# PRIVACY & SECURITY WHITEPAPER

DAPASOFT | 111 Gordon Baker Road, Suite 600, North York, ON, M2H 3R1

# Executive Summary

Dapasoft's management team is committed to maintaining a mature Information Security, Privacy & Data Protection program. Its key priority is always protecting personal information (PI), including personal health information (PHI)[1], as well as confidential information, and continuously maintaining the information security and privacy controls. This Privacy & Security White Paper gives an overview safeguards in place at Dapasoft to protect its Information Technology (IT) Services, ensure it only uses PI as authorized and supports individuals' privacy rights.

**Dapasoft's Information Security & Privacy Program** follows international ISO/IEC 27001:2013 standard for Information Security Controls and, privacy legislation for PI across Canadian private and public sector organizations (e.g., PIPEDA, Ontario's FIPPA), and PHI across Canadian provincial and U.S. health care providers (e.g., Ontario's PHIPA, U.S. HIPAA) to meet its privacy obligations and to support its customers in meeting their privacy obligations, where relevant. Privacy Impact Assessments (PIAs) and security assessments are periodically performed throughout the organization to ensure the mitigation of any emerging privacy and security risks. Dapasoft defines the privacy and security processes, roles, and responsibilities for implementing information privacy and security management as integral parts of its business and operations.

**Dapasoft Products and Solutions** are developed, operated, and maintained by skilled and certified personnel that are committed to maintaining a comprehensive Information Security control objective. Continuous Security aware controls review, and security testing methodologies are followed to ensure compliance to industry best practices. Specifically

- **Azure cloud services Virtual Networks use a combination of robust security framework including,** logical isolation, firewalls, access controls, authentication, and encryption to protect data in-transit. Microsoft's Azure datacenter operations implement comprehensive information security policies and processes using standardized industry control frameworks such as ISO 27001, SOC 1, and SOC 2. Third-party auditors regularly certify Microsoft's adherence to these standards for both the physical and virtual aspects of Azure infrastructure.

- **Business to Business (B2B) system Interface Encryption and authentication controls are defined** for protecting sensitive information in transit between hospital sites and Corolar Cloud Services.

- **Application security controls are defined** including role base access control for Corolar Application.

- **Dapasoft staff have demonstrated technical knowledge** both in security and application architecture.

[1] PHI includes protected health information under HIPAA, and PI includes personally identifiable information (PII), also under HIPAA.

**IT and Network Security controls** are implemented with comprehensive security architecture defense in depth security principles. The architecture is based on well-proven and widely used secure products, methods, and protocols, and it has been defined to protect data both in transit and at rest and to ensure its confidentiality, integrity, and availability. Strict access control allows only authorized users to access the data

**IT Security Operation** of the Platform follows documented processes and plans. Continuous monitoring of information security and system performance ensures that all deviations and incidents can be responded to in a timely manner by trained and competent personnel in accordance with the incident response process.

**Due to evolving security threat landscape,** Dapasoft's and its Third Party Manage Services Providers monitor for security updates, alerts, and advisories from applicable system and software vendors as well as various security organizations and authorities. Based on risk analysis, the IT Operations and Product team deploys applicable mitigation methods and security controls. Periodic security audits and technical tests performed by independent third-party information security companies ensure that information security fulfills all requirements and meets the highest standards. Dapasoft has also partners with leading Cybersecurity & Privacy firm "iSecurity Consulting" which provides advisory & Manage security & technical validation services for Architecture & Security. Dapasoft commits to conducting Privacy and Security assessments and validate the controls strength of the application and infrastructure services.

# Dapasoft Information Security & Privacy Management System

The information security management system has strategic importance to Dapasoft, as we recognize the importance of information security and confidentiality in a healthcare setting. Our information security management system is an integrated part of Dapasoft operations and governance covering technical, administrative and physical controls.

### POLICIES FOR INFORMATION SECURITY

Dapasoft has internal information security policies defining security requirements and controls. Employee awareness is ensured through new employee induction and regular training thereafter. The policies are reviewed at least annually and approved by Dapasoft's management team.

Dapasoft's customers are required to have their own Privacy & Security in place to ensure equipment which are installed in their local IT requirement also protects the local network.

## Risk Management

Dapasoft conducts periodic security assessments on its IT security program to assess the maturity of its security program along with Technical Vulnerability Assessment & Penetration testing conducted annually on its Network and Infrastructure Services.

## Network Architecture

Dapasoft is responsible for defining architecture standards and validating controls for Third Parties. External facing services include Web Application and Network Firewall along with Threat Detection Controls. Core services such as Web Servers are securely configured with an external facing IP which is only routed via the Load balancer. Application and DB servers are not directly accessible from the Internet.

## Integration services

B2B solutions are implemented for meeting business mandate for data exchange. Dapasoft has implemented a secure Web Services for securely facilitating the data flow

## Technical Security services

Dapasoft's IT technical team have deployed the following controls to protect the hosted infrastructure from any cyber intrusions:

- Anti-Virus and malware prevention services are deployed on all the servers.
- IDS/IPS and Packet Filtering FW is deployed for any inbound traffic inspection.
- Patch and Vulnerability Management services are deployed on Internal zones to facilitates security operations services.

## Software development, testing, and release

Dapasoft follows security standards and best practices for software development, testing, and management. Development and testing are performed in an environment that is separated from production environment.

Software developers are continuously being trained and attend security conferences to keep themselves updated with secure coding practices.

## Vulnerability management

Dapasoft closely monitors IT and Network security updates, alerts, and advisories from various security organizations and authorities to monitor security threats and possible vulnerabilities. Based on risk analysis results, Dapasoft deploys applicable mitigation

methods and security controls when required. Dapasoft maintains the same level of controls in the agreement for its Third Parties and its partners

As part of our commitment to product security, we are also working establishing a product security framework to ensure security updates are on our products are released in an effective and timely manner.

### INCIDENT MANAGEMENT

Dapasoft maintains a detailed IT and Network Security Incident Management Plan. All reported incidents are logged, and the remedial action indicated. Critical security incidents and data breaches are always promptly reported to the affected customers upon discovery.

## Privacy Management:

Dapasoft Privacy Program ensures compliance with privacy legislation in the various jurisdictions and sectors in which it operates, namely Ontario's Personal Health Information Protection Act (PHIPA) where Dapasoft is located, and the various jurisdictions and sectors in which its customers operate, including other Canadian provinces and the U.S. with its Health Insurance Portability and Accountability Act (HIPAA). Although Dapasoft provides its services to Canadian and U.S. customers, Dapasoft stores all customer PHI and PI in Canada.

### POLICY AND PROCEDURES:

Dapasoft has put in place a privacy governance framework to ensure Dapasoft meets its privacy obligations as a technology provider to custodians and that accountability for privacy is assigned to the appropriate individuals. The framework includes policies for the authorized use and protection of the PI Dapasoft processes on behalf of customers. The privacy practices are guided at an enterprise level by the corporate Privacy Policy. The Privacy Policy is supported by several other key privacy policies (e.g., third-party contracting) and procedures and forms (e.g., user access audits, annual privacy program review presentations).

### BREACH MANAGEMENT

Dapasoft has put in place a detailed procedure for managing privacy breaches. The procedure defines privacy breaches, and outlines standard breach management steps to report, contain, investigate, and notify affected customers, as well as remediate privacy program gaps to reduce the likelihood of a similar breach occurring again.

### PRIVACY IMPACT ASSESSMENT:

As part of the privacy program, Dapasoft conducts privacy impact assessment (PIAs) on its infrastructure, programs offered, and any new and updated business process on a regular

basis. PIAs assess Dapasoft governance program as well as identify privacy risks associated with its use and management of customer PI. Summaries of these assessments are made available to customers upon request.

### PRIVACY PROGRAM REVIEW:

An integral part of Dapasoft's privacy program, is regular review of its privacy program to ensure alignment with any changes to privacy legislation and regulatory guidance, agreements with customers, and its services where they impact privacy of PI. Key areas under review include: privacy governance, policies and procedures, privacy and security terms in third-party vendor agreements, outstanding privacy risks from PIAs, and outcomes of user access audits of its employees. Dapasoft reports on its privacy program review to the CEO annually and again provides summaries to customers upon request.

## FREQUENTLY ASKED QUESTIONS:

1. Does Dapasoft has written internal policies, guidelines, and documented practices for the safe handling and protection of data.

   Dapasoft has in place detailed privacy and security governance framework. The framework includes written directives, procedures and forms to document privacy and data protection practices.

2. Does staff receive privacy and security training?

   All staff are required to undergo privacy and security training at the time of hire, and annually thereafter. Delivery of privacy training to staff is tracked, and that all staff sign confidentiality agreements that demonstrate their commitment to uphold Dapasoft's privacy obligations under legislation and its customers

3. Are Dapasoft's product security certified or have gone under security testing and validation services?

   We maintain a secure code environment and are in a process of enhancing practices for validating our systems which include Software and hardware stack. This includes aligning our Product security practices with aligns with Industry Cybersecurity standards.

4. Are Yearly Security Vulnerability Assessment & Penetration Tests conducted?

   Third Party Yearly Penetration Tests are conducted on Corporate IT/IS Network and Product base Security Vulnerability Assessment and Penetration Tests are planned to be completed by year end 2018

5. What Industry Security Framework does Dapasoft follow?

   Dapasoft's Cybersecurity Program follows ISO 27002:2013 Security control objectives and Third-Party Security assessments are conducted on Periodic basis to assess the maturity of the security program.