SYSTEMS AND SECURITY OVERVIEW

Protecting your critical data

It's clear you have a vested interest in keeping your data secure. And at EyeMed, security is everyone's job. That's why we have system controls and protocols based on a comprehensive approach that's secure, managed and verified.

Secure

We're always working to protect internal, client and member data from external eyes.

END-TO-END ENCRYPTION (DATA IN-FLIGHT AND AT-REST)

Whether data is being stored or actively communicated, our system is designed so only appropriate and authorized users can access it. This means no third-party can eavesdrop, decipher or tamper with the data.

TWO-FACTOR AUTHENTICATION

This security enhancement requires 2 types of credentials for logging into accounts. When associates remotely connect to our network, or when members, clients or in-network providers log in to our websites, they need both a unique user ID and PIN.

SECURE CODING PRACTICES

We spot and fix security issues before code goes live through the use of a secure code analyzer. Using the widely accepted development standards of Open Web Application Security Project, our developers are well-trained in secure coding practices.

INDUSTRY-LEADING PLATFORMS

EyeMed is the only vision benefits company using 3 best-in-class systems (leaders in claims software, payment/billing processes and data management) to deliver a secure design and approach.

Managed

We have tools, training and tracking in place to meet rigorous security standards.

VENDOR OVERSIGHT

We conduct annual assessments of critical vendors through systemic tracking and regular site visits. We review security controls and compliance practices to make sure they satisfy our exacting criteria.

Over 1/3 of Americans have been the victim of a healthcare data breach[1]

Around the world, 7 million records are lost or stolen every day[2]

An average breach costs companies nearly $4 million[3]

[1] Washington Post, March 2015. [2] Data Privacy and New Regulations Take Center Stage"; 2018 Breach Level Index Report by Gemalto; accessed October 2018. [3] 2018 Cost of a Data Breach Study, by Ponemon; https//www.ibm.com/

SECURITY AWARENESS

Each of our associates is trained every year in security and compliance. In 2017, we earned industry honors for our interactive and engaging education approach.

24/7 COMMAND CENTER

We keep a close eye on our systems to make sure they're running like they should. 24/7 oversight – located right in our corporate headquarters, using advanced tools and dashboards.

TIER III CERTIFICATION

Our data center earned a Tier III certification from the Uptime Institute, a global authority on infrastructure performance and reliability. Among other things, it means that our data center keeps running during equipment replacement and maintenance.

Verified

We use third-party partners to test, prod and probe for weak points; then we do it again.

VULNERABILITY SCANS

Our equipment, applications and code are regularly checked by third-party experts to report on potential risks and prevent breaches.

PENETRATION TESTING

We don't stop with vulnerability scans – we take it a step further. We hire third-parties who actively try to poke holes and exploit any weaknesses in our system architecture.

SOC 1 AND SOC 2 SECURITY ASSESSMENTS

Every year, we undergo an even more thorough review by an AICPA-certified organization that covers our business operations and security practices.

24/7

Committed to 24/7 monitoring over our systems, located in our corporate headquarters.

Tier III

certified data center by Uptime Institute®

S-1808-CB-625