IPCIUM Holdings Pty Ltd
(ACN 647 647 194)

Suite 4D,
19 Lang Parade
Milton QLD 4064
Australia

CDMiQ + MyPERSN Platform Security Protocols

Security and protection of patient health data is IPCIUM's core business and has been at the forefront of our platform architecture research and development practice. Incorporating best practice security measures and international health data protection standards throughout our development lifecyle. Patient health data is stored in an encrypted form, in a secure private network within AWS (Amazon Web Services) Australian based cloud server. All data within the CDMiQ Application is encrypted at rest and in transit, ensuring protection against unauthorised access.

Industry leading user authentication and authorisation mechanisms are utilised to further protect our platform against malicious activities and security breaches. IPCIUM's platform has the inbuilt capability to automatically detect malicous activity. For example, when an individual (or generator) enters an incorrect password multiple times within a short timeframe whilst trying to access the platform at log-in, the system triggers an alert and block the IP address from accessing the web enabled application.

Each new feature undergoes a rigourous risk analysis process, which includes research and evaluation of multiple development pathways, interrogation and cross referencing of governing legislation and standards. Every software release undergoes extensive internal testing, across the entire team, including our dedicated Clincial QA Test Analyst.

CDMiQ Current Security Measures

SECURITY MEASURE	DESCRIPTION
AUTHENTICATION & AUTHORISATION	1. Auth0 is employed to provide authentication and authorization services in CDMiQ application. Auth0 follows industry best practices for security and compliance, including encryption of data at rest and in transit, regular security audits, and compliance with privacy regulations like GDPR and HIPAA. 2. Strong password policies and password reuse policy has been configured. 3. All type of data transfer passes through a authorization and filtering layer, which ensure that the user has required authorisation.

DATA ENCRYPTION	1. All patient and platform data is stored in PostgreSQL instance in AWS RDS. All database instances are encrypted at rest. 2. Data is encrypted in transit as application only uses secure HTTPS protocol.
DATA BACKUPS AND DISASTER RECOVERY	1. Databases are frequently backed up automatically throughout the day to protect against data loss due to system failures or other unforeseen events. Restoring database from these backup is highly automated and usually completed within few minutes.
SECURE ARCHITECTURE	1. App servers are deployed using containers (serverless) in AWS cloud. This means we don't need to maintain the security of OS (Operating System) images or instances, instead AWS expert team applies necessary security patches on regular basis to ensure the security of container engines. 2. App containers and database instances resides in private subnet. App containers only accept incoming requests from Elastic Load Balancer and database instance only accept requests from App containers. This ensures that attackers can't gain access to app servers or database instances. 3. Two-factor authentication is enabled for all AWS management users. 4. Security groups are defined with incoming and outgoing rules that only allow incoming requests on specific port and from set IP addresses. 5. Firewall is deployed to protect against malicious activities. Access from only expected geographical locations is permitted. 6. Database servers and app servers are hosted in the same region as the users so that all platform data remain within the geographical boundary to satisfy regulations and compliance needs. 7. Client application is deployed on AWS cloudfront which inherently provides security features like prevention agains DDoS (Distributed Denial of service) attacks, disallowing geographical regions from accessing web app, etc.
INPUT DATA VALIDATION AND SANITIZATION	1. All user input are validated and sanitized to prevent against SQL injection, cross-site scripting (XSS), and other inject attacks. 2. Server automatically strips out invalid data fields from all the incoming requests.
SECURE CODING PRACTICES	1. Usage of hardcoded credentials or sensitive information in the code is avoided. 2. Regularly update and patch third-party libraries to address security vulnerabilities.

	3. Code reviews are performed before every code change is merged to main development branch. 4. Employes are given least privileges to tools and environments to avoid attack vectors targeting admin users. 5. Development machines hard drives are encrypted. 6. VPN is required in order to debug and access QA environments. 7. Only specific users have access to environment logs on-need basis. 8. No sensitive patient data is stored on employee machines. 9. All incoming requests are logged. Important checkpoints in server also generate relavant logs for easy tracing of potential malicious activity.
SECURE DEPLOYMENTS	1. Continous deployments are only done from secure CI/CD (Continous Integration/Continous Deployment) pipelines. 2. Sensitive credentials and environment variables are stored in AWS Secrets Manager. 3. Each environment is separated from another to avoid any accidental cross-bleading of data. i.e, Each environment will required separate login credentials, database, user accounts etc.
REFERENCES & RESOURCES	
CDMIQ PRIVACY POLICY	Attached
CDMIQ TERMS & CONDITIONS	Attached
EU GENERAL DATA PROTECTION REGULATION	https://gdpr-info.eu/ https://gdpr.eu/what-is-gdpr/
GENERAL PRACTICE POLICY AND PROCEDURE TEMPLATES HEALTH INFORMATION AND MEDICAL RESEARCH – OAIC	https://www.oaic.gov.au/privacy-law/privacy-act/health-and-medical-research
INFORMATION SECURITY IN GENERAL PRACTICE	https://www.racgp.org.au/infosec
PRIVACY OF HEALTH INFORMATION	https://www.racgp.org.au/privacy
PRIVACY FOR HEALTH SERVICE PROVIDERS – OAIC	https://www.oaic.gov.au/privacy/privacy-for-health-service-providers/
RACGP USING EMAIL IN GENERAL PRACTICE FACTSHEET	https://www.racgp.org.au/running-a-practice/technology/business-technology/using-email-in-general-practice
SECURE MESSAGING – THE AUSTRALIAN DIGITAL HEALTH AGENCY	https://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/secure-messaging
THE USE OF SECURE ELECTRONIC COMMUNICATION WITHIN THE HEALTH CARE SYSTEM	https://www.racgp.org.au/secure-electroniccommunication