InterSystems HealthShare

Risk and Safety Alert

HS2026-01 Alert for InterSystems HealthShare and IRIS for Health Products

11-FEB-2026

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:

- HealthShare® products
- InterSystems IRIS® for Health
- InterSystems 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.

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 cybersecurity, privacy, or product security, you can reach our Data Protection Officer, Ken Mortensen, at cyber@intersystems.com.

If you ever have any clinical safety, privacy, security or operations related questions about HealthShare or any Intersystems product, 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,

Gokhan Uluderya
Acting Director, Product Management – HealthShare

InterSystems
One Congress Street
Boston, MA 02114
TEL: +1.617.621.0600

Summary of Alerts

Alert	Product & Versions Affected	Risk Category & Score	Requirements
HS2026-01-01 Unsafe Permission Granted to All Care Community Users	HealthShare Care Community: • All versions prior to 2025.2	Security: 4 – High Risk	• Care Community
HS2026-01-02 User Authentication from the FHIR Server APIs is not Logged	All versions after 2020.2 of: • HealthShare Unified Care Record • InterSystems IRIS for Health • InterSystems Health Connect	Security: 4 – High Risk	• FHIR Server
HS2026-01-03 Federated SSO Regressions in HealthShare Version 2025.2	Version 2025.2 of HealthShare: • Unified Care Record • Clinical Viewer • Provider Directory • Health Insight • InterSystems EMPI	Operational: 4 – High Risk	• Federated SSO • Third-party IdP or SAML
HS2026-01-04 FHIR Search with Chained Parameters May Reveal Unauthorized Data	Version 2024.1 and later of: • HealthShare Unified Care Record • InterSystems IRIS for Health • InterSystems Health Connect	Privacy: 4 – High Risk	• FHIR Server
HS2026-01-05 FHIR Server Reset May Cause Unavailability of Management Portal Pages	• InterSystems IRIS for Health • InterSystems Health Connect 2024.2 • 2024.3 • 2025.1 • 2025.1.1	Operational: 4 – High Risk	• FHIR Server • FHIR SQL projections
HS2026-01-06 FHIR SQL Builder Doesn't Account for FHIR Interactions HardDelete() Method	InterSystems IRIS for Health: • 2024.1.0 – 2024.1.4 • 2025.1.0 – 2025.1.1 • 2025.2.0	Privacy: 3 – Medium Risk	• FHIR SQL Builder • IRIS for Health Advanced Server license

Detail of Alerts

HS2026-01-01 Unsafe Permission Granted to All Care Community Users

Issue date: 11-FEB-2026

Risk Category and Score:

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

Version and System Area Affected

Products:	• All versions of HealthShare Care Community earlier than 2025.2: 2019.1 • 2019.2 • 2020.1 • 2020.2 •2021.1 • 2021.2 • 2022.1 • 2022.2 • 2023.1 • 2023.2 • 2024.1 • 2024.2 •2025.1
Requirements:	Care Community
System areas affected:	Security
Reference:	HSEUA-2052

Summary of Issue

All users of Care Community are granted the `%HSCM_CareCommunity` role. In versions prior to 2025.2, this role included a permission that grants users administrative access to the Management Portal. This type of access is usually recommended to be given only to administrators.

Risk Assessment

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

Security:	4 – High Risk	Impact of typical adverse outcome = 4 out of 5 Likelihood of typical adverse outcome = 4 out of 5
CVSS score:	High vulnerability 7.4	

Recommended Actions

The correction for this defect is identified as HSEUA-2052, which is included in HealthShare Care Community version 2025.2 and in all future product releases. Upgrading to version 2025.2 is the preferred resolution for this issue.

If an upgrade is not possible, then you can run the following procedure:

1. Open a Terminal on your Care Community instance and log in as a system user.
2. Change to your Care Community namespace.
3. Run the following line of code to apply the fix:
```
do ##class(HS.HC.SystemConfig.API).AddUpdateRole($namespace,
"%HSCM_CareCommunity", "Role granting access to the Care Community CSP
application", "%HSCM_CareCommunity:U,%HSCM_FHIRRepo:URW")
```
4. Run the following command to confirm that the fix works:
```
zw $system.Security.CheckRolesPermission("%HSCM_CareCommunity",
"%System_Callout", "USE")
```
5. If it prints out 0, then fix worked. If not, the fix failed. In this case, please contact the WRC.

For questions regarding this alert, contact the Worldwide Response Center and reference “Alert HS2026-01-01”.

– End of Alert HS2026-01-01 –

HS2026-01-02 User Authentication from the FHIR Server APIs is not Logged

Issue date: 11-FEB-2026

Risk Category and Score:

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

Version and System Area Affected

Products:	All versions after 2020.2: • InterSystems IRIS for Health • InterSystems Health Connect • HealthShare Unified Care Record
Requirements:	FHIR Server
System areas affected:	FHIR Auditing
Reference:	IF-8560

Summary of Issue

User interactions with the FHIR Server using OAuth tokens do not follow regular IRIS authentication routine enablement features. This means that the audit log is not populated with user-identifiable or authentication details. The unavailability of this information has the potential to obscure end-to-end security analysis and forensics.

Risk Assessment

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

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

Recommended Actions

The correction for this defect is identified as IF-8560, which is included in IRIS for Health and Health Connect 2025.3 and later releases. With the correction, the product logs automatic authentication and rejection.

Customers who are unable to upgrade are encouraged to implement compensating controls to address the lack of logging.

For questions regarding this alert, contact the Worldwide Response Center and reference “Alert HS2026-01-02”.

– End of Alert HS2026-01-02 –

InterSystems HealthShare

Risk and Safety Alert

HS2026-01-03 Federated SSO Regressions in HealthShare Version 2025.2

Issue date: 11-FEB-2026

Risk Category and Score:

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

Version and System Area Affected

Products:	Version 2025.2 of HealthShare: Unified Care Record • Clinical Viewer • Provider Directory • InterSystems EMPI • Health Insight
Requirements:	Federated SSO with SAML or Federated SSO with 3rd-party IdP
System areas affected:	System Availability, Login, Federated SSO
Reference:	HSIEO-14043 *and* HSIEO-14066

Summary of Issue

A change in the underlying platform has led to a regression in HealthShare for the 2025.2 release if the system is configured to use Federated SSO in either of the two following ways:

- delegating to a third-party IdP (e.g. OKTA or Azure)
- allowing user access via SAML SSO, for example, a Clinical Viewer embedded in an EMR

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 = 4 out of 5 Likelihood of typical adverse outcome = 4 out of 5

Recommended Actions

If you are using Federated SSO and want to install a new system with version 2025.2 or upgrade an existing system to 2025.2 and you are delegating to a third-party IdP or using SAML SSO, request an ad hoc patch that contains DP-447478 *and* DP-447386 as outlined in HSIEO-14043 and HSIEO-14066.

The correction will be included in version 2026.1 of all HealthShare products.

For questions regarding this alert, contact the Worldwide Response Center and reference “Alert HS2026-01-03”.

– End of Alert HS2026-01-03 –

HS2026-01-04 FHIR Search with Chained Parameters May Reveal Unauthorized Data

Issue date: 11-FEB-2026

Risk Category and Score:

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

Version and System Area Affected

Products:	Version 2024.1 and later of: • InterSystems IRIS for Health • InterSystems Health Connect • HealthShare Unified Care Record
Requirements:	FHIR Server
System areas affected:	FHIR Server, FHIR search
Reference:	IF-9038

Summary of Issue

The InterSystems FHIR Server stores and protects many sensitive resource types (Patient, Allergy, Encounter, etc.). If a client performs a series of chained searches, they may be able to infer information on resources they are not authorized to view. For example, a user with only *Patient* resource access could perform a chained search on *Conditions* to filter the *Patients* with a specific condition.

Risk Assessment

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

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

Recommended Actions

The correction for this defect is identified as IF-9038, which is included in the upcoming IRIS for Health and Health Connect 2026.1 release. InterSystems recommends that customers upgrade to this version when it becomes available. The correction is also available as an ad hoc patch for older releases back to version 2024.1.

For questions regarding this alert, contact the Worldwide Response Center and reference “Alert HS2026-01-04”.

– End of Alert HS2026-01-04 –

InterSystems HealthShare

Risk and Safety Alert

HS2026-01-05 FHIR Server Reset May Cause Unavailability of Management Portal Pages

Issue date: 11-FEB-2026

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: 2024.2 • 2024.3 • 2025.1.0 • 2025.1.1 • InterSystems Health Connect: 2024.2 • 2024.3 • 2025.1.0 • 2025.1.1
Requirements:	FHIR Servers with FHIR SQL projections using the FHIR Server "Reset" button
System areas affected:	FHIR, System Management Portal
Reference:	IF-8101

Summary of Issue

A user may encounter <CLASS DOES NOT EXIST> errors after resetting a FHIR Server when the SQL Builder is also in use. This results in the FHIR Server management interfaces being inaccessible.

This is caused by a bug in the reset function which deletes the FHIR SQL interaction classes. The deletion of this interactions class causes errors in the management portal and makes manual recovery of the FHIR endpoint difficult. The underlying FHIR databases are unaffected and can be recovered.

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 = 4 out of 5 Likelihood of typical adverse outcome = 4 out of 5

Recommended Actions

The correction for this defect is identified as IF-8101, which is included in version 2025.1.2 of IRIS for Health and Health Connect and in all future product releases. Upgrading to version 2025.1.2 is the preferred resolution for this issue.

If an upgrade is not possible, a correction is available for older versions via ad hoc change file (patch) or full kit distribution by contacting the Worldwide Response Center (WRC).

If you encounter the issue, to manually recover your system, follow the procedure below:

1. In the Portal, change to a different namespace with an associated FHIR Server and SQL Builder projection.
2. Navigate to **Home** > **System Explorer** > **Classes**.
3. Locate and export the following classes:
   - `FHIRSQL.Interactions1.cls`
   - `FHIRSQL.InteractionsStrategy1.cls`
   - `FHIRSQL.RepoManager1.cls`
4. Change to the namespace running the reset FHIR Server.
5. In the impacted namespace, import and compile the class files that you exported in an earlier step.

This manual recovery is not a permanent solution. Attempting to reset the FHIR Server again will result in the same <CLASS DOES NOT EXIST> error and must be permanently resolved with an upgraded product version or adhoc.

For questions regarding this alert, contact the Worldwide Response Center and reference "Alert HS2026-01-05".

– End of Alert HS2026-01-05 –

HS2026-01-06 FHIR SQL Builder Doesn't Account for FHIR Interactions HardDelete() Method

Issue date: 11-FEB-2026

Risk Category and Score:

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

Version and System Area Affected

Products:	InterSystems IRIS for Health: • 2024.1.0 • 2024.1.1 • 2024.1.2 • 2024.1.3 • 2024.1.4 • 2025.1.0 • 2025.1.1 • 2025.2.0
Requirements:	FHIR SQL Builder with the IRIS for Health Advanced Server license
System areas affected:	FHIR Server, FHIR SQL Builder
Reference:	IF-8424

Summary of Issue

Purging data from the FHIR repository without using the FHIR Server's REST APIs (for example, using ObjectScript APIs or SQL) may not remove indexes used in the FHIR SQL Builder. This may expose sensitive indexed data that was removed from the repository due to consent revocation.

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 = 3 out of 5 Likelihood of typical adverse outcome = 3 out of 5

Recommended Actions

The correction for this defect is identified as IF-8424, which is included in the following InterSystems IRIS for Health versions (and all subsequent versions):

- 2024.1.5
- 2025.1.2
- 2025.2.1
- 2025.3.0

Affected customers should upgrade to a version that contains the correction. An ad hoc patch is also available for older versions.

For questions regarding this alert, contact the Worldwide Response Center and reference “Alert HS2026-01-06”.

– End of Alert HS2026-01-06 –

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 operation or use or with all processing
4	**High risk**	Will probably happen/recur, but it is not a persisting issue/circumstance	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 to 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
	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

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 to 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						
	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 to 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						
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	Moderate risk
2	Low risk
1	Minimal risk

– End of HS2026-01 Alert Communication –

