Oculus Health

Security Overview

White paper - March 28, 2015

Introduction

Security and privacy are critical to the success of the Oculus Health platform. Our enterprise policies and processes encompass security, availability, processing integrity, confidentiality and privacy—the core principles that serve as the basis for SOC II and ISO27001. OculusHealth expects to complete the ISO 27001 certification process by early 2015. We are dedicated to continuing to update our solutions and our customers regarding important changes to our current approach.

Safeguards

The Oculus Health platform is designed to enable its members and provider teams to work better together in a highly collaborative, secure and protected environment. We have put the following safeguards in place to best protect our environment and the privacy of your confidential information:

Secure Access, Authentication and Persistence – Access to the OculusHealth platform is via HTTPS (SSL/TLS channel with 256-bit encryption). Additionally, our platform supports single sign-on (SSO) authentication standards to allow for seamless and secure interoperability with customers' existing authentication services. These open, SSO standards include OpenID. Moreover, data is encrypted whenever transmitted and when stored in the Oculus Health platform.

Secure Service Providers – As a software-as-a-service (SaaS)-based system, the Oculus Health platform only engages with enterprise infrastructure-as-a-service (IAAS) and platform-as-a-service (PaaS) providers that meet industry best practices and are compliant with Oculus Health security standards. To help ensure compliance, we review applicable SOC I & SOC II reports.

Network Isolation – Production and non-production networks are logically separated and protected by core firewalls and additional security controls. All administrative access in the Oculus Health platform requires Multi-Factor Authentication (MFA).

Continuous Assessment Model – Oculus Health believes in a continuous assessment model. This model includes static code analysis of all of our code prior to committing. Oculus Health also uses third-party providers to scan the application and network for vulnerabilities. The summary reports from these scans may be shared with customers as part of our Trust Program.

Automated Logging – The OculusHealth platform securely logs all changes to the customer tenant environment, and produces an auditable record of any action taken by OculusHealth or your employees. This allows you and Oculus Health to verify the security and integrity of your data.

Availability, Scalability and Recovery – Oculus Health provides reliable, available service by leveraging the numerous features of Amazon Elastic Compute Cloud (Amazon EC2). OculusHealth can in a secure and reliable manner add capacity in minutes or recover from instance failure.