**Novologix Claims Edit Walkthrough Meeting**

Monday, January 11, 2021

The reports are generated from the traditional site (The guest)

IT gets the reports from the “HMO” place.

IT will share contacts with us for more info on report

Traditional report: **Natalie**. IT then distributes to the creative part of the team.

We want to understand ITs responsibility:

**What happens if a report does not get available?**

It will be a system issue, and they will know the report was not generated or delayed. IT creates a notification to business team to let them know there will be a delay, when it will be generated and reason for the delay.

Over the last couple months, IT has encountered certain issues relating to this.

The responsibility for running these reports falls under the Application development team. It is part of their production support activity.

(Application Dev team) Referring to key contacts from HS side, from HMP side as well.

**Monitoring Transmission:**

**Q: Do we have any files we submit?**

A: No, those activities are pre-installed. It is part of the monitoring. If there any area of error logs, IT notifies the respective contacts. IT haven't seen much type of major issues such as that. The responsibility of monitoring falls under the application team. Going forward, it will fall under manage service team (project support team) Manage service team consist of a separate unit. They understand what was implemented as a project. They monitor all the activities; it will be like a production monitoring system. If there is a major issue, it will be taken as a production problem and escalated.

**System log application?**

IT has a system log. The process is actually interacting with all application. Change healthcare etc. The system can create data log and check similar groups so that any time there are error logs coming, the system owner is notified.

**Monitoring**.

**Q: Is it real time (frequency)**

A: It is incidental bases. If error is crossing a certain error threshold. It is exported to respective entities for review (Distribution can follow up on the errors)

**Q: Anyone responsible for monitoring these errors?**

A: Not at the moment. Depending on the issue, each team can take a look.

IT will provide contact lists to contacts in production support team, folks monitoring system on constant basis, and also distribution. Once transferred to production support team, their managers are typically responsible.

**Once errors are generated?** IT knows which application it is indicating. Connectivity issue and server issue are mostly common issues found.

Everything is encrypted. Data stored at rest are also kind of encrypted. Other information needed to be available are typically not encrypted.

**Q: If we request a data that is encrypted, can they provide for us?**

A: IT is not sure from a production perspective.

**Q: Any IT requirement in reviewing accuracy and completeness?**

A: There is no day to day regular monitoring.

The manage service team is level one. They raise a ticket, then it moves to level 2 and level 3 respectively.

**Q:** **Are any of the users communicated to Novologix**

**A:** IT has a separate contact. It is taken within the Novologix system and do not need to be taken care of from an IT side.

**Q:** **Any additional question regarding user access, modified user, user provisioning etc?**

**A:** None at this time.

**User entities are responsible for reviewing that access granted to the Novologix System is appropriate based on the access privileges that were requested.**

**User entities are responsible for timely communication of terminated users to the Novologix System**.

From a project perspective. IT Manager responsible. It is part of periodic access review.

**Q:** **Where does IT Lie on terminated user?**

A: It's up to project manager of employee. For contractors, it is done by management.

**User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with the Novologix System.**

This is handled by Global security.

Brian will be providing additional info and contact for "HMO" info.

**Client user IDs and passwords are restricted to authorized personnel with approved and proper assignment, administration oversight (terminations, etc.), and use of the application and direct connection accounts.**

**Q: If there is a security bridge, who is responsible?**

A: The application team is responsible.

**Q; If an account is compromised. How does Novologix know?**

A: It falls under CVS/Aetna security guidelines. They notify global security.

**Q: Who notifies global security?**

A: Whoever notifies this bridge, notifies the manager. IT notifies compliance team.

**Q:** **As an instance occurred that compliance team was brought in?**

A: None.

Communication on a more technical aspect is handled by IT, and business is typically not involved.

Starting next week, they will continue their Triage calls.

**MOVING FORWARD**

IA: We will reconvene with IT and operation and provide some of the controls we have tested and give ample time for Novologix review.