InterSystems HealthShare

Risk and Safety Alert

HS2024-03 Alert for InterSystems IRIS for Health and HealthShare

31-JUL-2024

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 with 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 IRIS® for Health
- HealthShare® Solutions products
- HealthShare® Health Connect

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

Note: Some changes were made to affected versions since the original release of this document on July 24, 2023. Those changes are noted.

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 IRIS for Health or 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	Requirements
HS2024-03-01 After Operating System Upgrade, HealthShare Instance May Require Upgrade	• InterSystems IRIS for Health 2021.2 + • HealthShare Health Connect 2021.2 + • All HealthShare Solutions products, version 2022.2 and higher: Care Community • Clinical Viewer • Health Insight • Healthcare Action Engine • Patient Index • Personal Community • Provider Directory • Unified Care Record	Operational: 4 – High Risk	• Linux operating system • Operating system upgrade (major version)
HS2024-03-02 Bearer Token String Is Visible in Message Viewer and FSLOG	• InterSystems IRIS for Health versions 2021.1 – 2024.1	Security: 3 – Medium Risk	• FHIR repository • IRIS interoperability production-based FHIR endpoint
HS2024-03-03 OnSystemStartup Methods not Run on Upgrade in Mirrored FHIR Systems	• InterSystems IRIS for Health 2023.x • HealthShare Unified Care Record versions 2023.1 and 2023.2 (**Note:** Version 2024.1 is *not* affected)	Operational: 3 – Medium Risk	• Mirroring • FHIR repository
HS2024-03-04 Clinical Consent Policies not Properly Evaluated with Custom-named Streamlets	• HealthShare Unified Care Record: all versions up-to-and-including 2024.1	Privacy: 3 – Medium Risk	• Clinical information type (CIT) consent policies • Custom SDA streamlets

Detail of Alerts

HS2024-03-01 After Operating System Upgrade, HealthShare Instance May Require Upgrade

Issue date: 24-JUL-2024

Risk Category and Score:

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

Version and System Area Affected

Products and Versions:
- InterSystems IRIS for Health version 2021.2 and higher
- HealthShare Health Connect version 2021.2 and higher
- All HealthShare Solutions products version 2022.2 and higher:

  Care Community • Clinical Viewer • Health Insight • Healthcare Action Engine • Patient Index • Personal Community • Provider Directory • Unified Care Record

Requirements: Linux operating system, Operating system upgrade (major version)

System areas affected: Product Upgrade Required

Reference: HSIEO-10507

Summary of Issue

Some InterSystems products require a separate product distribution (kit or container) for different versions of a particular operating system. For example, Unified Care Record 2024.1 has two separate distributions for Red Hat:

- Unified Care Record 2024.1 for Red Hat 8
- Unified Care Record 2024.1 for Red Hat 9

A HealthShare instance built for a specific OS version will not run if the OS version is upgraded. For example, “Unified Care Record 2024.1 for Red Hat 8” will not run if the server is upgraded to Red Hat 9.

There are now version-specific HealthShare distributions for all versions of the following operating systems:

- Red Hat
- Ubuntu

If, for example, you upgrade your server from Red Hat 8 to Red Hat 9, then you must "upgrade" your HealthShare instance as well, by running the installer for the Red Hat 9 version of HealthShare.

Failure to run this upgrade procedure may cause a HealthShare instance to unexpectedly not run when the operating system is upgraded.

Risk Assessment

The risk score and category were determined using the InterSystems Risk Rating process, and based on the following assessments:

Operational:	4 – High Risk	Impact of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

When you upgrade an Ubuntu or Red Hat server, obtain new kits or container images and follow the upgrade instructions to perform a same-version upgrade. Reference Information: HSIEO-10507

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2024-03-01”.

– End of Alert HS2024-03-01 –

InterSystems HealthShare

Risk and Safety Alert

HS2024-03-02 Bearer Token String Is Visible in Message Viewer and FSLOG

Issue date: 24-JUL-2024

Risk Category and Score:

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

Version and System Area Affected

Products:	InterSystems IRIS for Health
Versions:	Versions 2021.1 through 2024.1
Requirements:	FHIR repository, InterSystems IRIS interoperability production-based FHIR endpoint
System areas affected:	Secrecy of customer credentials
Reference:	IF-6106

Summary of Issue

InterSystems FHIR servers use bearer tokens for authentication. If a FHIR server endpoint uses an interoperability production for processing FHIR requests, the bearer token string is stored in the message trace log and is available for viewing by an administrative user. This might compromise a FHIR server user's security.

- In order to view the message log, a user must have InterSystems IRIS for Health credentials and a role that provides access to the Message Viewer. This is typically provided only to system administrators.
- If a namespace has full FSLOG logging enabled, then a user must have InterSystems IRIS for Health credentials and a role that provides access to the FSLOG global, which is also typically provided only to system administrators.

Risk Assessment

The risk score and category were determined using the InterSystems Risk Rating process, and based on the following assessments:

Security:	3 – Medium Risk	Impact of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 3 out of 5

Recommended Actions

If your FHIR server uses an interoperability production, either upgrade to version 2024.2 or later of IRIS for Health where the issue has been corrected, or contact the WRC to request a correction:

- For InterSystems IRIS for Health 2024.1, request IF-6106.
- For InterSystems IRIS for Health 2021.x through 2023.x, request IF-6106, IF-6171, and HSHC-4280.

As interim mitigation for the issue, you can remove existing FSLOG and disable further logging until a patch is installed. In each production FHIR-enabled namespace, perform the following actions in Terminal:

```
Kill ^FSLOG
Kill ^FSLogChannel
```

Reference Information: IF-6106

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2024-03-02".

– End of Alert HS2024-03-02 –

InterSystems HealthShare

Risk and Safety Alert

HS2024-03-03 OnSystemStartup Methods not Run on Upgrade in Mirrored FHIR Systems

Issue date: 24-JUL-2024

Risk Category and Score:

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

Version and System Area Affected

Products:
- InterSystems IRIS for Health
- HealthShare Unified Care Record

Versions:

If using both FHIR and mirroring, all versions when upgrading to version:
- 2023.x of IRIS for Health
- 2023.1 and 2023.2 of Unified Care Record

(**Note:** Version 2024.1 is *not* affected)

Requirements: Mirroring, FHIR repository

System areas affected: FHIR functionality after upgrade

Reference: IF-6132

Summary of Issue

If mirroring is enabled, when upgrading to affected versions of either InterSystems IRIS for Health or HealthShare systems with FHIR repositories, you may encounter half-completed upgrades and an unstable state, creating a system stability issue.

Incomplete indexing could lead to FHIR Search results that are missing data.

Risk Assessment

The risk score and category were determined using the InterSystems Risk Rating process, and based on the following assessments:

Operations:	3 – Medium Risk	Impact of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 4 out of 5

Recommended Actions

If you use both FHIR and mirroring and are on an affected version or plan to upgrade to one, contact the WRC to request a correction. The specific correction depends upon your situation:

- If you are planning to upgrade:

  Prior to performing an upgrade, affected customers should contact the WRC to request a full kit adhoc for the version that they are upgrading to that contains both IF-6132 and IF-6136.

- If you are already using an affected version (whether you performed an upgrade or started out on that version:

  Affected customers should contact the WRC to request an adhoc patch for IF-6132 only.

Reference Information: IF-6132

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2024-03-03”.

– End of Alert HS2024-03-03 –

HS2024-03-04 Clinical Consent Policies not Properly Evaluated with Custom-named Streamlets

Issue date: 24-JUL-2024

Risk Category and Score:

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

Version and System Area Affected

Products:	HealthShare Unified Care Record
Versions:	All versions up-to-and-including 2024.1
Requirements:	Clinical information type (CIT) consent policies, Custom SDA streamlets
System areas affected:	Patient consent
Reference:	HSDD-2397

Summary of Issue

If you use *clinical information type (CIT) consent* policies and have *custom SDA streamlets*, then it is important that your custom streamlets use the same class name as the standard streamlet, for example, LABORDER. A customer who used a different class name, for example ZLABORDER, found that consent rules were not being properly evaluated against data in pre-existing streamlets that used the base streamlet type (LABORDER), resulting in the potential for improper disclosure of restricted patient data.

MPI consent policies are not affected by this issue.

Risk Assessment

The risk score and category were determined using the InterSystems Risk Rating process, and based on the following assessments:

Privacy:	3 – Medium Risk	Impact of typical adverse outcome = 4 out of 5 Likelihood of typical adverse outcome = 3 out of 5

Recommended Actions

Confirm that any custom streamlets that you have defined use the standard class name, particularly if you also use CIT consent policies and have pre-existing data using the base streamlet type.

Reference Information: HSDD-2397

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2024-03-04".

– End of Alert HS2024-03-04 –

InterSystems Risk Rating Process

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	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	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	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	Moderate risk
2	Low risk
1	Minimal risk

– End of HS2024-03 Alert Communication –

