HealthShare HS2020-05 Alert

20-MAY-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 several risks related to the HealthShare Clinical Viewer, the ODS and online backups of large databases, that may affect the security, privacy, or operational use of InterSystems HealthShare.

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. The Alert process complements our existing support processes.

This document contains the following Alerts:

Alert	Product & Versions Affected	Risk Category & Score
HS2020-05-01: On an Android device that is in sleep mode, the standalone v2 Clinical Viewer using Chrome does not time out	The affected products & versions are: • Information Exchange 2018.1 • Unified Care Record 2019.1, 2019.1.2, 2019.2	3-Medium Risk (Security)
HS2020-05-02: FHIR Request from ODS Not Logged in ATNA if Custom Pairs are Used on the Patient Streamlet	The affected products & versions are: • Information Exchange 2018.1 • Unified Care Record 2019.1, 2019.2, 2020.1	3-Medium Risk (Privacy)
HS2020-05-03: Possible Data Integrity Issues with Online Backup of Large Databases	The affected products & versions are: • All versions of all InterSystems HealthShare products	5-Very High Risk (Operational)

We encourage you to read the information below and then reach out to InterSystems Support at support@intersystems.com or +1.617.621.0700 with any questions that might arise.

Detail of Alerts

HS2020-05-01: On an Android device that is in sleep mode, the standalone V2 Clinical Viewer using Chrome does not time out

Issue date: 20-MAY-2020

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Information Exchange and Unified Care Record
Versions:	2018.1, 2019.1, 2019.1.2, 2019.2
System areas affected:	V2 Clinical Viewer without Navigation Application (standalone, without frame)
Reference:	HSCV-3818

Summary of Issue

When a user accesses the V2 Clinical Viewer using the Chrome browser on an Android device, and the device then goes into sleep mode, the V2 Clinical Viewer may not log out after the configured session timeout period has expired. This issue only occurs when accessing the V2 Clinical Viewer as a standalone, unframed application (without the Navigation Application).

Risk Assessment

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

Privacy:	2 – Low Risk	Severity of typical adverse outcome = 2 out of 5 Likelihood of typical adverse outcome = 3 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

Recommended Actions

Examine your use of the relevant HealthShare releases to determine if you use the V2 Clinical Viewer as a stand-alone, unframed application (without the Navigation Application).

To mitigate the risk from this issue, InterSystems strongly recommends that customer organizations take the following actions:

- Enforce device-level authentication upon device resume/power-up on all devices.
- Customers using Unified Care Record 2019.2 may also obtain and apply patch to resolve the issue.

The correction for this defect is identified as HSCV-3818 which will be included in all future product releases. For HealthShare 2019.2 customers the correction is also available via an Ad hoc change file (patch) or full kit distribution from the WRC.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference "Alert HS2020-05".

End of Alert HS2020-05-01

HS2020-05-02: FHIR Request from ODS Not Logged in ATNA if Custom Pairs are Used on the Patient Streamlet

Issue date: 20-MAY-2020

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products: Information Exchange and Unified Care Record

Versions: 2018.1, 2019.1, 2019.2, 2020.1

System areas affected: FHIR Requests, ODS

Reference: HSIEC-2932 / MCZ151

Summary of Issue

InterSystems has corrected an issue that occurs when a FHIR request from the Operational Data Store (ODS) references CustomPairs, a deprecated method of extending SDA, on the Patient streamlet. These requests are not logged to the ATNA audit.

This is considered a privacy issue as it impacts the ability to produce a full record of disclosures and to detect improper disclosure.

A correction for this defect is available via Ad hoc distribution from the InterSystems Worldwide Response Center (WRC).

Full details of the identified issue appear in the Technical Addendum for HS2020-05-02

Risk Assessment

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

Privacy:	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 affected customer organizations apply the correction for this defect. It is identified as MCZ151 and is available via Ad hoc distribution from the InterSystems Worldwide Response Center (WRC). The fix will also be included in all future product releases, beginning with HealthShare 2020.2.

The correction for this defect does not address previous FHIR requests that were not logged in ATNA.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference "Alert HS2020-05".

Technical Addendum for HS2020-05-02

Description of Issue

InterSystems has corrected an issue that occurs when a FHIR request from the Operational Data Store (ODS) references CustomPairs on the Patient streamlet. These requests are not logged to the ATNA audit.

Only customers who meet the following criteria are affected by this defect:

- Request FHIR data
- Use the Operational Data Store (ODS)
- Use CustomPairs on the Patient streamlet. Other streamlets are not affected by this issue. CustomPairs are an older method of extending SDA, prior to the development of SDA Extensions which were introduced in HealthShare Information Exchange 15.01. Customers who do not use CustomPairs and instead use SDA Extensions on the Patient streamlet or do not extend the Patient streamlet are not affected by this issue.

This is considered a privacy issue as it impacts the ability to produce a full record of disclosures and to detect improper disclosure.

A correction for this defect is available via Ad hoc distribution from the InterSystems Worldwide Response Center (WRC).

Recommended Action

Customers should examine their Patient streamlet extension to identify if CustomPairs are used.

InterSystems strongly recommends that affected customer organizations apply the correction for this defect.

The correction for this defect does not address previous FHIR requests that were not logged in ATNA.

Information about the Correction

The correction for this defect is identified as MCZ151 and is available via Ad hoc change file (patch) or full kit distribution from the WRC. The fix will also be included in all future product releases, beginning with HealthShare 2020.2.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference “Alert HS2020-05”.

End of Alert HS2020-05-02

HS2020-05-03: Possible Data Integrity Issues with Online Backup of Large Databases

Issue date: 20-MAY-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: All InterSystems HealthShare® products

Versions: All versions

System areas affected: Online Backup

Reference: RJF437, RJF438

Summary of Issue

InterSystems has corrected two defects that affect online backup of very large databases. Backups taken via external methods, such as snapshots or direct file copies, are not affected. These defects exist in all released versions of all InterSystems products.

The first defect only affects databases with more than 231 blocks. It results in a degraded database after restoring from an online backup. For example, databases that have a block size of 8 KB (the default) are only affected if they are larger than 16 TB. The correction for this defect is identified as RJF437.

The second defect affects databases that have a block size of 8 KB and that are larger than ~29 TB. With this defect, the online backup fails due to an inaccurate <DATABASE> error; this results in a backup that cannot be restored. The correction for this defect is identified as RJF438. Note that this defect also affects databases that have block sizes smaller than 8 KB.

The corrections for these defects will be included in all future product releases. They are also available by requesting an Ad hoc distribution from the WRC.

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

If your databases fall into the size limits described in the alert, use a backup method other than online backup.

InterSystems recommends that customer organizations take the following actions:

1. If you wish to use online backup for large databases, request an ad hoc distribution from the WRC

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference "Alert HS2020-05".

End of Alert HS2020-05-03

– End of 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:

Severity	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 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:

Severity	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	Critical risk
4	High risk
3	Moderate risk
2	Low risk
1	Minimal 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	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	Critical risk
4	High risk
3	Moderate risk
2	Low risk
1	Minimal 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
	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

– End of HS2020-05 Alert Communication –

