes.

**References:**

Holmes, J. H., Beinlich, J., Boland, M. R., Bowles, K. H., Chen, Y., Cook, T. S., Demiris, G., Draugelis, M., Fluharty, L., Gabriel, P. E., Grundmeier, R., Hanson, C. W., Herman, D. S., Himes, B. E., Hubbard, R. A., Kahn, C. E., Kim, D., Koppel, R., Long, Q., … Moore, J. H. (2021, May). Why is the electronic health record so challenging for research and clinical care?. Methods of information in medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9295893/