**Fraud Risk Assessment Team:** This field should include a list of the individuals participating in the Fraud Risk Assessment session.

* Sol Vazquez
* Jason Nazare
* Seun Mafi
* Aerozona Obiadazie
* Tyrell Jarett
* Moriah Striegel

**Assess the Process**

**Process Complexity:** Assess the complexity of the process' moving parts. The more complex a process, the greater the chance that fraud could go undetected.

* CDR application is a single source of data for enterprise that is integrated with the Google Cloud Platform (GCP)
* There are firewalls and connectivity established between various source systems and GCP environment.
* CDR application hosts data from internal and external (contractor) sources for consumption by internal lines of business as well as external partners.
* CDR (Clinical Data Repository) contains sensitive data including PHI and PII
* Give clinical data is stored in the repository; hence, the process is not complex.

**Number of transactions:** The more transactions, the easier fraudsters can hide their crimes. Pay close attention to those processes that generate significant numbers of transactions, and design fraud detection tests accordingly.

* Given CDR is still in its infancy and had only one release, number of data stored in CDR is still minimal.
* **Question: How much data has been stored in CDR, and what is the threshold of scalability of storage over time? GB/TB size (Volume)?**
* The fraud risk around volume is high as a result of CDR hosting hosting data from internal and external (Contractor) sources. Types of data include: clinical data, member/patient and provider look up.
* Number of Transactions do not apply.

**Number of dollars, both large and small:** Auditors may be drawn to focus on the high-dollar transactions that are above a certain threshold. But a significant fraud scheme could be occurring just under established thresholds. In some instances, the smallest transaction could be the indicator of a large, ongoing fraud.

* Does not apply. Scope of audit is around security control regarding data storage.

**Manual vs. automated systems:** Discover if a process is manual or automated. Manual processes may allow for employees' manipulation. Understand the "touch points" in an automated system in which employees can enter, change and extract data.

* **Question: Is there any manual process with data storage from various source systems?**
* **Are there any checks/balances when regard to data flow from external/internal sources into CDR?**
* **User access request, manual process? Maven wave**
* Clinical Data is stored automatically into CDR Repository.

**New systems vs. legacy systems:** New and legacy systems can pose separate unique risks and challenges when you're trying to detect fraud. A new system may cause confusion, operator errors, manual workarounds and breakdowns of existing controls in peripheral systems. A potential fraudster waits for this sort of turmoil and opportunity.

* CDR (Clinical Data Repository) is a new program that is being integrated with the Google Cloud Platform (GCP)

**Question: Will CDR run in parallel with a existing legacy system?**

**Process control by non-employees — outsourced or contractors:** If contractors or non-employees have access to processes, audit staff should assess what frauds they could be committing. Lack of daily oversight and control and lack of their definitive reporting structures to the company could keep these non-employees out of sight and out of mind.

* Internal and external (Contracted) sources have access to store data within CDR.
* Data can be used for financial gain or provided to third parties without consent of company/client.

**Questions: What are the users access rights?**

* **What external users have access to CDR?**

**Internal: What are the potential fraud risk associated with patient health data?**

**External**

Fraud Risks Identified (should be mapped to RCA where controls are identified):

|  |
| --- |
| Data can be used for financial gain or provided to third parties without consent of company/client. |
| Inappropriate access to view clinical data by authorized and unauthorized users. |
| Clinical Data not being encrypted when stored unto repository. |
|  |
|  |