

HealthShare HS2021-04 Alert

29-NOV-2021

Dear HealthShare 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 HealthShare®, InterSystems is committed to providing you the necessary information so that you can assess your situation as quickly as possible.

We have identified a risk that may affect you when using InterSystems HealthShare Health Insight.

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 and our Clinical Safety Officer, Dr. Ethan Gershon 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

This document contains the following Alert:

Alert	Product & Versions Affected	Risk Category & Score
HS2021-04: Data stored in Unified Care Record may fail to transfer to Health Insight in specific circumstances when the MAXLEN is exceeded.	The affected HealthShare Products and Versions are: <ul style="list-style-type: none"><li data-bbox="574 401 911 428">• Health Insight 2021.1 Only	Clinical Safety: 2-Low Risk Operations: 2-Low Risk

We encourage you to read the information below and then reach out to the Worldwide Response Center (WRC) at support@intersystems.com or +1.617.621.0700 with any questions that might arise.

Detail of Alert

HS2021-04: Data stored in Unified Care Record may fail to transfer to Health Insight in specific circumstances when the MAXLEN is exceeded.

Issue date: 29-NOV-2021

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
2-Low Risk	Not Applicable	Not Applicable	2-Low Risk

Version and System Area Affected

HealthShare® Products: Health Insight
 Versions: 2021.1 Only
 System areas affected: Health Insight relational database tables
 Reference: HSHI-5353, HSHI-5627

Summary of Issue

Unified Care Record stores patient data in SDA3 streamlets. String data elements in the SDA have a MAXLEN parameter that indicates the maximum number of characters allowed in the data element. Most times, data is successfully stored in the SDA even when it exceeds the specified MAXLEN, as UCR does not enforce MAXLEN validation in most cases. The problem occurs when the system attempts to transfer this data to Health Insight, but only in very specific circumstances outlined in the technical addendum of this advisory.

If the defect occurs, the affected data is not transferred into the Health Insight relational tables and *no error is logged*.

Full details of the identified issue appear in the Technical Addendum for HS2021-04.

Risk Assessment

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

Clinical Safety:	2-Low Risk	Severity of typical adverse outcome = 2 out of 5 Likelihood of typical adverse outcome = 2 out of 5
Operational:	2-Low Risk	Severity of typical adverse outcome = 2 out of 5 Likelihood of typical adverse outcome = 2 out of 5

When data is missing in Health Insight, it creates a risk because queries that rely on that data may return different results. For example, a patient cohort definition built using such a query may exclude appropriate patients or may include inappropriate patients.

Recommended Actions

Any customers who are using HS 2021.1 should immediately request a patch to fix this defect to prevent further data loss from happening. InterSystems plans to communicate in the near future about any instructions and/or tool to help check if your Health Insight data has been impacted by this defect.

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference "Alert HS2021-04".

Technical Addendum for HS2021-04

Description of Issue

This issue affects only customers who are on the 2021.1 release and using Health Insight.

If data elements in SDA3 exceed the MAXLEN setting in the SDA3 data model, the data may not be transferred into Health Insight's HSAA relational tables if those data elements are *under a serial object* that is *embedded in an SDA3 streamlet object*.

This issue can occur when a data element of a string type exceeds the MAXLEN setting in the HealthShare SDA3 data model, and the string property either:

- lives under a serial object which could directly live within an SDA3 streamlet object.

or

- lives within a descendant serial object of the streamlet object.

Under these circumstances, the serial object that directly lives under the streamlet object, in its entirety, fails to be transferred into Health Insight relational tables. There are two possible failure modes:

- If the serial object is transferred to Health Insight still as an embedded object, all fields of that serial object will be empty.
- If the serial object is transferred to Health Insight as relational table records, there will be no corresponding records populated for the object.

If a string property exceeds the MAXLEN setting in SDA3, but the string property lives *directly* under a streamlet object, this issue will not be triggered.

The data loss in Health Insight caused by this issue is *not logged* in Health Insight when it occurs.

All customers using version 2021.1 of Health Insight are strongly encouraged to request the fix as soon as possible, in order to prevent data loss in the future. At the current time, there is no way to determine if you have been impacted by this issue, but the Health Insight product team is working on a strategy to identify and mitigate any data loss that may have already occurred. A follow-up communication for this issue is planned when that work is complete.

Customers who are on any HealthShare release earlier than 2021.1 will not experience this issue. This issue has been fixed in version 2021.2.

Recommended Action

InterSystems recommends that affected customer organizations take the following actions:

Contact InterSystems HealthShare Support to obtain a changed-file ad hoc for HSHI-5353. Once the ad hoc is applied, new data flowing into the HealthShare system will be ingested into Health Insight with the correct behavior.

Supported customers can request access to the WRC application by contacting the [Worldwide Response Center](#).

Information about the Correction

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference "Alert HS2021-04".

– End of Alert HS2021-04 –

Addendum

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	3y	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 HS2021-04 Alert Communication –