Background

The Oregon Health Authority (OHA) is implementing a Clinical Quality Metrics Registry (CQMR). The CQMR will collect, aggregate, and provide clinical quality metrics data to support quality reporting programs in the state of Oregon. The ability for health care providers and organizations, as well as OHA, to gather and analyze data is a key component to evaluating system performance, improving patient outcomes and reducing costs for Oregonians.

The CQMR will allow health care organizations to review local, regional, and state data to help inform decision-making and measure how they and others are doing to help improve patient care and reduce system costs. It will provide information that can be used to evaluate systems and processes to determine if changes can be made to help meet goals.

OHA and its vendors are committed to the privacy and security of the CQMR and the data in the system. OHA worked with internal privacy and security staff as well as with external stakeholders to develop program and operational requirements and guidelines that serve to safeguard all private information in the CQMR from external threats.

Top Weaknesses in IT Privacy and Security Protection*

***and how we mitigate those weaknesses in CQMR**

There is a saying: "Nobody thinks about safety until there is an accident." There are a multitude of considerations and risks to be observed in privacy and security IT, and it is important to understand some key aspects how OHA works to remediate risks related to the CQMR:

- Collection of personally identifiable information (PII) and personal health information (PHI)
    - Causes for Concern – Programs can create risks through development of poor user privacy provisions, exposure of data to unintended recipients, failure to properly classify.
    - CQMR Risk/Mitigation – The CQMR is a closed system where access is provided only to authorized users who are vetted and verified. Before being granted access to the CQMR, authorized users must complete training and must review and agree to follow the CQMR Policies and Procedures. Users and their organizations are monitored for suspicious behavior and access to data follows the "least necessary access to perform business function" methodology recommended by industry professionals. Particularly sensitive data is restricted to only certain roles. Each organization must identify an administrator who is responsible for identifying the individuals within the organization who should have access and the role that each individual should have. All data is classified (in OHA's system, CQMR data is categorized as data security level 3).
- Hackers/Malware penetrating and accessing customer data including names, addresses, health information, and other PII and PHI.
    - Causes for Concern – Hackers and Malware infection can take advantage of a solution's access to protected health information, financial data or other private data.
    - CQMR Risk/Mitigation – OHA mandates that vendor staff is trained not to expose the platform to threats via phishing, instant messaging, or other external stimulus. Our CQMR vendor uses real-time intrusion

and Malware prevention measures to monitor for 3rd parties attempting to infect the platform. Policies and procedures for use of the CQMR will require training, including training on use of the system and on privacy and security. With respect to financial data, for the quality reporting programs currently supported by the CQMR, OHA does not collect fees. If fees were collected as part of an expanded use case in the future, OHA mandates that vendors do not retain payment information after the transaction has been processed. Additionally, only the minimum required information necessary to process the transaction is provided to the credit card vendor as OHA policy.

- Unpatched vulnerabilities, administration tools access, and data encryption.
  - Causes for Concern – With web-based solutions, unauthorized access to internal tools and interfaces with access to consumer data is a concern. Reports of web control and supporting application vulnerabilities for web applications surface frequently. Solutions may store data in unencrypted or partially unencrypted formats.
  - CQMR Risk/Mitigation – Users cannot access any components of the CQMR over unauthenticated or public interfaces. Additionally, access to data is protected using industry standard access and security protocols and practices. Finally, CQMR data is always encrypted in motion and at rest, so even if someone were able to access the information illegally or attempt to access it during transfer, the data is protected via encryption.

CQMR Security Brief - August 2018

CQMR Security Approach In Review

- Access to the CQMR is available only through the latest HTTPS encrypted and TLS 1.2 compliant web browser interfaces
- Single Sign On Solution provides security and convenience as well as enforcement of Security Assertion Markup Language (SAML) tokens for authentication and Multi-Factor Authentication
- All organizations are reviewed and vetted prior to being granted access to the solution and are able to self-manage user populations
- All data for Oregon customers are segregated from other platform customers and are always encrypted in motion and at rest
- Vendor is compliant with all state identity and theft protection requirements, data retention policies, and federal and state privacy and security requirements and administrative rules
- All security related technology, training, and policies are verified by an independent 3rd party evaluator yearly and by OHA and or their designees per release and quarterly
- OWASP Top 10 Compliant App Scans are performed and assessed before each new release of the solution
- Strong Service Level Agreement (SLA) provisions are in place related to data protection, breach reaction, and resolutions to ensure compliance

CQMR Security Evaluation and Response Process

- How does OSPD respond in the unlikely scenario of a security event?
    - Alert – Vendor notifies OHA within one hour of discovery, and consults with OHA regarding procedures for providing the required notice(s)
    - Stop – Vendor terminates or restricts the access of any users, user accounts, or user services and interfaces associated with the breach (within 24 hours)
    - Notify – OHA begins the established state process of analyzing the breach, determining and correcting the fault, and notifying those affected

CQMR Security Brief - August 2018

List of MiHIN and Salesforce Certifications and Compliancy Certificates