Data Protection, Privacy & Security Policy

Table of Contents

Cybersecurity

InterSystems commits to its Cybersecurity program by providing appropriate and necessary protections and safeguards to ensure the legitimate use, proper disclosure, and minimal contact of any Personal Information, which, for InterSystems, encompasses the legal and regulatory definitions of personal data, whether InterSystems is a Covered Business, Personal Information Processor, Data Controller, Data Processor, Business Associate, or Covered Entity, to include any and all information or data (regardless of format) that (i) identifies or can be used to identify, contact or locate an individual, or (ii) that relates to an individual, whose identity can be either directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of any attributes or status of such individual.

Our Cybersecurity program uses a framework of controls based on ISO, HIPAA, NIST, APEC CBPR, and EU DPD/GDPR requirements. In order to support Cybersecurity we

(1) identify the specific purposes for which we may need to collect, use, or disclose Personal Information,

(2) operationalize protections surrounding Personal Information relating to the privacy rights of individuals while ensuring availability for proper and authorized uses and disclosures,

(3) implement safeguards to secure the confidentiality, integrity, and availability of Personal Information in our environments,

(4) address education and awareness through a comprehensive Cybersecurity training initiative, and

(5) respond promptly to any actual or suspected threats or vulnerabilities affecting Personal Information.

Our Cybersecurity program is led by our Data Protection Officer:

- *Name:* *Ken Mortensen*
- *Email:* *dpo@intersystems.com*
- *Phone:* *+1 (617) 621-0700*
  +44 (0)1753.855450
- *Post:* *One Congress St, Boston MA 02114 USA*
  One Victoria St, Windsor, Berkshire
  SL4 1HB England UK
- *Message:* *Contact Us Form*

This policy highlights more specifics of our data protection, privacy, and security practices as they pertain to the InterSystems processes, products, and services.

Purposes

Any collection, use, or disclosure (or processing) of Personal Information by InterSystems is directly related to the purposes for which the information was originally gathered either by InterSystems (or on behalf of InterSystems) or by a customer of InterSystems supporting the legitimate interests pursued by the appropriate party, which may be a personal information processor, covered business or data controller. Those interests may include:

- Support and advisory activities relating to InterSystems processes, products, or services, which will include necessary contract and response information for the issue reported (individual requesting support) and any personal information relating to the specific support information.
- Managed Services and hosting activities where InterSystems provides solutions to customers and their end users and participants, which would include not only any personal information relevant to the delivered solution (and any supporting environments), but the personal information of individual end users to the extent supported through the solution and shared with InterSystems.
- Issue investigation and resolution relating to personal information or personal data, including patient records – where this cannot be performed by the local organisation support or without access to the personal information, such as when a user has completed an action in error and wants to undo the transaction or rectify the result or a user is unable to complete an action due to application error.
- Implementation of a new system or an upgrade to existing system, to include testing that the system is functioning correctly, because behaviours may be specific to existing data rather than new data added.

- Data migration services, either during implementation for the population of a new live environment with data from a legacy system or for a major upgrade where database version compatibility is an issue.
- Interface testing where the external system does not have a test environment to which to connect.
- Support of interfaces between clinical systems and disparate operational support systems with patient data.
- Support of national reporting – e.g. Commissioning Data Sets.
- Sales and marketing activities related to InterSystems products and services and the contact information as well as interactions with individuals, including any online activities, attendance at InterSystems' events, and direct inquiries from individuals.
- Internal functions addressing personnel, facilities, and technology resources, such as payroll and email systems.

Technical and Organisational Measures

Privacy Protections

InterSystems incorporates and harmonizes the requirements of privacy and data protection legislation and regulation related to the collection, use, and disclosure of Personal Information through the implementation of Cybersecurity policies and procedures, training on support and operational practices, and controls and measures focused on the relevant protections.

- **Data Protection Officer – Ken Mortensen:** To oversee the accountability of InterSystems in delivering on its promises for data protection.

  InterSystems appointed a privacy and security professional with an IT and legal background to serve as the global Data Protection Officer for the company.

- **Fair Processing:** To assist our customers in carrying out their mission and objectives through our delivery, support, and maintenance of information systems and processes that collect, use, and disclose Personal Information.

  InterSystems educates our customers on the times and scenarios we need information to make sure that Personal Information is processed only in connection with our services. (see our Information Sharing Terms)

- **Lawful Purposes:** To ensure our collection, use, and disclosure of Personal Information links to our support of our customers as data controllers.

  InterSystems uses contracts and procedures with our customers to links any processing of Personal Information to the purposes relevant to the services or support we provide.

- **Minimum Necessary:** To make sure that InterSystems collection, use, and disclosure of Personal Information is adequate, relevant and not excessive.

  InterSystems examines incoming data for Personal Information to ensure receipt only that information relevant and related to the services or support delivered.

- **Data Integrity:** To address the accuracy of Personal Information that is collected, used, and disclosed.

  InterSystems employs its technology to make certain that data, including Personal Information, maintains integrity through our processing while providing our services or support.

- **Limited Retention:** To maintain Personal Information for only as long as appropriate and necessary to address the needs of our customers.

  InterSystems actively uses procedures to remove or to destroy any Personal Information once it is no longer needed to deliver our services or support.

- **Rights of Subjects:** To coordinate with our customers for any responses or inquiries regarding the processing of Personal Information as well as designing solutions permitting effective and efficient accessibility and portability of Personal Information within our products.

  InterSystems communicates with our customers to establish links with their data protection and security personnel to connect any data subject requests back to our customers in a timely and documented fashion.

- **Controls and Measures:** To put in place controls designed to protect privacy and safeguard Personal Information that InterSystems collects, uses, and discloses.

  InterSystems establishes controls for appropriate and necessary safeguards based upon recognized standards, such as ISO 27000 series and HITRUST, and industry best practices. Additionally, to ensure appropriate safeguards for customer environments, we have established the Data Protection Governance standard to govern how customer provide access to InterSystems Personnel.

- **Data Transfer:** To provide appropriate assurances regarding data protection requirements related to any internal sharing or external disclosures outside the country of origin for the Personal Information.

  InterSystems put in place an internal data transfer agreement using the Standard Contractual Clauses between its European entities and its non-European entities, such as in the U.S. and Australia, to obligate the entire organization to privacy and security goals consistent with European data protection laws. Additionally, with

regard to customer information that is personal information, customers must provide specific approval through the Rules of Engagement form (See also the Information Sharing Terms).

Security Safeguards

InterSystems designs and uses controls relevant to ensure the confidentiality, integrity, and availability of Information Assets, especially including Personal Information, based on the ISO 27001/2 standard with enhancement through the NIST SP 800-53r5 and HITRUST standards, as applicable, to ensure that the specific privacy, security, and business objectives of InterSystems and our customers are met. InterSystems takes a holistic, coordinated view of the privacy and security risks in order to implement a comprehensive suite of controls and measures under the overall framework of a coherent management system.

- **Policies and Procedures:** To ensure consistent and comprehensive application of the appropriate and necessary controls and measures, InterSystems documents its privacy and security processes through policies, procedures, standards, work instructions, guidance, and other means.

  InterSystems maintains an Information Security Management System, based upon ISO 27001/2 and NIST SP 800-53, as part of its Integrated Management System that forms the framework for InterSystems risk management program, Cybersecurity. The Data Protection Officer is accountable for the functional attributes of Cybersecurity though data protection, privacy, and security activities.

- **Organization:** To maintain appropriate accountability, InterSystems assigns personnel and third parties to roles that support data protection, privacy, and security responsibilities and to ensure the security of teleworking and use of mobile devices, InterSystems implements specific controls to protect Information Assets.

  InterSystems manages risk through its Cybersecurity program overseen by the Data Protection Officer with the Executive Management responsible for the necessary controls under Cybersecurity through personnel with specialized data protection, privacy, and security knowledge and experience. InterSystems limits access by and use of mobile devices to Information Assets requiring device locking (with at least 4-digit PIN) and restricting downloads of attachments.

- **Human Resources:** To promote understanding by InterSystems employees and contractors that have access to InterSystems' informational assets, including customer data and Personal Information, throughout their lifecycle with InterSystems of their responsibilities as well as to ensure suitability for the roles for which InterSystems employees and contractors are considered.

  InterSystems requires annually that all personnel, both employees and

contractors, to agree in writing to confidentiality obligations regarding Information Assets, especially personal information, and acceptable use regarding Technology Resources. InterSystems changes or terminates any access to Information Assets and use of Technology Resources of an employee or contractor when a role changes or upon leaving InterSystems. Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

- **Asset Management:** To ensure InterSystems identifies organizational assets and defines appropriate protection responsibilities as well as to ensure that information receives an appropriate level of protection in accordance with its importance to InterSystems and our customers.

  InterSystems classifies all categories of Information Assets that it maintains consistent with the relative risk rating to limit or restrict, as appropriate, any access or use. InterSystems uses procedures consistent with NIST SP 800-88, Guidelines for Media Sanitization, including cryptographic erase for any customer information assets (which may include sensitive and personal information), to ensure the appropriate deletion and destruction of Information Assets.

- **Access Control:** To limit access as appropriate and necessary to information assets through the management of authorized user access with accountability of InterSystems employees and contractors to prevent unauthorized access to systems and services.

  InterSystems requires all end users have unique accounts with password complexity (not less than 8 characters in length, disallowing use of compromised values) and lifecycle (expirations and revocation, but generally renewed on an annual basis) consistent with NIST SP 800-63-3, Digital Identity Guidelines (specifically, NIST SP 800-63B, Authentication and Lifecycle Management, including Appendix A, Strength of Memorized Secrets). Remote access to Information Assets requires 2FA (Two-factor Authentication).

- **Cryptography:** To implement cryptographic controls protecting the confidentiality, authenticity, and/or integrity of information, which includes the requirement that customer maintains and manage their own cryptographic material.

  InterSystems deploys at least AES-256 encryption for data-at-rest and at least TLS 1.2 (with SHA-256 and AES cipher suites) for data-in-transit to address the protection of Information Assets containing sensitive or personal information.

- **Physical and Environmental:** To define secure areas for the prevention of unauthorized physical access, damage and interference to the organization's information and information processing facilities and to facilitate the protection of

assets against loss, damage, theft or compromise of assets, and interruption to operations.

InterSystems maintains controls for its facilities (and ensure that its facilities partners, especially outsourced data centers) include specific physical access controls to prevent unauthorized access by establish a specific security perimeter and maintaining Technology Resources within an alarmed and monitored facility with appropriate physical separation of environments.

- **Operations:** To operate systems and facilities in a secure manner protecting against malware, conducting regular data backups to protect against loss of data, logging and monitoring to record events and generate evidence. Managing operational software to confirm the integrity of operational systems, mitigating technical vulnerabilities as discovered, and reviewing information system audit rules to minimize the impact of audit activities on operational systems.

  InterSystems performs secure backups of all environments containing Information Assets with planning and testing done consistent with ISO/IEC 22301, Security and resilience – Business continuity. InterSystems maintains virus and malware protection processes including enforcement of operation on all end user systems and at least daily updates. InterSystems updates Technology Resources within appropriate timeframes as dictated by the risk rating associated with the vulnerability ensuring that critical updates as applied on an expedited basis to prevent operations without known protections. InterSystems periodically scans Technology Resources, including performing penetration tests and vulnerability scans on at least an annual basis, to monitor for any vulnerabilities or weaknesses. InterSystems ensures the operational integrity of Technology Resources through documented operating procedures to maintain those Technology Resources in a manner that safeguards their confidentiality, integrity, and availability.

- **Communications and Networks:** To manage network security for the protection of information in networks and InterSystems information processing facilities and to maintain the security of information transferred both within InterSystems, to/from customers, and with any third party.

  InterSystems logs access, including any attempted access, to Technology Resources to monitor for unauthorized or improper access to and use of Information Assets and, on a risk basis related to the sensitivity and confidentiality of the relevant Information Assets, such as personal information, will lock out access to an environment to ensure protection of those Information Assets.

- **Acquisition, Development, and Maintenance:** To implement security requirements as an integral part of information systems across the entire lifecycle, including those that provide services over public networks, and in our development and support processes to design those requirements as part of the lifecycle of our products and systems.

  InterSystems maintains Technology Resources using a formal configuration and testing process that includes integration of available guidance for secure configurations. InterSystems implements processes that support a secure development process for its products and services through our Secure Coding Practices.

- **Third Parties:** To address information security in our relationships with vendors, suppliers, and other third parties for the protection of Information Assets

  InterSystems requires third parties to agree to specific contractual obligations for data protection in the form of our Information Privacy & Security Requirements and ongoing monitoring that includes the use of the Shared Assessments SIG (Standard Information Gathering) Questionnaire.

- **Incident Response:** To respond to information security incidents consistently and effectively to address security events and weaknesses as well as mitigate risks to information assets, including customer information assets and Personal Information.

  InterSystems investigates discovered privacy and security events to determine if a privacy and/or security incident has occurred and provide appropriate notification to customers and affected parties, including individuals, consistent with local law and regulation. InterSystems maintains an incident response plan as part of its Cybersecurity program with specific procedures to address regional and customer requirements.

- **Business Continuity:** To embed continuity of operations ensuring effective availability and integrity of information assets, which involves the planning and assessment of the business critical operations necessary for performance throughout and following an event impacting InterSystems and our customers.

  InterSystems developed and deploys a business continuity plan to ensure continued operations across its business functions and service delivery, including product and service support, during and following an interruption or disaster event.

- **Risk and Compliance:** To review ongoing compliance to avoid breaches of legal, statutory, regulatory or contractual obligations through information security assessments against InterSystems policies and procedures of implemented and operating controls and measures for information security.

InterSystems maintains certifications through external independent auditors for specific environments, especially those for the maintaining of operational Information Assets of customers, such as Managed Services environments, to cover certifications for Cyber Essentials Plus (Managed Services UK and UK operations), HITRUST (Managed Services US), ISO 27001 (Managed Services UK and UKI operations), and SOC 2/3 (Managed Services US). InterSystems performs internal audits under the Business Continuity, Information Security, Privacy Information, and Service Management Systems on the operations and functions supporting environments maintaining Information Assets.

Training

- Data protection training is provided to each new InterSystems Personnel to ensure an understanding of privacy and information security fundamentals as well as internal policies and procedures for data protection processes.
- All InterSystems Personnel receive data protection, privacy, and information security refresher training on an annual basis with specialized training provided for roles requiring additional knowledge concerning risks and vulnerabilities.
- Awareness and communications concerning risks and vulnerabilities are done on an ongoing basis and reviewed at the start of any project, internal or customer-related.

Security Incident Response

A security incident is any identified breach of access, data handling, or security policy. When identified, a security incident will be addressed with the highest level of response and will receive continuous effort 24/7 until any data risk is removed.

InterSystems has policy and procedure established, implemented and communicated to ensure a consistent and effective approach to managing information security incidents, including communication on security events and weaknesses.

- All security incidents will be reported to InterSystems Data Protection Officer immediately upon detection. The Data Protection Officer will coordinate communication with the customer and affected parties.
- The Vice President of Client Services will be informed and will be responsible for InterSystems senior management communication.
- Security incidents will NOT be documented in support tracking systems, such as WRC or iService in order to ensure that no additional data risk is introduced. Internal incident tracking is used to manage the incident response process including the assessment of the impact and classification of the incident.

- Separate procedures for the identification, collection, acquisition, and preservation of information that can serve as evidence in a disciplinary and legal actions is maintained for each particular operational function affected or involved in an incident and the response.
- Disclosure of security incidents related to Managed Services customers will not be made public without specific written authorization from the customer
- Any incident that results in a data breach will follow InterSystems standard data breach procedure and notification processes in accordance with applicable law.
- For any security incident, the response will prioritize data protection. The relevant InterSystems response team will evaluate the risk and may prioritize data security over system availability.

Following any incident, InterSystems performs a post-incident analysis to identify the root cause of the incident as well as develop a set of lessons learned that can be used to determine if a Plan of Action & Milestone (POA&M) is warranted to follow up on the incident.

The incident response management includes the quantifying and monitoring the types, volumes, and costs of information security incidents and the information gained from the evaluation of information security incidents is used to identify recurring or high impact incidents. With due care of confidentiality aspects, InterSystems uses anecdotes from actual information security incidents in user awareness training as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.

Data Protection

Although our Cybersecurity program looks to protect Personal Information by addressing global privacy and security requirements, InterSystems privacy and security controls are consistent with the obligations under the EU General Data Protection Regulation (GDPR). As noted above, our current controls ensure consistency across the existing principles for data protection and align with the GDPR and ongoing updates to EU member state legislation. InterSystems undertook several actions, some of which are ongoing – as required under GDPR – to address any new issues, in particular:

1. We have appointed a **Data Protection Officer**, as noted above.
2. We have mapped our personal information processing by identifying, as associated with our customers, what, if any, personal information we collection, use, or disclose.
3. We have prioritized relevant actions that include ongoing assessment of the personal information lifecycle and, through our DPO, ensuring our design processes take into account the risks associated with the privacy of individuals and the security of information.

4. We have processes in place to perform Data Protection Impact Assessments (DPIAs) when necessary to understand what if any risks exist to the rights of individuals are impacted by our processing and to identify appropriate and necessary mitigations to address the recognized risks.
5. We have ongoing organizational activities to organize our internal processes, including new and updated privacy and security policies, ongoing assessment of operational processing to ensure effective controls, new training and awareness on data protection for employees, and enhancements to our vendor program for data protection requirements.
6. We have put in place requirements to document decisions related to data protection so that our actions and processing can be explained and properly understood.

InterSystems uses its Cybersecurity program to elevate data protection through our relationships with our customers and continuing to build upon the trust that our customers have with us in delivering quality products and effective services.