HealthShare HS2023-02 Alert

13-NOV-2023

Dear InterSystems Customer:

I am writing because you are listed as the Security Contact for your organization. When risks have been uncovered that concern your use of InterSystems products, we are committed to providing you the necessary information so that you can assess your situation as quickly as possible.

We have identified several risks that may affect you when using InterSystems HealthShare® solutions, and the HealthShare® Health Connect and InterSystems IRIS for Health™ products.

Please read the information that follows. If you have any questions, please contact InterSystems Support at support@intersystems.com or +1.617.621.0700.

We understand and take very seriously our commitment to you to provide an effective and efficient solution while protecting patient safety and safeguarding patient information. Our Alert process complements our existing support processes. If you have questions about our processes for data protection, privacy, security, or clinical safety, including our Global Trust program, you can reach our Data Protection Officer, Ken Mortensen at globaltrust@intersystems.com.

If you ever have any clinical safety, privacy, security or operations related questions about HealthShare, do not hesitate to contact the Worldwide Response Center (WRC) through support@intersystems.com or +1.617.621.0700, so that we can assist you.

Respectfully,

Jonathan Teich, MD, PhD
Director, Product Management – HealthShare

InterSystems
One Memorial Drive
Cambridge, MA 02142
TEL: +1.617.621.0600

Summary of Alerts

Alert	Product & Versions Affected	Risk Category & Score
HS2023-02-01: Security Vulnerability on Patient Index UI Page	• Patient Index ○ All versions prior to 2023.2	Security: 4 - High Risk

HS2023-02-02: Security Vulnerability on Unified Care Record and Clinical Viewer UI Pages	• Unified Care Record
	  ○ All versions prior to 2023.2
	• Clinical Viewer
	  ○ All versions prior to 2023.2
		Security:
		3 - Medium Risk

HS2023-02-03: Security Vulnerability for IRIS for Health and Health Connect FHIR	• InterSystems IRIS for Health
	  ○ All versions prior to 2023.3
	• HealthShare Health Connect
	  ○ All versions prior to 2023.3
		Security:
		3 – Medium Risk

HS2023-02-04: HealthShare User Interface Session Fixation Vulnerability	• HealthShare Solutions products: Unified Care Record, Information Exchange, Clinical Viewer, Provider Directory, Care Community, and Personal Community
	  ○ All versions prior to 2023.1.1
	• InterSystems IRIS for Health and HealthShare Health Connect
	  ○ All versions prior to 2023.3
		Security:
		3 – Medium Risk

HS2023-02-05: HealthShare Mirror Monitor Agent May Perform Undesirable Configuration Steps after Upgrade	• HealthShare Solutions products: Unified Care Record, Patient Index, Provider Directory, Health Insight, Care Community
	  ○ 2022.2 and 2023.1
	• InterSystems IRIS for Health and HealthShare Health Connect
	  ○ 2022.3 , 2023.1.0
		Operational:
		5 – Very High Risk

HS2023-02-06: Possible HealthShare System Downtime Due to Instance Resource Exhaustion	• Unified Care Record (Information Exchange) ○ All versions prior to 2023.1.1	Operational: 5 – Very High Risk
HS2023-02-07: Health Insight Setup Step Restarts the Registry Production, Causing Downtime	• Health Insight: ○ 2022.2, 2023.1, 2023.1.1	Operational: 4 - High Risk

HS2023-02-08: Incorrect SQL Query Results When Runtime Plan Choice (RTPC) Is Enabled	• HealthShare Solutions products: Unified Care Record, Patient Index, Provider Directory, Health Insight, Care Community, Healthcare Action Engine
	  ○ 2022.2
	• Personal Community
	  ○ 2022.7, 2022.8, 2023.1, 2023.2
	• InterSystems IRIS for Health and HealthShare Health Connect
	  ○ 2022.1, 2022.2, 2022.3
		Operational:
		4 - High Risk

Alert	Product & Versions Affected	Risk Category & Score
HS2023-02-09: ODS Purge Logic is Inverted	• Unified Care Record ○ All versions prior to 2023.2	Operational: 3 – Medium Risk
HS2023-02-10: Do Not Use Version Number to Determine How Long to Preserve a FHIR Resource from Purge	• Unified Care Record ○ All versions prior to 2022.2	Operational: 3 – Medium Risk

Detail of Alerts

HS2023-02-01: Security Vulnerability on Patient Index UI Page

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	4-High Risk	Not Applicable

Version and System Area Affected

HealthShare® Products: Patient Index

Versions: All versions prior to 2023.2

System areas affected: UI Security

Reference: HSPI-3151

Summary of Issue

Some Patient Index user interface pages contain a security vulnerability with the following CVSS vector string:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:L/MAC:L/MPR:L/MUI:X/MS:C/MC:H/MI:H/MA:H&version=3.1

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Security: 4- High Risk CVSS overall rating of 7.7

Recommended Actions

Contact the WRC to request an ad hoc patch for HSPI-3151.

Reference Information: HSPI-3151

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-01".

– End of Alert HS2023-02-01 –

HS2023-02-02: Security Vulnerability on Unified Care Record and Clinical Viewer UI Pages

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	3-Medium Risk	Not Applicable

Version and System Area Affected

HealthShare® Products: Unified Care Record, Clinical Viewer

Versions:
- Unified Care Record: All versions prior to 2023.2
- Clinical Viewer: All versions prior to 2023.2

System areas affected: UI Security

Reference: HSCV-17668

Summary of Issue

Some Unified Care Record and Clinical Viewer user interface pages contain a security vulnerability with the following CVSS vector string:

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N&version=3.1

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Security: 3- Medium Risk CVSS Overall Rating of 5.4

Recommended Actions

Contact the WRC to request an ad hoc patch for HSCV-17668.

Reference Information: HSCV-17668

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-02".

– End of Alert HS2023-02-02 –

HS2023-02-03: Security Vulnerability for IRIS for Health and Health Connect FHIR

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	3-Medium Risk	Not Applicable

Version and System Area Affected

HealthShare® Products: InterSystems IRIS for Health, HealthShare Health Connect

Versions: All versions prior to 2023.3

System areas affected: FHIR with OAuth 2.0

Reference: IF-2896

Summary of Issue

InterSystems IRIS for Health and Health Connect systems using FHIR with OAuth2.0 include a security vulnerability with the following CVSS vector string:

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:N/E:F/RL:O/RC:C

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Security: 3- Medium Risk CVSS Overall Rating of 5.4

Recommended Actions

Contact the WRC to request an ad hoc patch for IF-2896.

Reference Information: IF-2896

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-03".

– End of Alert HS2023-02-03 –

HS2023-02-04: HealthShare User Interface Session Fixation Vulnerability

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	3-Medium Risk	Not Applicable

Version and System Area Affected

HealthShare® Products:	• HealthShare Solutions products: Unified Care Record, Information Exchange, Clinical Viewer, Provider Directory, Care Community, and Personal Community • InterSystems IRIS for Health • HealthShare Health Connect
Versions:	• HealthShare Solutions: All versions prior to 2023.1.1 • InterSystems IRIS for Health and HealthShare Health Connect: All versions prior to 2023.3
System areas affected:	Security, Login, Management Portal
Reference:	HSIEO-8613

Summary of Issue

A vulnerability has been discovered in which the UI session information of an authenticated and authorized user may be used by an attacker to gain access to a system and act as the authenticated and authorized user. The vulnerability is described by the following CVSS vector string:

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Security:	3 - Medium Risk	CVSS overall rating of 6.3

Recommended Actions

Contact the WRC to request an ad hoc patch for:

- HSIEO-8613
- HSIEO-8699
- DP-423252
- DP-421886

Reference Information: HSIEO-8613

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-04".

– End of Alert HS2023-02-04 –

HS2023-02-05: HealthShare Mirror Monitor Agent may Perform Undesirable Configuration Changes or Cause Unexpected System Downtime

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	Not Applicable	5-Very High Risk

Version and System Area Affected

HealthShare® Products:	• HealthShare Solutions products: Unified Care Record, Patient Index, Provider Directory, Health Insight, Care Community • InterSystems IRIS for Health • HealthShare Health Connect
Versions:	• HealthShare Solutions 2022.2, 2023.1 • InterSystems IRIS for Health 2022.3 , 2023.1.0, 2023.1.1, 2023.1.2 • Health Connect 2022.3 , 2023.1.0, 2023.1.1, 2023.1.2
System areas affected:	HealthShare Mirroring, Upgrades
Reference:	HSIEO-8820, HSHC-3587

Summary of Issue

The HealthShare Mirror Monitor Agent queues configuration changes made on the primary failover member to also occur on the backup failover member when it becomes the primary. Two separate defects have been observed on the affected products and versions related to the HealthShare Mirror Monitor Agent. The defects only exist on systems that include both of the following criteria:

1. Mirroring is enabled.
2. The HSSYS database is a mirrored database.
   Mirroring of the HSSYS database is required for HealthShare Unified Care Record, but optional for Health Connect and IRIS for Health.

Both defects are fixed by the same set of corrections: HSIEO-8820 which also requires HSHC-3587.

Defect #1

This defect is especially prevalent when upgrading an existing instance to one of the affected versions. In certain situations, it was found that configuration changes that occurred months or years before the upgrade may be mistakenly queued and executed again after the upgrade resulting in undesirable configuration changes to the instance. Configuration changes might have ranged from benign to extremely severe including the deletion of a production database.

An all-inclusive list of possible configuration changes that may be undesirably executed can be found in the class reference documentation for the HS.HC.SystemConfig.API.Methods class

Defect #2

This defect may affect instances that have been upgraded to an affected version or instances that were installed using an affected version. The defect may be encountered at any time on a mirrored instance running an affected version. If the primary and backup instances are not configured to communicate properly, the defect may cause many duplicated configuration steps to be incorrectly queued and executed again after a mirror failover event. The execution of many duplicated configuration steps may cause unplanned system downtime caused by resource exhaustion.

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Operational:	5 – Very High Risk	Severity of typical adverse outcome = 4 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

Contact the WRC to request an ad hoc patch for HSIEO-8820 (which also requires HSHC-3587).

Reference Information: HSIEO-8820, HSHC-3587

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-05".

– End of Alert HS2023-02-05 –

HS2023-02-06: Possible HealthShare System Downtime Due to Instance Resource Exhaustion

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	Not Applicable	5-Very High Risk

Version and System Area Affected

HealthShare® Products:	Unified Care Record (and Information Exchange)
Versions:	All versions prior to 2023.1.1
System areas affected:	Interoperability Productions
Reference:	HSIEO-2173 (and HSPI-2980 if also using Patient Index)

Summary of Issue

In all versions prior to HealthShare 2023.1.1, the HealthShare suite of products were susceptible to entering a troubled state in rare circumstances which could lead to downtime of the Registry or other instance in the federation.

The troubled state would be triggered by any request that took an unexpectedly long time to process by another instance acting as the server. If the server processing time was larger than the *Response Timeout* on the client instance, the client would send duplicate requests ad infinitum to the server, spawning duplicate long-running processes. Over time, the number of processes would grow and cause the server to crash.

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Operational:	5 – Very High Risk	Severity of typical adverse outcome = 4 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

To prevent this issue, contact InterSystems Worldwide Response Center (WRC) to obtain a patches for

- HSIEO-2173
- DP-417266
- DP-417996

Apply the patch to all instances in the HealthShare Federation.

In addition, if the federation uses HealthShare Patient Index, a patch for HSPI-2980 is required as well.

Reference Information: HSIEO-2173 (and HSPI-2980 if also using Patient Index)

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-06".

– End of Alert HS2023-02-06 –

HS2023-02-07: Health Insight Setup Step Restarts the Registry Production, Causing Downtime

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	Not Applicable	4-High Risk

Version and System Area Affected

HealthShare® Products: Health Insight

Versions: 2022.2, 2023.1. 2023.1.1

System areas affected: HealthShare federation downtime

Reference: HSHI-7963

Summary of Issue

In the 2022.2 and 2023.1 versions of HealthShare products, running the `SetHIDataFeed()` method triggers a restart of the Registry production. Restarting the Registry production can be disruptive to the entire HealthShare federation, causing unexpected downtime if it is not planned for.

Running `SetHIDataFeed()` is a necessary step when you do any of the following:

1) Set up a new Health Insight instance
2) Upgrade Health Insight from a pre-2022.2 kit to version 2022.2 or later
3) Switch Health Insight from using the AADBQ Feeder gateway to using System Index

This behavior has been corrected for HealthShare 2023.2.

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Operational:	4 - High Risk	Severity of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

Affected customers should contact the Worldwide Response Center to request an adhoc that includes the fix, HSHI-7963. Alternatively, customers should plan for the Registry restart by stopping all other productions in the federation before running the `SetHIDataFeed()` method.

Reference Information: HSHI-7963

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-07".

– End of Alert HS2023-02-07 –

HS2023-02-08: Incorrect SQL Query Results When Runtime Plan Choice (RTPC) Is Enabled

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	Not Applicable	4-High Risk

Version and System Area Affected

HealthShare® Products:	• HealthShare Solutions products: Unified Care Record, Patient Index, Provider Directory, Health Insight, Care Community, Healthcare Action Engine • Personal Community • InterSystems IRIS for Health • HealthShare Health Connect
Versions:	• HealthShare Solutions products 2022.2 • Personal Community 2022.7, 2022.8, 2023.1, and 2023.2 • InterSystems IRIS for Health 2022.1, 2022.2, 2022.3 • HealthShare Health Connect 2022.1, 2022.2, 2022.3
System areas affected:	SQL Queries
Reference:	HSIEO-8377 (DP-421755)

Summary of Issue

The issue can be triggered when SQL Runtime Plan Choice (RTPC) is enabled (the default) and the query contains a "truth value" WHERE ? = ?. When triggered, some predicates may not be evaluated correctly; this leads to incorrect query results.

Note that it is not possible to fully assess a query's vulnerability by reviewing the SQL. This is because InterSystems SQL query optimization can add truth values to the internal representation of queries.

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Operational:	4 - High Risk	Severity of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

If your environment uses InterSystems SQL, then you can immediately remediate the issue by disabling the RTPC feature. Disabling RTPC may negatively impact SQL query performance, but will remediate the possibility of incorrect SQL query results.

For a permanent solution to the defect in RTPC, either contact the Worldwide Response Center to request a patch or upgrade to one of the following versions:

- HealthShare Solutions products: 2023.1 or later
- Personal Community: 2023.3 or later
- InterSystems IRIS for Health and HealthShare Health Connect: 2022.1.3 or later

Reference Information: HSIEO-8377 (DP-421755)

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-08".

– End of Alert HS2023-02-08 –

HS2023-02-09: ODS Purge Logic is Inverted

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	Not Applicable	3-Medium Risk

Version and System Area Affected

HealthShare® Products: Unified Care Record

Versions: All versions prior to 2023.2

System areas affected: ODS Purging

Reference: HSDD-1468

Summary of Issue

An accidental inversion of query logic on the ODS resulted in incorrect purging behavior for streamlets and FHIR resources. The result is the retention of data that should be purged and purging of data that should be retained. This represents an operational issue with the Unified Care Record as customers may not be able to properly report on data access events within the ODS.

All customers running the ODS on versions prior to Unified Care Record 2023.2 are impacted. If purging is not being used, then this issue has no impact.

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Operational: 3 - Medium Risk

Severity of typical adverse outcome = 1 out of 5
Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

Contact the WRC to request an ad hoc patch for HSDD-1468.

Reference Information: HSDD-1468

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-09".

– End of Alert HS2023-02-09 –

HS2023-02-10: Do Not Use Version Number to Determine How Long to Preserve a FHIR Resource from Purge

Issue date: 13-NOV-2023

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	Not Applicable	3-Medium Risk

Version and System Area Affected

HealthShare® Products: Unified Care Record

Versions: 2019.1, 2019.2, 2020.1, 2020.2, 2021.1, 2021.2, 2022.1, 2022.2

System areas affected: ODS Purging, FHIR

Reference: HSDD-998

Summary of Issue

A flaw in the FHIR Resource versioning and purge logic results in incorrect purging of accessed FHIR resources. This results in a customer's inability to reproduce the data sent over-the-wire when running audit reports.

Customers who meet the following criteria are impacted by this issue:

- Running Unified Care Record with an ODS that is version 2022.2 or older
- Using FHIR on the ODS
- Using purging on the ODS
- Retaining data for auditing

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the Addendum), and based on the following assessments:

Operational:	3 - Medium Risk	Severity of typical adverse outcome = 1 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

Contact the WRC to request an ad hoc patch for HSDD-998. Customers may optionally disable purging until the adhoc is applied.

Reference Information: HSDD-998

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2023-02-10".

– End of Alert HS2023-02-10 –

Addendum

Contents:

Clinical Risk Rating Process

InterSystems' clinical risk rating uses standard methodology to estimate the risk of a system hazard based on the most typical foreseeable adverse patient outcome, as opposed to the worst-case scenario. Experienced clinicians on our clinical safety team provide an estimate of the severity and likelihood using standard ordinal scales to derive the risk category.

Description of Outcome Severity

Scale	Severity Classification	Number of Patients Affected	Interpretation
1	Minimal	Single	Minimal injury from which recovery is expected in the short term. Minor psychological upset. Inconvenience.
2	Minor	Single	Minor injury from which recovery is not expected in the short term. Significant psychological trauma.
		Multiple	Minor injury from which recovery is expected in the short term. Minor psychological upset. Inconvenience.
3	Moderate	Single	Severe injury or incapacity from which recovery is expected in the short term. Severe psychological trauma.
		Multiple	Minor injury from which recovery is not expected in the short term. Significant psychological trauma.
4	Major	Single	Death. Permanent life-changing incapacity. Severe injury or incapacity from which recovery is not expected in the short term.
		Multiple	Severe injury or incapacity from which recovery is expected in the short term. Severe psychological trauma.
5	Catastrophic	Multiple	Death. Permanent life-changing incapacity. Severe injury or incapacity from which recovery is not expected in the short term.

Ordinal scale for the quantification of the severity of a specified patient outcome

Description of Outcome Likelihood

Scale	Likelihood Classification	Interpretation	Frequency
1	Very low likelihood of harm	Harm will probably never happen/recur	Harm not expected to occur for years
2	Low likelihood of harm	Do not expect harm to happen/recur but it is possible it may do so	Harm expected to occur at least annually
3	Medium likelihood of harm	Harm might happen or recur occasionally	Harm expected to occur at least monthly
4	High likelihood of harm	Harm will probably happen/recur, but it is not a persisting issue/ circumstances	Harm expected to occur at least weekly
5	Very high likelihood of harm	Harm will undoubtedly happen/recur, possibly frequently	Harm expected to occur at least daily

Ordinal scale for the quantification of the likelihood of a specified patient outcome

Risk Category

Risk Category as Allocated by Likelihood and Severity						
		Risk Score				
Severity	5 - Catastrophic	3	4	4	5	5
	4 - Major	2	3	3	4	5
	3 - Moderate	2	2	3	3	4
	2 - Minor	1	2	2	3	4
	1 - Minimal	1	1	2	2	3
		1-V low	2-Low	3-Med	4-High	5-V High
		Likelihood of Harm				

Matrix showing risk category allocated on the basis of likelihood and severity for a specified patient harm.

Risk Acceptability

Risk Score	Risk Category	Response to Baseline Risk	Response to Residual Risk
1	Very low risk	Risk tolerable but mitigation is desirable.	Risk tolerable, passive surveillance recommended.
2	Low risk	Risk tolerable but mitigation is highly desirable.	Risk tolerable, passive surveillance required.
3	Medium risk	Undesirable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level.	Shall only be acceptable when further risk reduction is impractical.
4	High risk	Risk highly likely to be unacceptable. System, module or functionality should not go live, or should be taken out of use if possible, unless the risks arising from loss of use exceed those of continuing to use the system. Active surveillance required and urgent mitigation is mandatory.	Risk highly likely to be unacceptable unless the risks arising from loss of use exceed those of continuing to use the system. Consideration must be given to further risk mitigation and active surveillance required.
5	Very high risk	Unacceptable risk. System, module or functionality cannot go live, or must immediately be taken out of use. Mitigation mandatory.	System, module or functionality cannot go live, or must immediately be taken out of use. Further risk mitigation mandatory if system, module, or functionality to be returned to service.

InterSystems response to baseline and residual risks

Operational Risk Rating Process

InterSystems' risk rating uses standard methodology to estimate the risk to operations based on the most typical foreseeable adverse outcomes, as opposed to the worst-case scenario, which is used to determine the impact and likelihood using standard ordinal scales to derive the risk rating. Operational Risk is the failure of the operational system (application, O/S, database, etc.) relating to:

- **System Performance**: the system performs with the expected functionality, throughput, and utilization.
- **Data Quality**: the system can provide assurance of the accuracy and consistency of data over the entire life-cycle of the data, including recording the data exactly as intended and, upon later retrieval, ensuring the data are the same as when data were originally recorded.
- **System Availability**: the system responds to operations in a time better than the calculated or estimated Mean Time Between Failures (MTBF) and continues to operate without noticeable (based upon expected performance) interruption or delay.

Description of Impact Rating

5	**Very high risk**	Full failure of safeguard(s) (administrative, physical, or technical) relating to performance, quality, or availability
4	**High risk**	Major (majority) failure of safeguard(s) (administrative, physical, or technical) relating to performance, quality, or availability
3	**Medium risk**	Limited failure of safeguard(s) (administrative, physical, or technical) relating to performance, quality, or availability
2	**Low risk**	Marginal failure of safeguard(s) (administrative, physical, or technical) relating to performance, quality, or availability
1	**Very low risk**	Incomplete (or intermittent) failure of safeguard(s) (administrative, physical, or technical) relating to performance, quality, or availability

Description of Outcome Likelihood

5	**Very high risk**	Will undoubtedly happen/recur, possibly frequently	Expected to occur at every operational or use or with all processing
4	**High risk**	Will probably happen/recur, but it is not a persisting issue/ circumstances	Expected to occur regularly or with most processing
3	**Medium risk**	Might happen or recur occasionally	Expected to occur occasionally or with some processing
2	**Low risk**	Do not expect it to happen/recur but it is possible it may do so	Expected to occur a few times or with limited processing
1	**Very low risk**	Unlikely happen/recur	Not expected to occur over time of normal operation

Risk Score & Category

The combination of the Impact and Likelihood produce an overall Risk Score and Risk Rating as follows:

Impact	Likelihood 1	2	3	4	5
5	3	4	4	5	5
4	2	3	3	4	5
3	2	2	3	3	4
2	1	2	2	3	4
1	1	1	2	2	3

Risk Score	Risk Category
5	Very high risk
4	High risk
3	Medium risk
2	Low risk
1	Very low risk

Privacy Risk Rating Process

InterSystems' risk rating uses standard methodology to estimate the risk to privacy based on the most typical foreseeable adverse outcomes, as opposed to the worst-case scenario, which is used to determine the impact and likelihood using standard ordinal scales to derive the risk rating.

Description of Impact Rating

5	**Critical**	Full public disclosure of confidential information, complete impact to data integrity, severe violation of legitimate basis for processing.
4	**High**	Disclosure to improper and unauthorized parties, operational impact to data integrity, elevated violation of legitimate basis for processing
3	**Moderate**	Limited disclosure to improper or unauthorized parties, limited impact to data integrity, existing violation of legitimate basis for processing
2	**Low**	Restricted disclosure to improper parties, restricted impact to data integrity, marginal violation of legitimate basis for processing
1	**Minimal**	No disclosure to improper or unauthorized parties, no discernable impact to data integrity, trivial or technical violation of legitimate basis for processing

Description of Outcome Likelihood

5	**Critical**	Will undoubtedly happen/recur, possibly frequently	Expected to occur at every operational or use or with all processing
4	**High**	Will probably happen/recur, but it is not a persisting issue/ circumstances	Expected to occur regularly or with most processing
3	**Moderate**	Might happen or recur occasionally	Expected to occur occasionally or with some processing
2	**Low**	Do not expect it to happen/recur but it is possible it may do so	Expected to occur a few times or with limited processing
1	**Minimal**	Unlikely happen/recur	Not expected to occur over time of normal operation

Risk Score & Category

The combination of the Impact and Likelihood produce an overall Risk Score and Risk Category as follows:

Impact	1	2	3	4	5
5	3	4	4	5	5
4	2	3	3	4	5
3	2	2	3	3	4
2	1	2	2	3	4
1	1	1	2	2	3
	1	**2**	**3**	**4**	**5**
	Likelihood				

Risk Score	Risk Category
5	Very high risk
4	High risk
3	Medium risk
2	Low risk
1	Very low risk

Security Risk Rating Process

InterSystems' risk rating uses standard methodology to estimate the risk to security based on the most typical foreseeable adverse outcomes, as opposed to the worst-case scenario, which is used to determine the impact and likelihood using standard ordinal scales to derive the risk rating.

Description of Impact Rating

5	**Critical**	Full failure of safeguard(s) (administrative, physical, or technical) relating to confidentiality, integrity, and/or availability
4	**High**	Major (majority) failure of safeguard(s) (administrative, physical, or technical) relating to confidentiality, integrity, and/or availability
3	**Moderate**	Limited failure of safeguard(s) (administrative, physical, or technical) relating to confidentiality, integrity, and/or availability
2	**Low**	Marginal failure of safeguard(s) (administrative, physical, or technical) relating to confidentiality, integrity, and/or availability
1	**Minimal**	Incomplete (or intermittent) failure of safeguard(s) (administrative, physical, or technical) relating to confidentiality, integrity, and/or availability

Description of Outcome Likelihood

5	**Critical**	Will undoubtedly happen/recur, possibly frequently	Expected to occur at every operational or use or with all processing
4	**High**	Will probably happen/recur, but it is not a persisting issue/ circumstances	Expected to occur regularly or with most processing
3	**Moderate**	Might happen or recur occasionally	Expected to occur occasionally or with some processing
2	**Low**	Do not expect it to happen/recur but it is possible it may do so	Expected to occur a few times or with limited processing
1	**Minimal**	Unlikely happen/recur	Not expected to occur over time of normal operation

Risk Score & Category

The combination of the Impact and Likelihood produce an overall Risk Score and Risk Rating as follows:

Impact	1	2	3	4	5
5	3	4	4	5	5
4	2	3	3	4	5
3	2	2	3	3	4
2	1	2	2	3	4
1	1	1	2	2	3
	Likelihood				

Risk Score	Risk Category
5	Very high risk
4	High risk
3	Moderate risk
2	Low risk
1	Minimal risk

– End of HS2023-02 Alert Communication –

