CDR – Information Gathering Session Brainstorm – 6.1.2021

**Initial questions**

What is the goals of CDR?

How many members do they have residing in their now? Future growth?

Any future plans/strategy?

**Data Governance**

1. High level – what is the governance function?
2. Who is part of the governance group?
3. How often do they meet?
   1. What is discussed?
4. Governance policies and procedures?
5. Is any of the data leaving CVS Health?
   1. Do requests go through data governance board?

**Change Management**

1. How are changes managed?
   1. Team on prem that manages or third party?
2. Where are artifacts being held?
3. Who can make changes to the application code?

**Access Management**

1. Who has to CDR?
   1. Super users?
   2. Is this being tracked?
   3. Is logging/monitoring enabled? Is this information being sent somewhere? (Splunk)
   4. Who has access to the Google cloud?
      1. Does anyone at Google have access to our data?
      2. Part of contract/agreement?
   5. How is periodic access review performed? Part of enterprise PAR?
      1. Who is doing it/responsible? (IAM or someone on CDR team)
   6. How is user access provisioned?
      1. Access now?
      2. Or something different.
   7. Is Single Sign On utilized?

**Vulnerability Management**

1. When was the last time the servers have undergone vulnerability scanning?
   1. What servers are associated with CDR?
   2. Who is performing?
   3. When was the last scan?
   4. Policies and procedures – if scans are not completed by EIS.

\*Walkthrough question – How are vulnerabilities remediated.

**Data Integrity**

1. Understand the various source systems feeding into CDR.
   1. How is the CDR team verifying the data against a source system?
   2. How are errors detected and remediated?
      1. Who is responsible for remediating?
      2. Is there an errors report that is generated?

\*Obtain data security, privacy, and legal protocols

**Data Protection**

1. How is data protected (In transit and at rest)?
   1. Masked
   2. Encrypted
2. Data retention policy
3. Business continuity and disaster recovery plans

\*Walkthrough question - Where backups are stored?

* 1. How frequently?
  2. Who is responsible?