HealthShare HS2020-09 Alert

22-DEC-2020

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 number of risks that may affect you when using InterSystems HealthShare, including any customer trying to install or upgrade to any HealthShare 2020.2 kit, customers using Health Insight and customers using FHIR and the ODS with the Unified Care Record 2020.1. These alerts do not affect HealthShare Health Connect or HSAP customers.

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 HealthShare Alert process complements our existing support processes. If you have questions about our processes for data protection, privacy, and security, including our Global Trust program, you can reach our Data Protection Officer Ken Mortensen at dpo@intersystems.com.

If you ever have any privacy, security, patient safety 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
Director, Product Management – HealthShare

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

Summary of Alerts

This HealthShare Alert ensures that InterSystems gets you the information you need to understand important clinical safety, privacy, security, and operational risks that have been identified and complements our existing support processes.

This document contains the following Alerts:

Alert	Product & Versions Affected	Risk Category & Score
HS2020-09-01: Internal Web Traffic between Productions in a Federation may be Insecure or Blocked	Unified Care Record 2020.2 Patient Index 2020.2 Health Insight 2020.2 Clinical Viewer 2020.2 Personal Community 2020.2 Provider Directory 2020.2 Care Community 2020.2	5-Very High Risk (Operations) 3-Medium Risk (Security) 2-Low Risk (Clinical)
HS2020-09-02: Invalid Patient Medication Streamlet Triggers Erroneous Data Ingestion Errors for Subsequent Patients	Health Insight 2019.1.0, 2019.1.2, 2019.1.3, 2020.1, and 2020.2	3-Medium Risk (Clinical Safety) 3-Medium Risk (Operations)
HS2020-09-03: FHIR Resource Purge Task in ODS fails with <METHOD NOT FOUND>	Unified Care Record 2020.1 with the ODS and FHIR	5-Very High Risk (Operations)

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 Alerts

HS2020-09-01: Internal Web Traffic between Productions in a Federation may be Insecure or Blocked

Issue date: 22-DEC-2020

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
2-Low Risk	Not Applicable	3-Medium Risk	5-Very High Risk

Version and System Area Affected

HealthShare® Products:	Unified Care Record, Patient Index, Health Insight, Clinical Viewer, Personal Community, Provider Directory and Care Community
Versions:	2020.2
System areas affected:	• Security (SSL/TLS) • New HS 2020.2 installations • Customers upgrading to HS 2020.2
Reference:	HSIEO-3593

Summary of Issue

HealthShare best practices recommend that customers encrypt all web traffic, including internal traffic between productions in a federation. A change to the Installer Wizard in HealthShare 2020.2 inadvertently causes the SSL Configuration setting in service registry entries for namespaces in the federation to reset to an empty value when the client instance connects to the Registry after a production restart.

This occurs both in a new install or an upgrade. With no SSL Configuration specified, HealthShare attempts to downgrade connections from HTTPS to HTTP for internal communication between the HealthShare productions in a federation. Customers who follow InterSystems guidance on configuring their production environments typically do not allow unencrypted HTTP traffic between productions in a federation.

There are two possible modes of failure related to this issue:

1) If there is no SSL Configuration and the *environment allows only HTTPS encrypted traffic*, then the system becomes unresponsive.

   This situation creates an operational risk because the system stops applying new data, the system cannot process FHIR requests, and the Clinical Viewer cannot load and display data. As discovery of this failure will likely extend the planned downtime for an upgrade, it introduces a clinical risk as well if the system is unavailable for longer than expected.

2) If there is no SSL Configuration and the *environment allows unencrypted HTTP traffic*, then the system continues to function, but a security risk has been introduced.

   While the system appears to function normally, web traffic between productions is now flowing unencrypted. This a silent failure, in that the customer does not know their traffic is now flowing unencrypted. A constraint is that this traffic is behind the customer fire wall.

Risk Assessment

The risk score and category were determined using InterSystems' Risk Rating process (outlined in the hs-2020), 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
Security:	3-Medium Risk	Severity of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 3 out of 5
Operational:	5-Very High Risk	Severity of typical adverse outcome = 4 out of 5 Likelihood of typical adverse outcome = 4 out of 5

Recommended Actions

A correction for this issue is available from the InterSystems Worldwide Response Center (WRC) and is strongly recommended for all customers using HealthShare 2020.2.

This correction is identified as HSIEO-3593 and is available via Ad hoc change file (patch) or full kit distribution from the WRC. If you choose an ad hoc, be sure to follow the provided installation steps. The correction will be included in all future product releases.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2020-09".

End of Alert HS2020-09-01

Detail of Alerts

HS2020-09-02: Invalid Patient Medication Streamlet Triggers Erroneous Data Ingestion Errors for Subsequent Patients

Issue date: 22-DEC-2020

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Health Insight
Versions:	2019.1.0, 2019.1.2, 2019.1.3, 2020.1, and 2020.2
System areas affected:	Health Insight data transfer from SDA3 to HSAA source tables
Reference:	HSHI-4616

Summary of Issue

Health Insight ingests data from Unified Care Record using a transfer operation. If an error occurs in the transfer operation because one patient's medication administration streamlet contains bad data, it can lead to errors for subsequent patients even though their streamlets contain valid medication administration data.

An initial data error that occurs during the transfer of a patient's medication administration streamlet into Health Insight blocks the transfer of that patient's data as expected and reports an error describing the invalid data. However, this initial error can then block the transfer of medication administration data from each subsequent patient processed in the same transfer operation job, with an error message of:

```
<INVALID OREF>zUpdateMedicationAdministration+8 ^HSAA.TransferSDA3.Post.1 > ERROR
<HSAAErr>ProcessStreamlet: Error caught processing streamlet.
```

While the initial error type may vary (for example, a datatype validation error in a timestamp, or a MAXLEN error on a long string), the subsequent errors that are triggered are all of the same type, namely <INVALID OREF>.

This issue can lead to a number of patients with missing medication administration data in Health Insight. The missing data will be indicated by an <INVALID OREF> error message for each affected patient. Missing patient data could potentially impact the following Health Insight and Unified Care Record functionality:

- Dynamic cohorts
- Advanced clinical notifications
- Clinical message delivery subscriptions

A customer who sees one or more of the error messages described above may be experiencing this issue.

Regardless of whether a customer has encountered this issue, all Health Insight customers should contact the InterSystems Worldwide Response Center to request an adhoc to remedy the issue. After applying the adhoc patch, customers should check for patients with transfer errors and resend each failed patient as appropriate.

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:	3-Medium Risk	Severity of typical adverse outcome = 2 out of 5 Likelihood of typical adverse outcome = 4 out of 5
Operational:	3-Medium Risk	Severity of typical adverse outcome = 2 out of 5 Likelihood of typical adverse outcome = 4 out of 5

Recommended Actions

InterSystems strongly recommends that customers take the following action, regardless of whether they encounter the <INVALID OREF> error as described in this alert:

1. Contact the Worldwide Response Center to request an Ad hoc change file (patch) that includes the correction for this issue, HSHI-4616, and apply the Ad hoc to your Health Insight instance.
2. After the adhoc is applied, obtain a list of patients with transfer errors from the Health Insight Management Portal: Internal Management > Patient Error Management, or by using the corresponding APIs, and then resend any patients that had errors.

This correction is identified as HSHI-4616 and is available via Ad hoc change file (patch) or full kit distribution from the WRC. The correction will be included in all future product releases.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2020-09".

End of Alert HS2020-09-02

Detail of Alerts

HS2020-09-03: FHIR Resource Purge Task in ODS fails with <METHOD NOT FOUND>

Issue date: 22-DEC-2020

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

Versions: 2020.1 with the ODS and FHIR

System areas affected: Database Size

Reference: IF-1219

Summary of Issue

Scheduled purging of FHIR Resources from the ODS FHIR Gateway may fail with a <METHOD NOT FOUND> error. This prevents the resources from being purged which causes increased database sizes as purge-ready FHIR Resources accumulate within the ODS.

This issue affects database sizes on the ODS. Because FHIR resources are not properly purged according to configured retention times, database storage is not released and the database for the ODS will continue to grow. If left in this state for a prolonged period of time, the ODS may run out of database space resulting in system downtime.

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

View the error logs on your ODS namespace to see if you are impacted by this problem. Contact the WRC to request an Ad hoc, IF-1219. After application of the update, the system should begin purging FHIR resources without error.

This correction is identified as IF-1219 and is available via Ad hoc change file (patch) or full kit distribution from the WRC. The correction will be included in all future product releases.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2020-09".

End of Alert HS2020-09-03

– End of HS2020-09 Alerts –

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 in 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

5	**Catastrophic**	Multiple patients	Death. Permanent life-changing incapacity. Severe injury or incapacity from which recovery is not expected in the short term.
4	**Major**	Single patient	Death. Permanent life-changing incapacity. Severe injury or incapacity from which recovery is not expected in the short term.
		Multiple patients	Severe injury or incapacity from which recovery is expected in the short term. Severe psychological trauma.
3	**Moderate**	Single patient	Severe injury or incapacity from which recovery is expected in the short term. Severe psychological trauma.
		Multiple patients	Minor injury from which recovery is not expected in the short term. Significant psychological trauma.
2	**Minor**	Single patient	Minor injury from which recovery is not expected in the short term. Significant psychological trauma.
		Multiple patients	Minor injury from which recovery is expected in the short term. Minor psychological upset. Inconvenience.
1	**Minimal**	Single patient	Minimal injury from which recovery is expected in the short term. Minor psychological upset. Inconvenience.

Description of Outcome Likelihood

5	**Very High**	Will undoubtedly happen/recur, possibly frequently	Expected to occur at least daily
4	**High**	Will probably happen/recur, but it is not a persisting issue/ circumstances	Expected to occur at least weekly
3	**Medium**	Might happen or recur occasionally	Expected to occur at least monthly
2	**Low**	Do not expect it to happen/recur but it is possible it may do so	Expected to occur at least annually
1	**Very low**	This will probably never happen/recur	Not expected to occur for years

Risk Score & Category

The combination of the Severity 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

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 HS2020-09 Alert Communication –