InterSystems
Health | Business | Government

HealthShare Alert

HealthShare HS2020-03 Alert

25-Mar-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 that may affect you when using 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 operational 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

The information provided in this message is proprietary information being shared with you on the basis of your identification as a contact for product updates from InterSystems. This message may contain confidential information, and you should ensure that its contents are disclosed solely in compliance with any nondisclosure obligations between our organizations. The information provided in this InterSystems Product Alert or Service Bulletin is provided "as is" and without additional warranty. Except as provided for in a mutually executed agreement between you and InterSystems Corporation, its subsidiaries, and affiliates, InterSystems disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose.

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 & Advisory process complements our existing support processes.

This document contains the following Alerts:

Alert	Product & Versions Affected	Risk Category & Score
HS2020-03-01: Break-the-Glass Events not Properly Audited for ODS	HealthShare Unified Care Record 2019.1 and 2019.2 using the Operational Data Store	4-High Risk (Privacy)
HS2020-03-02: Archiving of Historical Aliases Causes System Hang	HealthShare Patient Index 2018.1, 2019.1, and 2019.2	3-Medium Risk (Operational)
HS2020-03-03: Permissions to Access Patient Records Vary Between Clinical Viewer v1 and v2	HealthShare Information Exchange and Unified Care Record v2 viewer in 2018.1, 2019.1 and 2019.2	4-High Risk (Privacy)
HS2020-03-04: Invalid Handling of Improperly Formatted Reference Ranges in HL7 V2 Result Messages	HealthShare Information Exchange 15.03 and 2018.1; Unified Care Record 2019.1 and 2019.2	3-Medium Risk (Clinical)
HS2020-03-05: AngularJS 1.5.8 Vulnerability	All versions of HealthShare Personal Community	External (Security)
HS2020-03-06: “LogCounter” in Access Gateway is Reset on Upgrade	All versions of HealthShare Information Exchange and Unified Care Record up to and including 2019.1	3-Medium Risk (Operational)
HS2020-03-07: Possible Data Integrity Issues after Compaction or Defragmentation	All HealthShare products starting from HealthShare 15.x and Personal Community 12.x and above. HealthShare Health Connect 2019.1.0 and 2019.1.1 based on InterSystems IRIS®, and older Health Connect versions built on Cache/Ensemble 2016.2 and above.	2-Low 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:

HS2020-03-01: Break-the-Glass Events not Properly Audited for ODS

Issue date: 25-Mar-2020

Risk Category and Score

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

Version and System Area Affected

Product Versions:	HealthShare Unified Care Record 2019.1 and 2019.2
System areas affected:	Auditing
Reference:	HSIEO-2405

Summary of Issue

"Override Consent Policy" (or "break-the-glass") events allow a clinician to search for a patient and override consent policies that would otherwise block them from viewing certain details. For customers using the Operational Data Store (ODS), these events are not properly recorded in the audit log, resulting in an empty "Emergency Access Log" management report.

Another, related audit event is being recorded, and details of how to recover missing audit information is included in the Technical Addendum for HS2020-03-01.

A correction for this issue is available from the InterSystems Worldwide Response Center. Use reference HSIEO-2405.

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:	4-High Risk	Severity of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

InterSystems recommends that customers take the following actions:

1. If you use or plan to use the ODS, obtain and apply the correction.
2. Consult the Technical Addendum for HS2020-03-01 to identify the missing audit items so you can maintain compliance reporting requirements for your system.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference "Alert HS2020-03-01".

Technical Addendum for HS2020-03-01

Description of Issue

When a clinician accesses a patient record and overrides consent policies that would otherwise block them from viewing certain details, three audit events should be recorded:

- *SearchPatientBreakGlass* - The Registry received a patient search response from the MPI and is about to send the result to the Access Gateway. The request included an emergency consent override. A single event is generated for the MPIID.
- *ConsentEvaluationBreakGlass* - Consent policies were evaluated at the Access Gateway during a patient search with an emergency consent override. A separate event is generated for each MRN.
- *RecordRequestBreakGlass* - An Edge Gateway or the ODS received a fetch request for patient clinical data with an emergency consent override. A separate event is generated for each MRN.

For customers using the Operational Data Store (ODS), the *RecordRequestBreakGlass* is not being recorded in the audit log. The "Emergency Access Log" management report is based on this field, so this report appears empty. The other two audit events are being recorded, so there is still a record of the activity.

You can use the following query in your audit namespace to locate these events. You can adjust the dates in the query to capture any missed events from the time you started using the ODS until the present day:

```
SELECT EventDateTime,UserName,PatientFacility,MRNs
FROM HS_IHE_ATNA_Repository.Aggregation
where EventType = 'ConsentEvaluationBreakGlass'
and IndexedDate > '2020-01-01'
and IndexedDate < '2020-03-15'
```

A correction for this issue is available from the InterSystems Worldwide Response Center. Use reference HSIEO-2405.

Recommended Action

InterSystems recommends that customers take the following actions:

- Obtain and apply the correction.
- Run the query above to recover any audit data missing for your Emergency Access Log in order to maintain compliance reporting requirements.

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. Reference “Alert HS2020-03-01”.

– End of Alert – HS2020-03-01

HS2020-03-02: Archiving of Historical Aliases Causes System Hang

Issue date: 25-Mar-2020

Risk Category and Score

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

Version and System Area Affected

Product Versions:	HealthShare Patient Index 2018.1, 2019.1, and 2019.2
System areas affected:	Database Size, Patient Add/Update, System Responsiveness
Reference:	HSPI-1745/NDT326, HSPI-1766/NDT330

Summary of Issue

The “Preserve Historical Data” feature currently permits storage of duplicate *Primary Names* and *Aliases* for individual patients. This duplication results in unnecessary expansion of records and consequent increases in time required for patient search and add.

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

Recommended Actions

InterSystems strongly recommends that customers take the following actions:

1. Run the Data Cleanup Utility described in the Technical Addendum for HS2020-03-02.
2. Install the ad hoc described in the Technical Addendum for HS2020-03-02.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference “Alert HS2020-03-02”.

Technical Addendum for HS2020-03-02

Description of Issue

The “Preserve Historical Values” feature currently permits storage of duplicate *Primary Names and Aliases* for individual patients; no other fields display this behavior. The names, which are stored in both the raw and normalized patient tables, are used for comparison against future patients. This duplication results in unnecessary expansion of records and consequent increases in time required for patient search and add. The duplicated records continue to increase in size as new names are received, eventually resulting in system timeouts on patient update. The ad hoc is required to prevent duplicated names from being stored. Subsequently, the data cleanup utility will purge duplicate names from the raw patient table. Following the data cleanup, a linkage rebuild repopulates the normalized table.

This issue only affects users who have enabled the “Preserve Historical Values” feature. This feature is only available from HealthShare Patient Index 2018.1 or later and is disabled by default.

Recommended Action

InterSystems strongly recommends that customers apply the corrections for this defect by completing the following procedure:

1. Request an Ad Hoc kit from the Worldwide Response Center, using references NDT326 and NDT330.
2. Log in to a Terminal session on your HealthShare Patient Index instance, and ensure you are in the Patient Index production’s namespace
3. Execute the following code:

   ```
   w ##class(HSPI.Data.Patient).deduplicateNames()
   ```

   This will run the utility in read-only mode and report how many records require updating.
4. If any updates are required, run the following code:

   ```
   w ##class(HSPI.Data.Patient).deduplicateNames(0)
   ```

   Passing an argument of 0 to the function will cause it to update the records.
5. Rebuild your linkage data, using the Normalized option.

Information about the Correction

The correction for this defect is identified as HSPI-1745/NDT326, which will be included in all future product releases and is also available via Ad Hoc from the Worldwide Response Center.

The utility for already-affected systems is identified as HSPI-1766/NDT330.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference “Alert HS2020-03-02”.

– End of Alert – HS2020-03-02

HS2020-03-03: Permissions to Access Patient Records Vary Between Clinical Viewer v1 and v2

Issue date: 25-Mar-2020

Risk Category and Score

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

Version and System Area Affected

Product Versions:	HealthShare Information Exchange and Unified Care Record v2 viewer in 2018.1, 2019.1 and 2019.2
System areas affected:	User Permissions
Reference:	HSCV-2537/WRS1040

Summary of Issue

If you either use the provided `HS_Operator` role or create users with the patient search resource but without the patient retrieval resource, those users will encounter the issue with Clinical Viewer v2.

A correction for this issue is available in the form of an Ad Hoc from the InterSystems Worldwide Response Center. Use reference WRS1040.

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:	4-High Risk	Severity of typical adverse outcome = 2 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

InterSystems strongly recommends that customers take the following actions:

1. Review the information in the Technical Addendum for HS2020-03-03
2. Apply the correction for this defect identified in WRS1040.

This correction is available in the form of an Ad Hoc from the InterSystems Worldwide Response Center.

Technical Addendum for HS2020-03-03

Description of Issue

Roles configured with the patient search resource and without the patient retrieval resource can access patient charts in the v2 viewer. The only role provided that includes this scenario is the `HS_Operator` role. This issue has been resolved in future kits and should be requested as an ad hoc for users of HealthShare 2018.1, 2019.1 and 2019.2.

Recommended Action

InterSystems strongly recommends that customers take the following action:

1. Apply the correction for this defect identified in WRS1040. This correction is available in the form of an Ad Hoc from the InterSystems Worldwide Response Center.

Information about the Correction

The correction for this defect is identified as WRS1040, which will be included in all future product releases. It is also available via Ad Hoc change or full kit distribution from the InterSystems Worldwide Response Center.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference “Alert HS2020-03-03”.

– End of Alert – HS2020-03-03

HS2020-03-04: Invalid Handling of Improperly Formatted Reference Ranges in HL7 V2 Result Messages

Issue date: 25-Mar-2020

Risk Category and Score

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

Version and System Area Affected

Product Versions:	HealthShare Information Exchange 15.03 and 2018.1 and Unified Care Record 2019.1 and 2019.2
System areas affected:	Observations and Results
Reference:	HSIEC-1926/MCZ125, HSIEC-2184/SKK1035

Summary of Issue

InterSystems has corrected a patient safety issue that occurs when the Reference Range (OBX-7) value in HL7 V2 messages is a single number. Unified Care Record improperly interprets a single number as the lower bound in a reference range. Therefore, a reference range of “0” is interpreted as “>0”, which can lead users to improperly interpret results or fail to identify abnormal ones.

A correction for this issue is available in the form of an Ad Hoc from the InterSystems Worldwide Response Center. Use references HSIEC-1926/MCZ125 and HSIEC-2184/SKK1035.

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

Recommended Actions

InterSystems strongly recommends that customers take the following actions:

1. Review the information in the Technical Addendum for HS2020-03-04
2. Apply the corrections for this defect, identified as MCZ125 and SKK1035. and are available via Ad hoc distribution from the InterSystems Worldwide Response Center.
3. The corrections for this defect do not address HL7 V2 messages that have already been processed. To correct previously processed messages, the messages must be reloaded and reprocessed.

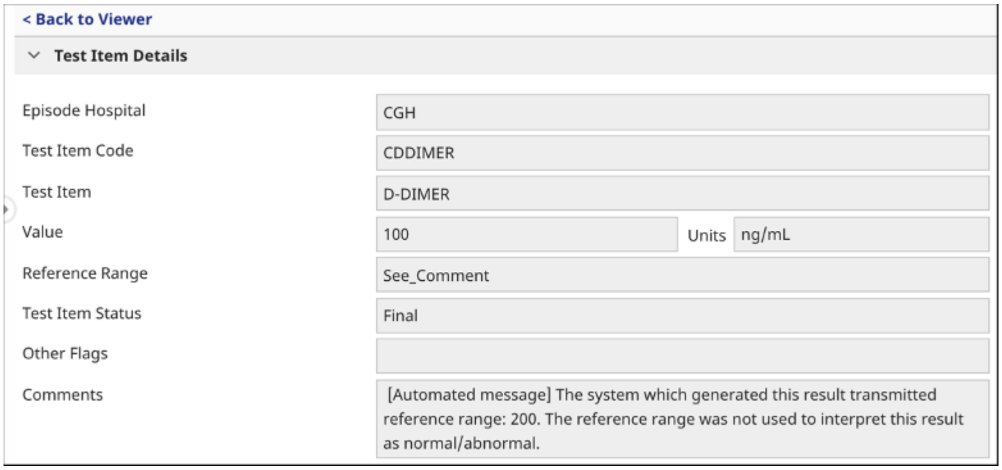
The information provided in this message is proprietary information being shared with you on the basis of your identification as a contact for product updates from InterSystems. This message may contain confidential information, and you should ensure that its contents are disclosed solely in compliance with any nondisclosure obligations between our organizations. The information provided in this InterSystems Product Alert or Service Bulletin is provided "as is” and without additional warranty. Except as provided for in a mutually executed agreement between you and InterSystems Corporation, its subsidiaries, and affiliates, InterSystems disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose.

Technical Addendum for HS2020-03-04

Description of Issue

InterSystems has corrected a patient safety issue that occurs when the *Reference Range* (OBX-7) value in HL7 V2 messages is a single number. Unified Care Record improperly interprets a single number as the lower bound in a reference range. Therefore, a reference range of “0” is interpreted and stored in the streamlet on the Edge Gateway as “>0”. The system uses this converted reference range to compute the *Flag* column value in the Clinical Viewer **Lab Results Table** and in other lab result views if an *Abnormal Flag* (OBX-8) was not present in the HL7 V2 message (see Additional Information below for more details). This can cause flags to be incorrect.

The correction for this defect replaces reference ranges that are not in the format of “>x”, “<x”, “x – y” (where “x” and “y” are numbers) or text values (e.g., “NEGATIVE”) with the literal string “See_Comment” in the streamlet on the Edge Gateway. A note containing the original reference range value is placed within the streamlet comment and is visible in the Clinical Viewer **Test Item Details** *Comments* field, as shown in the screenshot below. A warning is also logged in the production Event Log on the Edge Gateway. *Flag* values will not be computed for these values. If an OBX-8 value is present in the HL7 message, it will be stored and displayed in the Clinical Viewer in all lab result views except for the **Lab Results Table** *Flag* column value.



Episode Hospital	CGH		
Test Item Code	CDDIMER		
Test Item	D-DIMER		
Value	100	Units	ng/mL
Reference Range	See_Comment		
Test Item Status	Final		
Other Flags			
Comments	[Automated message] The system which generated this result transmitted reference range: 200. The reference range was not used to interpret this result as normal/abnormal.		

Screenshot of Test Item Details, displaying See_Comment value and automated message in ***Comments*** field.

As a special case, the correction also accounts for reference ranges of “0”, as this value is relevant for computing the *Flag* in the Clinical Viewer. A reference range of "0" is converted to “0 – 0” to conform to the HL7 V2 format for OBX-7. No warning is logged.

Additional Information

If an OBX-8 value is present in the HL7 V2 message, that value determines the following behavior in the Clinical Viewer lab result views. If an OBX-8 value is not present, the flag computed by the Clinical Viewer will be used in these views instead.

- The red row indicator in all views where the red row indicator is present.
- The color of the Lab Results value in all views.
- The value in the **Test Item Details** *Other Flag* field.
- The value in the **Results Detail** *Message Flag* field.

Recommended Action

InterSystems strongly recommends that customers take the following actions:

1. Apply the corrections for this defect, identified as MCZ125 and SKK1035. and are available via Ad hoc distribution from the InterSystems Worldwide Response Center. .

2. The corrections for this defect do not address HL7 V2 messages that have already been processed. To correct previously processed messages, the messages must be reloaded and reprocessed.

Information about the Correction

The corrections for this defect are identified as HSIEC-1926/MCZ125 and HSIEC-2184/SKK1035, will be included in all future product releases. They are also available via Ad hoc change file (patch) or full kit distribution from the Worldwide Response Center.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference “Alert HS2020-03-04”.

– End of Alert – HS2020-03-04

HS2020-03-05: AngularJS 1.5.8 Vulnerability

Issue date: 25-Mar-2020

Risk Category and Score

There is no risk rating for this issue because the reported vulnerability does not affect the HealthShare Personal Community product, however Customers that choose to implement extensions in the product will need to evaluate their code against this reported vulnerability.

Version and System Area Affected

Product Versions:	All versions of HealthShare Personal Community
System areas affected:	User Interface, Customization
Reference:	HSPC-9876

Summary of Issue

The Personal Community public application currently uses AngularJS version 1.5.8.

This version of AngularJS has a known vulnerability. After an internal review, InterSystems has determined that the HealthShare Personal Community product as released by InterSystems is not affected by this vulnerability, but Customers that have implemented custom extensions through their own code to the product may be affected.

Recommended Actions

InterSystems strongly recommends that customers take the following actions:

1. Review the information in the Technical Addendum for HS2020-03-05
2. Customers that choose to implement extensions in the product will need to evaluate their code against this reported vulnerability.

The information provided in this message is proprietary information being shared with you on the basis of your identification as a contact for product updates from InterSystems. This message may contain confidential information, and you should ensure that its contents are disclosed solely in compliance with any nondisclosure obligations between our organizations. The information provided in this InterSystems Product Alert or Service Bulletin is provided "as is" and without additional warranty. Except as provided for in a mutually executed agreement between you and InterSystems Corporation, its subsidiaries, and affiliates, InterSystems disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose.

Technical Addendum for HS2020-03-05

Description of Issue

The Personal Community public application currently uses AngularJS version 1.5.8.

This version of AngularJS has a known vulnerability. In this version, both Firefox and Safari are vulnerable to XSS in `$sanitize` if an inert document created via `document.implementation.createHTMLDocument()` is used. Additional information about this can be found at:

https://github.com/angular/angular.js/commit/8f31f1ff43b673a24f84422d5c13d6312b2c4d94

After an internal review, InterSystems has determined that the official release of HealthShare Personal Community is not affected by the vulnerability, but if a Customer has developed custom code extensions to their implementation of the product, they should assess their coding to determine whether or not they are affected.

Recommended Action

Customers that choose to implement extensions in the product will need to evaluate their code against this reported vulnerability.

Information about the Correction

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference "Alert HS2020-03-05".

– End of Alert – HS2020-03-05

HS2020-03-06: “LogCounter” in Access Gateway is Reset on Upgrade

Issue date: 25-Mar-2020

Risk Category and Score

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

Version and System Area Affected

Product Versions:	All versions of HealthShare Information Exchange and Unified Care Record up to and including 2019.1
System areas affected:	Auditing
Reference:	HSIEO-1983

Summary of Issue

HealthShare audits a variety of user and system actions. When there is an SDA associated with a particular user action, for example, a patient fetch, the relevant SDA container is saved and marked with a unique "initiating log ID" so that it can be associated with the audit log entry for the action that created it. The counter that produced the initiating log ID was being inadvertently reset whenever an Access Gateway was reset, resulting in unrelated SDA containers being marked with the same initiating log ID.

In a UCR system affected by this issue, when you view the SDA associated with an audit log entry, you will see the correct SDA container associated with the underlying audit event, as well as one or more SDA containers for other audit events related to different patients. The patient name or MPIID that appears in the container can be used to distinguish the correct SDA from the unrelated ones.

No audit data is lost, and the audit log is complete, however, some audit log entries have additional erroneous data associated with them.

A fix for this issue maintains the uniqueness of initiating log ids when an Access Gateway is reset. For existing audit logs that are affected by this issue, there is no repair utility. Users of the audit logs should be made aware that they must pay attention to the patient name or MPIID on the associated SDA containers in order to identify the correct container associated with the user action in the audit log entry.

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

Recommended Actions

Users of the audit logs should be made aware that they must pay attention to the patient name or MPIID on the associated SDA containers in order to identify the correct container associated with the user action in the audit log entry.

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference “Alert HS2020-03-06”.

– End of Alert – HS2020-03-06

HS2020-03-07: Possible Data Integrity Issues after Compaction or Defragmentation

Issue date: 25-Mar-2020

Risk Category and Score

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

Version and System Area Affected

Product Versions:	All HealthShare products starting from HealthShare 15.x and Personal Community 12.x and above. HealthShare Health Connect 2019.1.0 and 2019.1.1 bases on InterSystems IRIS, and older Health Connect versions built on Cache/Ensemble 2016.2 and above.
System areas affected:	Database Operations
Reference:	RJF423/RJF424

Summary of Issue

InterSystems has corrected two defects that, in rare circumstances, can result in data integrity corruption after running global compaction, database compaction, or database defragmentation. InterSystems recommends avoiding these utilities until after applying the corrections listed below.

Corrections for both defects will be included in all future product releases. They are also available by requesting an Ad hoc distribution from the InterSystems Worldwide Response Center (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:	2-Low Risk	Severity of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 2 out of 5

Recommended Actions

InterSystems recommends that customers take the following actions:

1. Review the information in the Technical Addendum for HS2020-03-07
2. Avoid using these utilities listed above, until after applying the corrections listed below.
3. Request an Ad hoc distribution from the InterSystems Worldwide Response Center (WRC).

If you have any questions regarding this alert, please contact the Worldwide Response Center. Reference "Alert HS2020-03-07 Dev Key RJF423/RJF424".

Technical Addendum for HS2020-03-07

Description of Issue

InterSystems has corrected two defects that, in rare circumstances, can result in data integrity corruption after running global compaction, database compaction, or database defragmentation. InterSystems recommends avoiding these utilities until after applying the corrections listed below.

1. The first defect is caused by database compaction, defragmentation, or global compaction, and can result in database corruption. If you have used one of these utilities on a database, InterSystems recommends that you perform an integrity check on it. This will identify any data corruption that has occurred. The correction is RJF424.

   This defect has been observed on deployed systems and exists for the following versions:

   - All released versions of InterSystems IRIS and IRIS for Health
   - Caché/Ensemble versions beginning with 2016.2.0
   - All HealthShare products based on the above Data Platforms versions
2. The second defect may occur under extremely rare timing conditions, if processes are modifying (sets/kills) a database concurrently with database compaction or defragmentation. In this case, the processes may either make global updates that are not written to the database or access stale data. There is no way to definitively determine if this has occurred. Global compaction is unaffected by this defect. The correction is RJF423.

   This second defect exists in all released versions of all InterSystems products, though it is highly unlikely to have occurred on deployed systems

These utilities are not used within the HealthShare products; however, they are available to HealthShare environment administrators or Database Administrators outside the product and may be used to maintain the HealthShare environment.

Recommended Action

InterSystems recommends that customers take the following actions:

1. Avoid using these utilities listed above, until after applying the corrections listed below.
2. Request an Ad hoc distribution from the InterSystems Worldwide Response Center (WRC).

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. Reference “Alert HS2020-03-07 Dev Key RJF423/RJF424”.

– End of Alert – HS2020-03-07

– End of Alerts –

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

The information provided in this message is proprietary information being shared with you on the basis of your identification as a contact for product updates from InterSystems. This message may contain confidential information, and you should ensure that its contents are disclosed solely in compliance with any nondisclosure obligations between our organizations. The information provided in this InterSystems Product Alert or Service Bulletin is provided "as is" and without additional warranty. Except as provided for in a mutually executed agreement between you and InterSystems Corporation, its subsidiaries, and affiliates, InterSystems disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose.

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	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	**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 HS2020-03 Alert Communication –

The information provided in this message is proprietary information being shared with you on the basis of your identification as a contact for product updates from InterSystems. This message may contain confidential information, and you should ensure that its contents are disclosed solely in compliance with any nondisclosure obligations between our organizations. The information provided in this InterSystems Product Alert or Service Bulletin is provided "as is" and without additional warranty. Except as provided for in a mutually executed agreement between you and InterSystems Corporation, its subsidiaries, and affiliates, InterSystems disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose.