

HealthShare HS2024-limited Alert

27-FEB-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 the necessary information so that you can assess your situation as quickly as possible.

On November 13, 2023, InterSystems released Alert HS2023-02, which discussed several issues. Your organization was identified as a recipient of the ad hoc correction associated with the issue labeled HS2023-02-04. Subsequent testing has revealed that applying the ad hoc correction associated with HS2023-02-04 causes a regression in functionality when using Studio.

Please read the information that follows to learn how to remediate the regression. 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
HS2024-limited-01: Regression in Studio Functionality in HealthShare after Applying Corrections Recommended in Alert HS2023-02-04	Customers who received an ad hoc correction for HSIEO-8613.	Operations: 4 – High Risk

Detail of Alerts

HS2024-limited-01: Regression in Studio Functionality in HealthShare after Applying Corrections Recommended in Alert HS2023-02-04

Issue date: 1-FEB-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:	Customers who received and applied an ad hoc correction for HSIEO-8613
Versions:	See above
System areas affected:	Studio
Reference:	HSIEO-10155

Summary of Issue

On November 13, 2023, InterSystems HealthShare Released Alert HS2023-02. One of the alerts was designated HS2023-02-04. In that alert, readers were informed about a defect. Affected customers were given the recommendation to request an ad hoc patch with corrections.

One of the corrections (reference DP-421886) recommended for alert HS2023-02-04 has been found to cause regressions in functionality when using Studio. Specifically, HealthShare systems containing DP-421886 are not able to use Studio to load or edit Business Process Language (BPL) and Data Transformation Language (DTL) graphical editors. In addition, any ZEN page templates including the ZEN Page Wizard, SOAP Wizard and others would be non-functional when loading in Studio.

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	Impact of typical adverse outcome = 5 out of 5
		Likelihood of typical adverse outcome = 2 out of 5

Recommended Actions

To work around the issue, HealthShare developers working in a non-production environment may choose to do BPL/DTL editing in the Management Portal rather than in Studio. Separately, developers loading ZEN Page Templates can disable the "Prevent login CSRF attack" flag in the `/isc/studio/templates` web application definition.

Customers may also request an ad hoc patch containing correction DP-428566 which will allow developers to continue using Studio for BPL/DTL editing and loading of ZEN Pages.

Reference Information: HSIEO-10155

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference "Alert HS2024-limited-01".

– End of Alert HS2024-limited-01 –

– End of Alerts for HS2024-limited –

Addendum

Contents:

1. [Clinical Risk Rating Process](#)
2. [Operational Risk Rating Process](#)
3. [Privacy Risk Rating Process](#)
4. [Security Risk Rating Process](#)

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	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 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	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	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 HS2024-limited Alert Communication –