# Security Plan for the Clinical Care Pathway Project

# INDIVIDUAL ASSIGNMENT #2 – (STROKE PREVENTION APP)

1. **TRA (Threat Risk Assessment) Summary Matrix:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Description** | **Severity** | **Likelihood** | **Recommendation** |
| 1 | **Unauthorized access to user data by malicious insiders** | High  (Due to the sensitivity of personal health information and violation of PHIPA) | Moderate  (App implements robust security controls, but threats like hacking and insider threats can never be entirely eliminated) | Implement AWS Cognito for user authentication with multi-factor authentication (MFA), enforce Role-Based Access Control (RBAC) using Amazon Web Services Identity and Access Management (AWS IAM), encrypt data at rest with AWS KMS (Key Management Service), conduct security audits and penetration testing, establish an incident response plan2. |
| 2 | **PHI Data breaches due to app vulnerabilities** | High  (Due to the potential exposure of sensitive health data leading to legal issues) | Moderate  (Since secure app development practices and vulnerability management processes are established, but still vulnerabilities can be introduced in the application) | Make sure that the app is PIPEDA compliant, adopt coding practices with high level of security, perform security testing, leverage AWS2 for protection of data and monitoring the threats |
| 3 | **DoS attacks by malicious actor disrupting app availability** | Medium  (Although affects the availability of the application, but doesn’t lead to data exposure directly) | Low  (Has good DDoS mitigation strategies and failover mechanisms such as firewall configurations). | Implement load balancing, leverage cloud provider DDoS mitigation services1, monitor firewall1. |
| 4 | **Malware infections compromising the security of the application** | Medium  (As it can lead unauthorized access and expose the personal data) | Moderate  (Because of the risk of users inadvertently installing malware or becoming victim of phishing attacks) | Provide user education, ensure regular updates of the application, consider app shielding techniques like data encryption1. |
| 5 | **Non-compliance with regulations due to PHI data mishandling** | High  (Due to the potential legal and financial implications of non-compliance) | Low  (Due to implementation of robust compliance program and employee training) | Ensure that compliance program are in place, conduct regular audits, provide security awareness training5. |
| 6 | **User profiling or tracking without consent** | Medium  (As it violates user data privacy principles) | Low  (As privacy-by-design principles and user consent mechanisms are implemented) | Implement privacy-by-design principles, obtain explicit user consent, provide transparency on data handling practices. |
| 7 | **Vulnerabilities introduced by third-parties** | Medium  (As it can potentially lead to data exposure or unauthorized access) | Moderate  (Due to the inherent risks associated with third-party integrations and the need for regular monitoring and update) | Conduct security assessments of third-parties, establish safe API gateways, monitor integrations. |

1. **PIA (Privacy Impact Assessment) Summary Matrix:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Personal Information** | **Collected By? From? How? When? Where? Why?** | **Used By? How? When? Where? Why?** | **Retained By? How? When? Where? Why?** | **Disclosed By? To? How? When? Where? Why?** | **Risk and Recommendation** |
| **User Demographics** | App; User; During sign up; To create user profile and personalize content. | App; To tailor educational materials, track progress. | Cloud (AWS) Database¹; For as long as necessary to provide services. | Not Disclosed. | High risk. Implement robust access controls², data encryption³, and obtain explicit user consent⁵. |
| **Health Information** | App; User; Through self-reporting and wearables; To evaluate stroke risk and provide personalized interventions. | App; To calculate stroke risk, provide educational materials. | Cloud Database¹; For as long as necessary to provide services. | Healthcare Providers (with consent); For care coordination. | High risk. Ensure compliance with health regulations⁵, implement data protection measures³, obtain user consent⁵. |
| **Activity Tracking** | App; User; Through inputs and wearables; To monitor lifestyle habits and identify improvement areas. | App; To provide personalized health coaching, set goals. | Cloud Database¹; For as long as necessary to provide services. | Not Disclosed. | Medium risk. Implement secure data transmission protocols³, obtain user consent⁵. |
| **Medication and Appointment Info** | App; User; Through inputs and healthcare systems; To provide reminders and track adherence. | App; To send reminders for medication intake and appointments. | Cloud Database¹; For as long as necessary to provide services. | Healthcare Providers (with consent); For care coordination. | High risk. Ensure strict access controls², data encryption³, and obtain user consent⁵. |
| **User Preferences and App Usage Data** | App; User; Through interaction within app; To personalize app experience and track usage analytics. | App; To tailor user interface and content delivery. | Cloud Database¹; For as long as necessary to provide services. | Not Disclosed. | Medium risk. Implement data anonymization techniques⁴, obtain user consent⁵. |

# Security Plan for the Stroke Prevention App

The security plan for our Stroke Prevention App aims to safeguard the confidentiality of users’ data while adhering to the Canadian regulations5. By employing a defense-in-depth cybersecurity strategy1, our security plan establishes a comprehensive range of security measures and controls at multiple levels for preventing potential cybersecurity threats and for addressing the vulnerabilities effectively.   
  
**Access Controls and Authentication**  
Our plan includes the deployment of advanced authentication channels, like multi-factor authentication (MFA)2 and role-based access controls (RBAC)2, for secure user access and verification. As part of our strict password policy, we will hash passwords and change them on a regular basis to make things safer. Access for users will be tightly limited based on their roles and permissions. This way, patients will only be able to see their own health data and healthcare professionals will only be able to see data for patients who have provided them the access.

**Data Protection**  
PHI will be encrypted using Advanced Encryption Standard (AES-256)3 and other industry-standard algorithms. Based on the data sensitivity , suitable access controls and encryption levels will be put in place. In case there is a system failure, we plan to establish regular data back-ups and recovery plans to make sure that data is available throughout that period.  
  
**Secure Development and Vulnerability Management**  
Secure coding practices, such as input validation, secure coding techniques, and vulnerability testing4 will be taken into consideration. A vulnerability management program will be executed, which will include regular security updates to address identified vulnerabilities. Additionally, security audits will be conducted timely to identify and remediate potential vulnerabilities   
  
**Threat Mitigation**  
Protection against Denial of Service (DoS) attacks, will be accomplished through cloud-based DDoS protection services and load balancing techniques to manage traffic efficiently1. The application will be shielded from the prevalent web attackers by Web Application Firewalls (WAFs)1. We will also launch a user education program which will focus on cybersecurity awareness to reduce the risk of phishing and malware.  
  
**Compliance and Privacy**  
The security plan ensures compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA)5 by implementing robust access controls, auditing mechanisms, and end-to-end encryption of sensitive data. Regular audits and assessments will be conducted based on PIPEDA requirements and industry guidelines (e.g., FHIR)5 to ensure ongoing compliance. Privacy-by-design principles will be used throughout the entire development and deployment process of the app to ensure that user privacy is a top concern from the start.  
 **Third-Party Integrations**  
Third-party services, such as APIs and wearable tech, will not be added until security checks and attack tests are completed.6. We will set up secure communication methods and use OAuth 2.0 for authentication2, and conduct periodic reviews to fix any emergent compatibility problems.  
  
**Incident Response and Breach Notification**  
A detailed incident response plan will outline swift identification, containment, and mitigation strategies for security incidents. In line with PIPEDA guidelines5, our breach notification process will make sure that affected parties and regulatory bodies are notified right away after a data breach.

**References**

1. NIST Cybersecurity Framework (CSF). National Institute of Standards and Technology. <https://www.nist.gov/cyberframework>

2. AWS Security Best Practices. Amazon Web Services. <https://aws.amazon.com/security/>

3. ISO/IEC 27001:2013. International Organization for Standardization. <https://www.iso.org/isoiec-27001-information-security.html>

4. OWASP Top 10. OWASP Foundation. <https://owasp.org/www-project-top-ten/>

5. PIPEDA Compliance Guidelines. Office of the Privacy Commissioner of Canada. <https://www.priv.gc.ca/en/>

6. CERT Secure Coding Standards. Software Engineering Institute Carnegie Mellon University. [https://wiki.sei.cmu.edu/confluence/display/seccode](https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/)

7. OWASP Secure Coding Practices. OWASP Foundation <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/>