**Misdirected Patient Information Resulting from Data Integrity Error**

Staff at all levels have a role in data entry and in accurately recording patient information whether this involves Medical Staff recording notes in the patient record, administrative staff registering and updating patient demographics, or Finance staff recording guarantor or payer information. The information recorded on the front end of a patient encounter or transaction has a direct impact on the downstream sending of patient correspondence whether this is in electronic or paper form. Maintaining data integrity is an important part of maintaining the privacy and security of patient information and ensuring it is directed to the right individual or location.

This scenario is designed to prompt thinking about ways to improve data integrity whether it involves system controls or processes or human behavior. It is also framed to provide recommended remediation actions in the event data integrity errors are identified. As with many privacy incidents, early intervention will help to mitigate the chance of a privacy issue becoming a privacy breach.

# **Start of Scenario**

Several new staff were being trained in Patient Registration on a day that was particularly busy. Many new patients arrived for surgical appointments and the staff were struggling just to keep up with the workload. All new staff had been trained in their duties, but data integrity and the need to check data entry was not particularly emphasized.

During registration, one patient was particularly agitated at the line to registration and when they met the registrar let them know their displeasure loudly. The registrar entered the patient’s information and then proceeded to the step for address verification. This step entails opening the portal of a contracted service to enter the patient’s demographics (name and DOB) and checking the data entry in the patient record against the returned information.

In this case, the patient had a very common name and the registrar did not enter the middle initial. When several name entries were returned, the registrar just chose the first one thinking it was correct and updated the patient’s electronic record without asking or verifying the address information with the patient. This caused the address in the patient record to be updated to a wrong address. The result was that following the patient’s surgery, information was mailed to the wrong address including bills, test results, and routine correspondence.

## **Questions to consider:**

1. How did the hospital receive notification? Through the patient? Were there instructions on the correspondence for alerting the organization?
2. What process errors occurred when the registrar accessed the verification information?
3. What steps should have been taken to verify the returned information against the patient record?
4. What human behavior could help mitigate the chance of pulling in the wrong information?
5. Who (e.g. compliance officer) in the hospital would need to be notified of this incident?
6. When being investigated, are there electronic record audit entries available showing how the transaction was handled?
7. Is an approved Business Associate being used to provide the address verification?
8. Which departments are likely to identify the misdirected information first? Is there a reporting process in place?
9. How can the risk of the incident rising to a breach be mitigated with the individual(s) or location(s) that received the wrong information?

# **Inject 1:**

About a month after the patient’s surgery, another patient notified the facility that they had received bills that were not theirs and were concerned about identity misuse. They were also concerned about privacy since the name on the bills was not theirs.

## **Questions to consider**

1. What steps can the facility take to investigate this issue?
2. What steps could be taken to identify the scope of the problem (e.g. how many patients may be impacted by situations like these?)
3. What can be done to reduce the risk of a privacy breach from a high to a lower risk of compromise?
4. What criteria would be used to determine if this situation crosses from an inappropriate disclosure into breach territory?
5. If a breach is determined, what steps would the facility take next in terms of patient and government notification?