Eyeonic Cybersecurity Best Practice - Key Features that Ensure a Robust and Secure Customer Experience

1. Executive summary

Eyeonic has pioneered a novel web based application that is revolutionising visual field testing. Understandably, customers and end users want to know how the application has ensured Data Security and what preventative measures have been taken to defend against potential cyber crime.

In the last decade, cyberattacks targeting healthcare organisations have featured prominently in the news media, with incidents revealing compromised patient records by malicious actors. These reports have instilled significant caution among individuals regarding the use of web-based tools within the healthcare industry.

Likewise, businesses that depend on an online presence for transactions have experienced service disruptions or faced ransom demands after their sensitive data was encrypted, hindering operations until a ransom payment is made.

Many cyberattacks have targeted older applications or legacy systems as they present a “soft target” for online criminals with malicious intent.

This report outlines the measures undertaken by Eyeonic to safeguard data privacy, emphasising the central role of cybersecurity within the application. Combining industry recognised best practices, such as robust log on credentials, with a state of the art secure cyber environment, this novel application is one of a new generation of web based tools that ensure a safe and secure experience.

From the user interaction of patients and clinicians who demand a safe, rapid and reliable test, to those that develop and manage the application, every aspect is briefly summarised and the implemented security features highlighted.

2. Introduction

Eyeonic is a pioneering Australian company that is revolutionising glaucoma detection with its web based Visual Field Test. Through innovative technology and a future-forward approach, Eyeonic aims to redefine how visual field testing is conducted and results accessed and processed.

At the heart of Eyeonic's offering is a cutting-edge web-based application designed to facilitate visual field testing. Unlike traditional methods that require specialised equipment and dedicated testing facilities, Eyeonic's application enables visual field testing to be performed conveniently on any computer or tablet device. This approach significantly reduces the cost associated with testing, making it more accessible to a broader range of individuals.

Moreover, Eyeonic's web-based application enhances the overall user experience of visual field testing. By leveraging intuitive interfaces and modern design principles, the

application provides a seamless and user-friendly testing experience, ensuring that individuals can undergo testing with ease and confidence.

Eyeonic's solution enables proper digital integration with modern electronic medical records (EMRs) and telemedicine systems. Though not currently available, this integration will soon allow healthcare providers to seamlessly capture and store visual field test results within existing patient records, streamlining clinical workflows and facilitating more informed decision-making.

The prevalence of cybercrime, which encompasses various criminal activities conducted online, is a significant and escalating concern in today's digital health landscape. Cybercriminals employ a wide range of tactics and techniques to exploit vulnerabilities in computer systems, networks (3), and software applications and pose serious threats to individuals, businesses, and organisations.

Among the sectors frequently targeted by cybercriminals, healthcare organisations stand out as particularly vulnerable due to the sensitive nature of the data they handle and the critical services they provide (4). The healthcare industry is entrusted with critical personal and medical information, making it an attractive target for cyberattacks aimed at stealing data, disrupting operations, or extorting ransom payments.

One notorious cyberattack that underscored the vulnerability of healthcare organisations was the Wannacry ransomware assault in 2017 (5). This widespread attack infected hundreds of thousands of computers across the globe, encrypting their data and demanding ransom payments in exchange for decryption keys. The impact was particularly severe in the United Kingdom, where the National Health Service (NHS) was heavily affected. The attack disrupted vital healthcare services, forcing hospitals to cancel appointments, divert patients, and revert to manual processes to mitigate the damage.

In the past, healthcare organisations have been perceived as vulnerable targets due to their focus on patient care and reliance on a variety of IT systems to enhance and expedite services (6). While these IT systems themselves may not be inherently insecure, each system may have varying levels of susceptibility to cyber-attacks. Cybersecurity measures associated with older platforms in the healthcare industry often involve applying a general layer of protection across existing systems, some of which may still use outdated operating systems.

The Wannacry incident was a wake-up call for healthcare organisations and governments worldwide, highlighting the urgent need for improved cybersecurity measures and greater resilience against cyber threats. It highlighted the importance of implementing robust security protocols, regular software updates, and enhancing cybersecurity awareness and training among staff (8).

Most cyber attacks on healthcare organisations are for financial gain. Cybercriminals aim to either steal patient records or extort payments by encrypting data and rendering it inaccessible to its rightful owner. While an individual medical record may fetch around US$20 on the black market, its value increases 100 fold if used to create fake prescriptions, passports, and other documents (1).

Given the heightened awareness of cybercrime, new and innovative IT-based medical tools must undergo thorough scrutiny (7) to guarantee protection against criminal attacks and ensure their operation is entirely safe and secure.

Eyeonic has taken all concerns associated with data privacy and cybersecurity into consideration when developing its groundbreaking online visual field product. As a newcomer in the field, cybersecurity is not just an add-on but an integral part of the platform's core framework. Collaborating closely with Microsoft experts, the Eyeonic team has engineered a resilient and secure service that seamlessly integrates cloud computing.

Cybersecurity measures are deeply embedded within every aspect of the platform's architecture, safeguarding sensitive patient data and bolstering trust among users. By prioritising security from the outset, Eyeonic demonstrates its commitment to delivering cutting-edge solutions while maintaining the highest standards of data protection and privacy.

3. How Eyeonic implements robust Data Safety and secure operation

Let’s examine how Eyeonic ensures a safe, secure and reliable service by grouping the features into two; those important to external users and those employed internally within the company. “External users” are those who access the Eyeonic Visual Field Test application; namely Clinicians and Patients. “Internal systems” include all of the design features, safety protocols and organisational structures that combined ensure a robust cybersecure ecosystem.

3.1 Cybersecurity measures for external users

3.1.1 Overview

Data Privacy is a primary concern of many individuals that use online, web based resources. An extremely important initial point to make is that Eyeonic does not sell information from Patients or Clinicians to any third parties.

The Eyeonic Visual Field Test application is accessible solely through secure HTTPS protocols. HTTPS ensures that data is encrypted while in transit, safeguarding it in both directions—when transmitted to and from the origin server. By encrypting communications, the protocol effectively prevents malicious entities from intercepting and observing the data being transmitted. Consequently, usernames and passwords are protected against theft during transmission when users input them into a form.

Stringent password policies are implemented for user accounts, requiring a combination of letters, numbers, and symbols to bolster security measures. Using a diverse range of characters significantly reduces the likelihood of unauthorised access and fortifies the overall integrity of the system. This approach not only enhances the resilience against brute-force attacks but also elevates the overall robustness of the authentication process, thereby safeguarding user accounts from potential breaches.

User authentication and password management are entrusted to a reputable and globally recognised entity, Auth0. Renowned for its reliability, Auth0 serves as an authentication and authorisation service utilised by numerous Bluechip companies and boasts a robust infrastructure that incorporates multi-layered security protocols. (9)

Like thousands of global enterprises, the Eyeonic web application uses hCaptcha as another line of protection. CAPTCHA or “Completely Automated Public Turing test to tell Computers and Humans Apart” distinguishes between humans and automated bots. hCaptcha is often used by websites and online services to prevent spam, abuse, and other malicious activities by remote bots, while also providing a more user-friendly experience compared to earlier text based CAPTCHA systems (10)

The application includes a stringent data privacy policy, which has been established in strict accordance with legal regulations. Additionally, there are separate terms and conditions for clinicians and patients that users must carefully read and acknowledge during the signup process. These policies serve to ensure transparency, protect user privacy, and outline the responsibilities and expectations of both the users and the application provider. By requiring users to acknowledge these policies upon signup, the application fosters a secure and trustworthy environment for all stakeholders involved.

3.1.2 The Clinician

Clinicians interested in utilising the service are required to provide multiple pieces of identifying information during the registration process. This will be their medical registration number, photo ID (which contains their name and Date of Birth), along with a practice address. Every Clinician account undergoes manual verification by Eyeonic administrative staff to confirm its accuracy. If the provided identifying information is insufficient, the account will be temporarily suspended. In these cases the Clinician will be contacted and advised to provide the appropriate data, at which point it is unfrozen.

3.1.3 The Patient

Like Clinicians, patients are also required to read and acknowledge the legally created data privacy policy along with the terms and conditions prior to signup.

The Eyeonic Visual Field Test is designed to be simple to use for Patients and ensures a smooth and efficient experience. Individuals must create password-controlled accounts online and are guided through the process by instructions on the web page. They have direct control and ownership of their own data and can edit identifying details at any time, including changing their name, date of birth, email, password or even adding an image to their account.

Patients can, if desired, access their visual field data conveniently through their password-protected Eyeonic account. This feature enables patients to maintain control over their data, allowing them to decide whether they want to share it with clinicians. Moreover, patients have the flexibility to deselect clinicians at any time, which immediately revokes the named clinician's access to their test data. This functionality ensures that patients have autonomy over their health information, fostering transparency and trust in the overall process.

All of these best practice measures ensure strict Data Privacy and compliance with International Privacy and data collection laws.

3.1.4 Summary

How Eyeonic implements robust Data Safety and secure operation for users:

- Data Privacy Measures:
  - Eyeonic does not sell patient or clinician information to third parties.
  - Application accessible solely through secure HTTPS protocols, encrypting data in transit.

- Stringent Password Policies:
  - Implemented for user accounts requiring a combination of letters, numbers, and symbols.

- Authentication and Password Management:
  - Entrusted to reputable entity Auth0, renowned for reliability and multi-layered security.
  - Utilises hCaptcha to distinguish between humans and automated bots, preventing spam and abuse.

- Clinician Registration:
  - Strict data privacy policy and terms and conditions established in accordance with legal regulations.
  - Clinicians provide multiple pieces of identifying information, undergo manual verification by Eyeonic staff.

- Patient Registration:
  - Patients required to read and acknowledge data privacy policy and terms and conditions.
  - Patients create password-controlled accounts online.
  - Patients maintain direct control and ownership of their data, including the ability to edit identifying details.
  - Access to visual field data granted to patients, who can choose to share it with clinicians and revoke access at any time.

- Compliance with International Privacy Laws:
  - Ensured through best practice measures, maintaining strict data privacy and compliance.

3.2 Internal Factors that Ensure Cybersecurity

Summarising current cybersecurity issues Bhuyan et al. (2) describe the role of developers as applying "*security-risk-aware programming principles … in developing software*". In modern software development security, above all, is fundamental to the very design of any service.

3.2.1 Firewall for virtual networking

As a first line of defence at Eyeonic, a strict firewall is implemented along with virtual networking rules for databases. These combine to enhance security by reducing the areas that can be attacked by malware and reduces the risk of unauthorised access, data breaches, and other security incidents.

Passwords, which are used to authenticate users or applications, are securely stored and access to them is tightly controlled. Only authorised personnel or systems have access to these passwords.

3.2.2 Using the Azure ecosystem

Ensuring uninterrupted availability of services is imperative for any business, regardless of the time, date and geographical location. Safeguarding against Distributed Denial of Service (DDoS) attacks is paramount to guaranteeing the continuous availability of the Eyeonic service. By proactively defending against DDoS attacks, the integrity and reliability of the service remains uncompromised, allowing users to access it whenever needed without disruption or delay.

Working hand in hand with Microsoft, the Eyeonic development team are utilising the robust Azure ecosystem to help deliver robust and reliable security. For instance Azure DDoS Protection, combined with application design best practices, provide a strong defence against attacks that might halt or severely slow down the application.

Azure also serves as the central element of security for both deploying and hosting the Eyeonic application. The web application is safely hosted within a specialised web container and accessible through the secure Azure Front Door configuration. Acting as a gateway for web applications, Azure Front Door ensures secure access by leveraging the Microsoft Global Edge network to manage incoming traffic and shield the applications from potential malicious attacks.

The Visual Field Test database is securely hosted on an Azure database server, leveraging its high-performance capabilities to ensure swift and responsive database operations. Azure's infrastructure provides a reliable and scalable environment for hosting databases, allowing for efficient management of data storage and retrieval. By leveraging Azure's infrastructure for hosting the secure database, Eyeonic ensures the reliability, scalability, and performance.

To safeguard the integrity and confidentiality of the stored data, robust security measures are implemented. These measures include encryption both at rest and in transit, ensuring that data remains protected whether it's stored on disk or being transmitted over the network. Encryption at rest encrypts the data while it resides on the database server's storage, making it unreadable to unauthorised users or malicious actors who might gain physical access to the server. Encryption in transit encrypts data as it travels between the database server and client applications, preventing eavesdropping or interception by unauthorised parties.

Overall, hosting the database on an Azure database server with robust security features provides Eyeonic with the assurance that it’s data is protected against unauthorised access, interception, or tampering, while also ensuring high performance and reliability for database operations.

3.2.3 Security during Product Development

Eyeonic also follows rigorous security protocols during product development.

In the process of coding the application, a separate and secure database is utilised, again, hosted within an Azure server infrastructure.

All code artifacts, including source code, configuration files, and related assets, are stored within a private Git repository. This Git repository is exclusively accessible to the Eyeonic staff, limiting access to authorised personnel only. Access to the Git repository is fortified with robust two-factor authentication (2FA), requiring users to provide two forms of identification before accessing the codebase.

Using a private Git repository coupled with 2FA enhances the security of the code development environment. It mitigates the risk of unauthorised access, data breaches, or tampering with sensitive code assets.

A well-designed DevOps pipeline is a critical component of modern software development methodologies, functioning as the foundation upon which organisations can deliver software efficiently and effectively. This pipeline integrates various stages of the software development lifecycle, from code creation to deployment and beyond, streamlining processes and enabling rapid iteration and delivery of high-quality software.
By implementing a DevOps pipeline, Eyeonic can achieve its performance goals

Linking Github with Azure web containers creates a secure DevOps pipeline that enhances collaboration, automation, and deployment capabilities. Github serves as the central repository for source code, allowing teams to collaborate on code changes, track revisions, and manage project workflows effectively. Azure web containers provide a reliable environment for hosting applications, enabling seamless deployment and management of software releases.

By integrating Github and Azure web containers within a secure DevOps pipeline, Eyeonic leverages on the strengths of both platforms to accelerate software delivery while ensuring reliability, scalability, and security. This linkage enables teams to automate the deployment process, monitor performance, and respond quickly to changes in customer requirements or market conditions, ultimately driving innovation and business success.

Overall, this approach to code development is a best practice. At Eyeonic, we emphasise cyber-security and confidentiality as top priorities. Our staff are equipped with cutting edge tools and infrastructure which paves the way for seamless collaboration and the creation of high-quality, secure software solutions.

3.2.4 Other security features

When incorporating third-party services like Google Maps into an application, it's crucial to ensure the security of access credentials.

To achieve this, all code is stored in a private Git repository protected by 2FA only accessible by Eyeonic technical staff. Third party services are accessed by secure passwords controlled by Eyeonic technical staff. Keys for all third party services are securely encrypted upon upload from Eyeonic, and only accessible to limited Eyeonic technical staff.

By implementing this secure approach, Eyeonic's technical staff ensures that sensitive credentials used for accessing third-party services are properly protected against unauthorised access or exposure. This mitigates the risk of potential security breaches

and maintains the integrity and confidentiality of the application's interactions with external services.

As a final measure of Eyeonic's commitment to cybersecurity, regular vulnerability assessments are conducted by the technical team to evaluate the security of the Azure system.

3.2.5 Summary

Internal factors that ensure cybersecurity:

- First Line of Defence:
  - Strict firewall and virtual networking rules implemented for databases.
    - Enhances security by reducing attack surface and risk of unauthorised access or data breaches
- Secure Handling of Passwords and Keys:
  - Passwords securely stored, encrypted, and tightly controlled.
- Protection Against DDoS Attacks:
  - Proactive defence against Distributed Denial of Service (DDoS) attacks.
    - Ensures uninterrupted availability of Eyeonic service.
- Azure as Central Element of Security:
  - Azure serves as central security element for deploying and hosting Eyeonic application.
  - Accessible through secure Azure Front Door configuration.
- Secure Hosting and Management:
  - Database securely hosted on Azure database server.
    - Utilises high-performance capabilities for swift operations.
    - Robust security measures including encryption at rest and in transit.
- Strict Security Protocols in Code Development:
  - Separate and secure database hosted on Azure server infrastructure.
  - Code artefacts stored in private Git repository accessible only to Eyeonic staff.
  - Access fortified with robust two-factor authentication (2FA).
- Implementation of Well-Designed DevOps Pipeline:
  - DevOps pipeline integrates various stages of software development lifecycle.
  - Linking Github with Azure web containers enhances collaboration, automation, and deployment capabilities.
- Regular Vulnerability Assessments:
  - Technical team conducts regular vulnerability assessments.

- Evaluates security of Azure system to maintain integrity and reliability of Eyeonic's infrastructure.

4 Conclusion

The web based Eyeonic Visual Field Test application is an innovative advanced glaucoma detection tool. It is accurate, reliable, and user-friendly.

Being a web-based application there may be resistance to its use because of fears associated with Data Privacy and Cybersecurity. However, being an absolutely new application, security and data safety are at the very backbone of the software architecture and implementation. Eyeonic, using industry best practices and working closely with Microsoft engineers, has produced an application that revolutionises vision health management while also being secure, reliable and easy to use.

References

(1) M K McGee “Research Reveals Why Hacked Patient Records Are So Valuable” (https://www.databreachtoday.com/interviews/research-reveals-hacked-patient-records-are-so-valuable-i-3341 (accessed Mar 2024)

(2) SS Buyan et al. “Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations” Journal of Medical Systems 44, 98, 2020

(3) C.S. Kruse, et al. “Cybersecurity in healthcare: A systematic review of modern threats and trends”: Technol. Heal. Care. 25, 1–10, 2017

(4) Elham Abdullah Al-Qarni “Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies”: International Journal of Advanced Computer Science and Applications 14, 5, 2023

5) L. Coventry Lynne et al. “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward”: Maturitas, Volume 113, 48 - 52, 2018

(6) Osterman Research “Cybersecurity in Healthcare” – White Paper February 2020 (https://ostermanresearch.com/2020/02/28/orwp_0323/ accessed March 2024)

(7) G Bell and M Ebert “Health Care and Cyber Security: Increasing Threats Require Increased Capabilities”: KPMG White Paper (https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf accessed March 2024)

(8) R.S. Ross, et al. “Rethinking Security through Systems Security Engineering” ITL Bull. - December 2016. (https://www.nist.gov/publications/rethinking-security- through-systems-security-engineering - accessed March 2024).

(9) Auth0 by Okta https://auth0.com/

(10) hCaptcha Enterprise https://www.hcaptcha.com/