HealthShare HS2022-01 Alert

1-MAR-2022

Dear HealthShare Customer:

I am writing because you are listed as the Risk Contact for your organization. When risks have been uncovered that concern your use of our products, InterSystems is committed to providing you the necessary information so that you can assess your situation as quickly as possible.

This package contains 22 alerts that affect InterSystems IRIS for Health™ and HealthShare® products. The alerts are grouped by product and cover all risk areas: Clinical Safety, Patient Privacy, Security, and Operations. Please review the issues and take the recommended actions as appropriate to your situation.

InterSystems uses two channels to communicate risks:

- *Alert* communications such as this one are sent to Risk Contacts periodically for all high risk issues and for other issues that are judged to merit an alert. Alerts are also posted on the InterSystems Website.
- *Advisories* for lower risk issues are posted to the InterSystems Website. No communication is sent to Risk Contacts, but you can subscribe to receive notifications of advisories.

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, Ph.D.
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

Alert	Products & Versions	Risk Rating
HS2022-01-01: Vaccination Dates Misrepresented in Some Circumstances	• All versions of: ○ Information Exchange ○ Unified Care Record ○ Personal Community ○ HealthShare Health Connect ○ InterSystems IRIS for Health	• Medium Risk: *Operational* • Low Risk: *Clinical Safety*
HS2022-01-02: Invalid Handling of Multiple Reference Ranges in CDA and C-CDA Documents	• All versions of: ○ Information Exchange ○ Unified Care Record (through 2021.1)	• Medium Risk: *Clinical Safety*
HS2022-01-03: Security Check for Emergency Access to Patient Records Fails to Occur in Some Situations	• All versions of: ○ Information Exchange ○ Unified Care Record (through 2020.2)	• Medium Risk: *Privacy*
HS2022-01-04: Security Vulnerability in Unified Care Record 2020.2.0	• Unified Care Record: ○ 2020.2.0 (Build 8620)	• High Risk: *Privacy*
HS2022-01-05: Customers on Unified Care Record 2020.2 and 2021.1 Must Install a Patch Before Upgrading to a Later Version	• Version 2020.2, 2021.1 of: ○ Unified Care Record ○ Clinical Viewer ○ Health Insight ○ Patient Index ○ Personal Community ○ Care Community • Version 2020.2, 2021.1, 2021.2, 2021.3 of: ○ Provider Directory	• High Risk *Operational*
HS2022-01-06: Configuring the Classic Clinical Viewer Requires Outdated Third-Party Software	• All versions of: ○ Unified Care Record (Classic Clinical Viewer only)	• High Risk: *Security*
HS2022-01-07: Users may not be able to Log Out of Clinical Viewer	• All versions of: ○ Information Exchange ○ Unified Care Record (through 2020.2)	• High Risk: *Privacy*
HS2022-01-08: Access Gateway Aggregation Cache Grows over Time	• Unified Care Record: ○ 2020.1, 2020.2, 2021.1, 2021.2	• Low Risk: *Operational*
HS2022-01-09: Incompatibility in HL7toSDA3 Customizations when Upgrading from HealthShare 15.03 or earlier	• Information Exchange: ○ 15.03 or earlier (when upgrading to Unified Care Record)	• Not Rated
HS2022-01-10: IHE Endpoints should use Appropriate Credentials	• All versions of: ○ Information Exchange ○ Unified Care Record	• Medium Risk *Security*
HS2022-01-11: ODS Namespace Reactivation Can Result in Prolonged Downtime	• Unified Care Record: ○ 2019.1, 2019.2	• High Risk: *Operational*
HS2022-01-12: Upgrade of ODS may Require Manual Intervention to Complete	• Unified Care Record: ○ 2020.1 (when upgrding to version 2020.2)	• Very High Risk: *Operational*
HS2022-01-13: ODS Audit Data Inaccessible after Upgrade to Version 2020.1	• Unified Care Record: ○ 2019.1 or 2019.2 (when upgrading to 2020.1)	• Medium Risk: *Privacy*

Alert	Products & Versions	Risk Rating
HS2022-01-14: System-wide and Facility-level Clinical Consent Policies Ignore Event Dates	• All versions of: ○ Information Exchange ○ Unified Care Record (through 2021.1)	• Low Risk: *Privacy*
HS2022-01-15: FHIR Requests Not Being Evaluated Properly for Consent	• Unified Care Record: ○ 2020.1	• High Risk: *Privacy*
HS2022-01-16: FHIR “$everything” Operation Can Return Unconsented Demographics	• All versions of: ○ Information Exchange ○ Unified Care Record (through 2021.1)	• Medium Risk: *Privacy*
HS2022-01-17: FHIR Index Performance Issue Can Cause ODS Instability	• Information Exchange: ○ 2018.1 • Unified Care Record: ○ 2019.1, 2019.2	• Very High Risk: *Operational*
HS2022-01-18: Security Vulnerability in FHIR Gateway/FHIR Server	• Unified Care Record: ○ 2021.1 • InterSystems IRIS for Health: ○ 2021.1	• Medium Risk *Security*
HS2022-01-19: FHIR Server Does Not Verify Token Revocation	• Unified Care Record: ○ 2020.1, 2020.2, 2021.1 • InterSystems IRIS for Health: ○ 2020.4, 2021.1 • HealthShare Health Connect: ○ 2020.4, 2021.1	• Medium Risk: *Security*
HS2022-01-20: OAuth Token Scope Not Applied in FHIR Batch Transaction Bundles	• InterSystems IRIS for Health: ○ 2021.1	• Medium Risk: *Privacy* • Low Risk: *Security* • Medium Risk: *Operational*
HS2022-01-21: FHIR Server Interoperability REST Client does not Properly Clean Up Data	• InterSystems IRIS for Health: ○ 2020.2, 2020.3 • HealthShare Health Connect: ○ 2020.2, 2020.3	• High Risk: *Operational*
HS2022-01-22: Security Issue in Patient Index	• All versions of: ○ Patient Index (through 2021.2)	• Medium Risk *Security*

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

HS2022-01-01: Vaccination Dates Misrepresented in Some Circumstances

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Information Exchange, Unified Care Record, Personal Community, and Health Connect. InterSystems IRIS for Health.
Versions:	All versions
System areas affected:	Data Transformations, Data Transmission, Personal Community, Health Insight, Clinical Viewer
Reference:	HSIEC-5565

Summary of Issue

InterSystems has identified a clinical safety and operational data integrity issue in which the dates associated with vaccination events are misrepresented in some circumstances.

In the HealthShare SDA data model, there is a date associated with a *vaccination order* and a date associated with a *vaccination administration*. The vaccination administration date is the most clinically significant, as it indicates when a patient received a vaccine. The vaccination order date may represent either when the order was entered or when the vaccine is ordered to be administered. The clinical safety issue is that sometimes the vaccination order date is presented or transmitted as if it is the vaccination administration date.

The issue in this alert affects how vaccination dates are represented in HealthShare and in data exports from HealthShare, Health Connect, and InterSystems IRIS for Health.

Due to the complexity of how data import and export transformations interact, the outcome may vary based on the source data, as shown in the table below:

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.

Source	***HealthShare Component***			***Data Export in HealthShare, Health Connect, and InterSystems IRIS for Health***	
Data Format	**Clinical Viewer**	**Personal Community**	**Health Insight**	**Outbound CDA/CCDA Data Transformations**	**Outbound FHIR Data Transformations (STU3 and R4)**
CDA or C-CDA document	Correctly displays *administration date*	Correctly displays *administration date*	• *Order date* property incorrectly contains *administration date* • *Administration date* property is empty	Correctly uses *administration date*	Correctly uses *administration date*
FHIR R4 resource	Correctly displays *administration date*	Correctly displays *administration date*	• *Order date* property incorrectly contains *administration date* • *Administration date* property is empty	Correctly uses *administration date*	Correctly uses *administration date*
FHIR STU3 resource	Date is not displayed	Correctly displays *administration date*	• *Order date* property incorrectly contains *administration date* • *Administration date* property is empty	Correctly uses *administration date*	Date is not populated
HL7 v2 message	Incorrectly displays *order date* as *administration date*	Incorrectly displays *order date* as *administration date*	All properties are correct	Incorrectly uses *order date* as *administration date*	Incorrectly uses *order date* as *administration date*

Custom data transformations may also be impacted, depending on how the source data is mapped to the SDA data model and how SDA data is mapped to target outbound schemas.

All HealthShare customers that ingest and use vaccination data are impacted. Health Connect and InterSystems IRIS for Health customers are impacted if their system receives vaccination data from CDA/C-CDA documents, FHIR resources, or HL7 v2 messages AND transforms the data into SDA using InterSystems' base data transformations.

This issue has been identified as a clinical safety risk because vaccination dates are used in clinical decision making. As a result of this issue, the *vaccination administration date* in HealthShare:

- may be prior to the actual date the patient received the vaccination
- may represent a vaccination order that was never filled
- may be absent

While the clinical safety rating for this issue is lower than that for which InterSystems typically distributes alerts, we are applying discretion in issuing this alert due to the high importance and visibility of vaccination data at this time.

The issue has also been identified as an operational data integrity issue as the meaning of the vaccination date data within the HealthShare system will differ depending on the data source format.

InterSystems is issuing this as an immediate alert while development work is ongoing. A correction is not yet available for this issue. InterSystems will distribute updates to this alert when a correction or remediation is available. Further details for this issue appear in the Technical Addendum for HS2022-01-01.

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

Recommended Action

InterSystems recommends immediately taking the following actions for the relevant products:

Unified Care Record:

- Inform your users and the recipients of your outbound data that *vaccination date* information should not be relied upon for clinical decision making.

Health Connect / InterSystems IRIS for Health:

- If your incoming feeds contain vaccination data and you transform that data into SDA, inform your users and the recipients of your outbound data that *vaccination date* information should not be relied upon for clinical decision making.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-01”.

– Additional details for this issue appear in the Technical Addendum below –

Technical Addendum for HS2022-01-01

Description of Issue

Dates associated with *vaccination orders* are represented in SDA in the following properties:

- `Vaccination.FromTime`
- `Vaccination.ToTime`
- `Vaccination.EnteredOn`
- `Vaccination.UpdatedOn`

Dates associated with *vaccination administrations* are represented in SDA in the following properties:

- `Vaccination.Administrations.Administration.FromTime`
- `Vaccination.Administrations.Administration.ToTime`
- `Vaccination.Administrations.Administration.EnteredOn`
- `Vaccination.Administrations.Administration.UpdatedOn`

The *vaccination administration dates* are more clinically relevant as they represent when the patient received a vaccine. *Vaccination order dates* may represent either when the order was entered or when the order specifies that it should be fulfilled.

InterSystems has identified the following issues with import and export transformations:

- *Vaccination administration dates* are inappropriately mapped to and from `Vaccination.FromTime` or `Vaccination.EnteredOn`, which are intended for *vaccination order dates*.
- `Vaccination.Administrations.Administration.FromTime` is not populated even though there is a *vaccination administration date* in the inbound data.

Additionally, the Clinical Viewer and Personal Community both display the order date data stored in `Vaccination.FromTime` when they should display the vaccination administration data stored in `Vaccination.Administrations.Administration.FromTime`.

The sections below provide additional details, and the master table at the end of the document shows how these mappings interact.

HL7 v2 Transformation

This transformation correctly maps between the HL7 v2 VXU_V04 segments and the SDA3 Vaccination order and administration properties as follows.

ORC is the segment representing the order and RXA is the segment representing the vaccination administration:

HL7v2	SDA3
ORC-7.4.1 Start Date/Time	`Vaccination.FromTime`
ORC-7.5.1 End Date/Time	`Vaccination.ToTime`
ORC-9.1 Date/Time of Transaction	`Vaccination.EnteredOn`
RXA-3.1 Date/Time Start of Administration	`Vaccination.Administrations.Administration.FromTime`
RXA-4.1 Date/Time End of Administration	`Vaccination.Administrations.Administration.ToTime`
RXA-22.1 System Entry Date/Time	`Vaccination.Administrations.Administration.EnteredOn`

CDA C32 Transformations

This transformation *incorrectly* maps the administration times to the SDA3 Vaccination order properties as follows:

CDA C32 In	/entry/substanceAdministration/effectiveTime[@xsi:type='IVL_TS']/low/@value
SDA3	`Vaccination.FromTime`
CDA C32 Out	/entry/substanceAdministration/effectiveTime/@value

CDA C32 In	/entry/substanceAdministration/author/time/@value or /entry/substanceAdministration/entryRelationship[@typeCode='REFR']/supply[@moodCode='EVN']/author/time/value
SDA3	`Vaccination.EnteredOn`
CDA C32 Out	if no `Vaccination.FromTime`, then use `Vaccination.EnteredOn` for: /entry/substanceAdministration/effectiveTime/@value

CCDA 1.1 and CCDA 2.1 Transformations

This transform *incorrectly* maps the administration times to the SDA3 Vaccination order properties as follows:

CCDA 1.1 and CCDA 21. In	/entry/substanceAdministration/effectiveTime/@value or /entry/substanceAdministration/effectiveTime[@xsi:type='IVL_TS']/low/@value
SDA3	`Vaccination.FromTime`
CCDA 1.1 and CCDA 21. Out	/entry/substanceAdministration/effectiveTime/@value

CCDA 1.1 and CCDA 21. In	/entry/substanceAdministration/effectiveTime[@xsi:type='IVL_TS']/high/@value
SDA3	`Vaccination.ToTime`
CCDA 1.1 and CCDA 21. Out	if no `Vaccination.FromTime`, then use `Vaccination.EnteredOn` for: /entry/substanceAdministration/effectiveTime/@value

FHIR R4 Import Transformation

This transformation *incorrectly* maps the administration time to the SDA3 Vaccination order property as follows:

FHIR R4 In	SDA3	FHIR R4 Out
Immunization.occurrenceDateTime	`Vaccination.FromTime`	Immunization.occurrenceDateTime

FHIR STU3 Import Transformation

This transformation *incorrectly* maps the administration time to the SDA3 Vaccination order properties as follows:

FHIR STU3 In	SDA3	FHIR STU3 Out
Immunization.date	`Vaccination.EnteredOn`	
	`Vaccination.FromTime`	Immunization.date

Display in Clinical Viewer

On the Immunization chart the *Start Date* field displays the value in `Vaccination.FromTime`. On the Details screen, the *Administration Details Start Date* field displays the value in `Vaccination.FromTime` . Based on the data model, these should be `Vaccination.Administrations.Administration.FromTime` .

However, whether the value displayed to the user is incorrect depends upon the data source:

- When the source of this data is HL7 v2, then the value displayed is the *vaccination order date* (incorrect value displayed)
- When the source of this data is CDA/C-CDA or FHIR R4, then the value displayed is the *vaccination administration date* (correct value displayed)

Display in Personal Community

The *My Immunizations* section, *Details* screen, and the *Share My Records* printout from Personal Community display the SDA order times associated with a vaccination in the *Date* field. These *Date* fields are populated from SDA3 in order of preference as follows:

```
1.     Vaccination.FromTime
2.     Vaccination.EnteredOn
3.     Vaccination.UpdatedOn
```

Based on the data model, the *Date* field should be populated by `Vaccination.Administrations.Administration.FromTime` .

However, whether the value displayed to the user is incorrect depends upon the data source:

- When the source of this data is HL7 v2, then the value displayed is the *vaccination order date.* The incorrect value is displayed because the source mapping was correct.
- When the source of this data is CDA/C-CDA or FHIR R4, then the value displayed is the *vaccination administration date.* In this case, the correct value is displayed because the source mapping was also incorrect.

HTML Patient Reports

The Patient Summary Report (Classic) and Patient Summary Report (Expanded) HTML reports display `Vaccination.FromTime` in the *Immunization Date* field. Based on the data model, the *Immunization Date* field should be populated by `Vaccination.Administrations.Administration.FromTime` .

However, whether the value displayed is incorrect depends upon the data source:

- When the source of this data is HL7 v2, then the value displayed is the *vaccination order date.* The incorrect value is displayed because the source mapping was correct.
- When the source of this data is CDA/C-CDA or FHIR R4, then the value displayed is the *vaccination administration date.* In this case, the correct value is displayed because the source mapping was also incorrect.

Health Insight

While the mappings from SDA to Health Insight are correct, Health Insight properties will be incorrect when the source data was mapped incorrectly into SDA as follows:

Source Data Format	Health Insight
CDA/C-CDA document	• The *administration date* populates the `HSAA.Vaccination:FromDate` property that is intended for *order date* • The *administration date* property, `HSAA.MedicationAdministration:FromTime`, does not get populated
FHIR R4 resource	• The *administration date* populates the `HSAA.Vaccination:FromDate` property that is intended for *order date* • The *administration date* property, `HSAA.MedicationAdministration:FromTime`, does not get populated
FHIR STU3 resource	• The *administration date* populates the `HSAA.Vaccination:EnteredOn` property that is intended for *order date* • The *administration date* property, `HSAA.MedicationAdministration:FromTime`, does not get populated
HL7 v2 message	• The *administration date* correctly populates the `HSAA.MedicationAdministration:FromTime` property • The *order date* correctly populates the *order date* properties (`HSAA.Vaccination`...)

Other HealthShare Components

There are no known mapping issues from SDA to other HealthShare components, but they are subject to the original incorrect mapping from the source data into SDA.

Master Routing Table

The table below illustrates all of the routes that inbound data map into the SDA and all of the downstream and outbound routes where that SDA data is used.

To accommodate page size limitations, the table displays an abbreviation of the clinical meaning of the data element, rather than the exact name or path of the data element. The exact name and paths are detailed in the tables above.

KEY:

Term	Meaning
Admin date	Administration date, single date
Admin date - *From*	Administration date, lower end of the date range
Admin date - *To*	Administration date, upper end of the date range
Admin date - *Entered*	Date the administration was entered in the system
Order date	Order date, single date
Order date - *From*	Order date, lower end of the date range
Order date - *To*	Order date, upper end of the date range
Order date - *Entered*	Date the order was entered in the system

Term	Meaning
Order date - *Updated*	Date the order was updated in the system
secondary, tertiary preference	Indicates that this mapping is secondary or tertiary in order of preference and will only be populated if a preferred property is not available

Inbound Transformations					***Storage***	***Downstream HealthShare Components***			***Outbound Transformations***		
FHIR STU3	**FHIR R4**	**CDA C32**	**CCDA 1.1 and 2.1**	**HL7v2 VXU_V04**	**SDA**	**Clinical Viewer**	**Personal Community**	**Health Insight**	**CDA C32, CCDA 1.1 and CCDA 2.1**	**FHIR R4**	**FHIR STU3**
				Admin date - *From*	**Admin date - *From***			Admin date - *From*			
				Admin date - *To*	**Admin date - *To***			Admin date -*To*			
				Admin date - *Entered*	**Admin date - *Entered***			Admin date - *Entered*			
	Admin date	Admin date	Admin date Admin date - *From*	Order date - *From*	**Order date - *From***	Admin date	Admin date	Order date - *From*	Admin date	Admin date	Admin date
			Admin date - *To*	Order date -*To*	**Order date - *To***			Order date - *To*			
Admin date				Order date - *Entered*	**Order date - *Entered***		Admin date, secondary preference	Order date - *Entered*	Admin date, secondary preference		
					Order date - *Updated*		Admin date, tertiary preference	Order date - *Updated*			

Recommended Action

How to Determine Whether Necessary Conditions are Present

1. Review your use of the data transformations and HealthShare components listed above.
2. Review whether your system uses custom transformations for vaccination data. Within any such custom transformations, identify the mappings between the source data and the SDA target properties. Review the

outbound data transformations and HealthShare components listed above to determine how that data is transmitted throughout and from HealthShare.

Steps to take if these Conditions are Present

InterSystems is issuing this as an immediate alert while development work is ongoing. Corrections are not yet available for this issue. InterSystems will distribute alert updates when the corrections are available or if there is additional information to communicate. Monitor InterSystems alerts for this information.

While development work is ongoing, HealthShare recommends immediately taking the following actions for the relevant products:

Unified Care Record:

- Inform your users and the recipients of your outbound data that vaccination date information should not be relied upon for clinical decision making.

Health Connect / InterSystems IRIS for Health:

- If your incoming feeds contain vaccination data and you transform that data into SDA, inform your users and the recipients of your outbound data that vaccination date information should not be relied upon for clinical decision making.

Information about the Correction

This defect is identified as HSIEC-5565.

Corrections are in development but not yet available. InterSystems anticipating issuing one set of corrections to cover:

- Inbound and outbound CDA, CCDA, and FHIR transformations
- Clinical Viewer
- Personal Community
- HTML Patient Reports

Along with these corrections, InterSystems will issue a utility to reprocess previously received CDA documents that contain vaccination data, if those documents are stored in one or more document repositories.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-01".

End of Alert HS022-01-01

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.

HS2022-01-02: Invalid Handling of Multiple Reference Ranges in CDA and C-CDA Documents

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Information Exchange and Unified Care Record
Versions:	All versions (through 2021.1)
System areas affected:	Data Transformations, Clinical Viewer, Data Transmission
Reference:	HSIEC-4549

Summary of Issue

InterSystems has identified a patient safety issue that occurs when laboratory results in CDA and C-CDA documents contain multiple reference ranges. Unified Care Record stores only a single reference range to represent a Lab Result Item Normal Range. For each affected result entry, the data transformations store only the last reference range in the list. This may not be the range representing the normal range for the result. For example, if the result entry lists three reference ranges in the following order of *Normal*, *Low*, and *High*, Unified Care Record records only the *High* reference range.

The system displays references ranges in the Clinical Viewer and uses them to compute *Flag* values in the Clinical Viewer in some circumstances when an interpretation is not available from the source document. This can cause *Flag* to be incorrect and could lead to users to fail to identify abnormal laboratory results or to improperly interpret results.

Full details of the identified issue appear in the Technical Addendum for HS2022-01-02.

Risk Assessment

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

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

Recommended Action

InterSystems recommends that customer organizations apply the correction for this defect. It is identified as HSIEC-4549 and is available via ad hoc distribution from the InterSystems Worldwide Response Center (WRC). This correction will also be included in all future product releases, beginning with HealthShare 2021.2.

InterSystems is also providing utilities to repair previously processed CDA documents. The utilities are identified as HSIEC-4614. These utilities require that customers have maintained their documents in one or more repositories.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-02".

– Additional details for this issue appear in the Technical Addendum below –

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 HS2022-01-02

Description of Issue

InterSystems has identified a patient safety issue that occurs when laboratory results in CDA and C-CDA documents contain multiple reference ranges. Unified Care Record only stores a single reference range in the *ResultNormalRange* property of the LabResultItem streamlet. For each affected result entry, the data transformations will store whichever reference range is last in the list. This may not be the range representing the normal range for the result.

For example, the following CCDA entry lists three reference ranges:

```
<entry>
...
   <code xmlns="urn:hl7-org:v3" code="24113" codeSystem="2.16.840.1.113883.6.1"
   codeSystemName="LOINC" displayName="ALBUMIN">

   </code>

...
   <value xsi:type="PQ" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" value="4.0"
   unit="g/dL">

   </value>

   <interpretationCode code="N" codeSystem="2.16.840.1.113883.5.83"
   codeSystemName="Observation Interpretation (HL7)" displayName="Normal">

   </interpretationCode>

...
   <referenceRange>

   <observationRange>

   <value xsi:type="IVL_PQ" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <low value="3.2" unit="g/dL">

   </low>

   <high value="5.5" unit="g/dL">

   </high>

   </value>

   <interpretationCode code="N" codeSystem="2.16.840.1.113883.5.83"
   codeSystemName="ObservationInterpretation" displayName="Normal">

   </interpretationCode>

   </observationRange>

   </referenceRange>

   <referenceRange>

   <observationRange>

   <value xsi:type="IVL_PQ" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <high value="3.2" unit="g/dL">

   </high>

   </value>

   <interpretationCode code="L" codeSystem="2.16.840.1.113883.5.83"
   codeSystemName="ObservationInterpretation" displayName="Low">

   </interpretationCode>

   </observationRange>
```

```
     </referenceRange>

     <referenceRange>

     <observationRange>

     <value xsi:type="IVL_PQ" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

     <low value="5.5" unit="g/dL">

     </low>

     </value>

     <interpretationCode code="H" codeSystem="2.16.840.1.113883.5.83"
     codeSystemName="ObservationInterpretation" displayName="High">

     </interpretationCode>

     </observationRange>

     </referenceRange>

  ...
```

Unified Care Record records the final reference range listed. In the example above, this would be the *High* reference range and the value stored in *LabResultItem.ResultNormalRange* would be ">=5.5" when the true normal range is "3.2-5.5".

The Clinical Viewer displays references ranges in the **Lab Results Table** and in other lab result views and uses them to compute *Flag* values if the *interpretationCode* value is not present in the source document. This can cause *Flag* to be incorrect and could lead a user to fail to identify abnormal laboratory results or to improperly interpret results. In the example above where the value of the lab result is "4.0", the lab result would be incorrectly flagged as *Low* if the *interpretationCode* element was not present.

Additional Information

If an *interpretationCode* is present in the document, that value determines the following behavior in the Clinical Viewer lab result views. If an *interpretationCode* 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.

This defect impacts all customers who process lab results from CDA or C-CDA documents.

Recommended Action

InterSystems recommends that customers apply the correction for this defect. It is identified as HSIEC-4549 and is available via ad hoc distribution from the InterSystems Worldwide Response Center (WRC). It will also be included in all future product releases, beginning with HealthShare 2021.2.

The correction consists of a set of new XSLT files. If there is more than one reference range for a Result Entry, the code checks the *referenceRange/observationRange/interpretationCode/code* and only takes the value where */interpretationCode/code* = "N". If there is no *interpretation code/code*, no reference range will be ingested and *LabResult.ResultNormalRange* will be empty. If there is only one reference range for a Result Entry, that value will be ingested regardless of whether or not *interpretationCode/code* is present.

InterSystems is also providing utilities to repair previously processed CDA documents. The utilities are identified as HSIEC-4614. These utilities require that customers have maintained their documents in one or more repositories.

There are two utilities:

1. The **Census Utility** conducts a comprehensive scan of all records affected by this issue and provides a list of MRNs that will be processed by the Repair Utility.
2. The **Repair Utility** queues the MRNs provided by the Census Utility for reprocessing by the ECR Query Task. The ECR Query Task finds and reprocesses these MRNs during its next scheduled run.

Please contact InterSystems' Worldwide Response Center (WRC) with any questions or for additional information.

Information about the Correction

This defect is identified as HSIEC-4549. The utilities are identified as HSIEC-4614. If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-02".

End of Alert HS022-01-02

HS2022-01-03: Security Check for Emergency Access to Patient Records Fails to Occur in Some Situations

Issue date: 1-MAR-2022

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:	All versions (through 2020.2)
System areas affected:	Clinical Viewer, Consent
Reference:	HSIEC-4145

Summary of Issue

InterSystems has corrected a patient privacy issue caused by situations where the security check fails to occur for emergency access to patient records. Emergency access is also known as “break the glass” or “overriding consent.”

The issue can result in users being able to inappropriately override consent if they are permitted to search and view patient records but are restricted from overridding consent by using emergency access.

This issue only occurs if both the following criteria are met:

1. The system is configured to enable emergency access functionality.
2. One or more user roles is permitted to search and view patient records but is not permitted to override consent with emergency access.

This issue does not grant any access to unauthorized users or affect users whose roles permit emergency access.

Full details of the identified issue appear in the Technical Addendum for HS2022-01-03.

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 Action

InterSystems recommends that all customers who permit emergency access take the following actions:

1. Apply the correction for this defect. The correction is identified as HSIEC-4145 and is available via ad hoc distribution from the InterSystems Worldwide Response Center (WRC). It will also be included in all future product releases, beginning with HealthShare 2021.1.
2. Review the Emergency Access Log to check for cases of inappropriate emergency access as described in the technical addendum.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-03”.

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 HS2022-01-03

Description of Issue

InterSystems has corrected a patient privacy issue caused by situations where the security check fails to occur for emergency access to patient records. The issue can result in users being able to inappropriately override consent if their user roles allow them to search for and view patient records but not to override consent by using emergency access. If such a user does override consent, this event *will be logged* in the Emergency Access Log.

This issue does not grant any access to unauthorized users or affect users whose roles permit emergency access.

This issue occurs only if *both* the following criteria are met. Customers should verify whether their system is configured as described below:

1. The system is configured to enable emergency access — "Allow Override Consent Policy" is selected in the consent registry for system-level MPI consent.
2. One or more user roles has permission to search and view patient records, but does not have permission to invoke emergency access:
    a. User role *has* permissions for these resources: `%HS_PatientSearch`, `%HS_PatientRetrieval`
    b. User role has *does not have* permissions for this resource: `%HS_EmergencyAccess`

Among the set of roles provided by default in Unified Care Record, `%HS_Nurse` and `%HS_Clerical` have the combination of permissions described above.

Because the default `%HS_Clinician` role is granted `%HS_EmergencyAccess`, it is *not affected* by this issue.

To determine which default roles are in use in your system and also whether any custom roles are in use that may be affected, review the list of roles in your system by navigating to **Home > System Administration > Security Management > Roles**. Select each role and view the **General** tab to see which privilege resources are granted.

Recommended Action

InterSystems recommends that all customers who enable emergency access take the following actions:

1. Apply the correction for this defect.
2. Review the Emergency Access Log to check for cases of inappropriate emergency access. The Emergency Access Log may be accessed via **Home > HealthShare > HSREGISTRY > Report Management > Run Management Reports > Select Report: Emergency Access Log**. Enter a *From Date* and *Thru Date* and select the *Format* in which to view the results.

Please contact InterSystems' Worldwide Response Center (WRC) with any questions or for additional information.

Information about the Correction

The correction for this defect is identified as HSIEC-4145 and is available as an ad hoc patch or full kit distribution from the InterSystems Worldwide Response Center (WRC). It will also be included in all future product releases, beginning with HealthShare 2021.1.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-03".

End of Alert HS022-01-03

HS2022-01-04: Security Vulnerability in Unified Care Record 2020.2.0

Issue date: 1-MAR-2022

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	High Risk CVSS: 7.7	Not Applicable

Version and System Area Affected

HealthShare® Products:	Unified Care Record
Versions:	Unified Care Record 2020.2.0, Build 8620
System areas affected:	Security
Reference:	HSIEO-3532

Summary of Issue

A security vulnerability has been found in the initial release of Unified Care Record 2020.2 which may allow a user with insufficient permissions to access resources on the system.

Risk Assessment

Security:	High Risk	CVSS: 7.7

Recommended Action

The initial release of Unified Care Record 2020.2.0 Build 8620 was removed from the WRC Distribution site in 2021. It was replaced by maintenance release 2020.2.1 Build 8624. If you have downloaded or installed version 2020.2, check whether you have Build 8620. If so, please download the maintenance kit or contact the WRC to request an ad hoc patch for HSIEO-3532.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-04".

End of Alert HS022-01-04

HS2022-01-05: Customers on Unified Care Record 2020.2 and 2021.1 Must Install a Patch Before Upgrading to a Later Version

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Unified Care Record, Clinical Viewer, Health Insight, Patient Index, Personal Community, Provider Directory, Care Community
Versions:	• 2020.2, 2021.1 for all products • For Provider Directory only, also versions 2021.2 and 2021.3
System areas affected:	Upgrades to later versions
Reference:	HSIEO-5568

Summary of Issue

Customers using either version 2020.2 or 2021.1 of HealthShare products must *install a patch* and *run a utility method* before they upgrade to version 2021.2 or any later version. A mismatch in a versioning global will prevent users from logging into the system after the upgrade if the utility method is not run on the system prior to the upgrade.

InterSystems strongly recommends that all customers who have installed these versions take this action now in order to prevent a problem later.

Risk Assessment

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

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

Recommended Action

All HealthShare Unified Care Record customers on version 2020.2 or 2021.1 should obtain the ad hoc patch for HSIEO-5568 and follow the instructions provided with the patch to run the *FixSystemSecurityVersion()* utility method on all of their HealthShare instances. If you do not run this utility prior to upgrading to a later version, all users will be locked out when you complete your upgrade.

While the kits for version 2020.2 and 2021.1 on the WRC download site have been replaced with a maintenance version that remediates this issue, customers who already have those versions installed must install the patch and run the utility.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-05".

End of Alert HS022-01-05

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.

HS2022-01-06: Configuring the Classic Clinical Viewer Requires Outdated Third-Party Software

Issue date: 1-MAR-2022

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	High Risk CVSS: 9.3	Not Applicable

Version and System Area Affected

HealthShare® Products:	Information Exchange and Unified Care Record
Versions:	All versions, when using Classic Clinical Viewer
System areas affected:	Classic Clinical Viewer, Layout Editor, DHTML Control
Reference:	HSCV-7178

Summary of Issue

The DHTML Editing Control and Internet Explorer are required to access the Layout Editor in order to configure the Classic Clinical Viewer. Internet Explorer is being deprecated by Microsoft. The DHTML Editing Control is no longer available from Microsoft. Customers who do not have copies in their internal systems will need to this access control from third party sites.

As this control and the browser are not considered secure, customers who need to use the Layout Editor should isolate any system where this software is installed as described in the Recommended Action section.

Risk Assessment

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

Security:	High Risk	CVSS: 9.3

Recommended Action

Create a VM and install Internet Explorer and the DHTML Editing Control. If the VM is on the same subnet as the Classic Clinical Viewer, update the network configuration on the VM to *not have* a default Gateway. This will block routing to any other subnet.

HealthShare continues to recommend customers migrate to the new Clinical Viewer.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-06".

End of Alert HS022-01-06

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.

HS2022-01-07: Users may not be able to Log Out of Clinical Viewer

Issue date: 1-MAR-2022

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	4-High 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, 2020.2
System areas affected:	Clinical Viewer
Reference:	HSCV-6780

Summary of Issue

User A logs into the Clinical Viewer on a shared system followed within minutes by **User B**. When **User B** clicks “Log Out”, the page may instead reload. Because **User B** was not logged out, another user may access the screen after **User B** departs. This occurs only on secure (https) connections with back-to-back logins by different users.

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 Action

To resolve this issue, access the TrakCare user interface:

1. Select **Tools > Technical Tools > Configuration Manager**
2. Locate *External Authentication Settings*

For IRIS-based HealthShare versions

Change the *External Authentication Logout URL* setting from:

```
/csp/healthshare/hsviewer/web/HS.UI.ClinicianPortalV2.Launch.cls
```

to:

```
/csp/healthshare/hsviewer/web/HS.UI.ClinicianPortalV2.Launch.cls?IRISLogout=end
```

For Cache-based HealthShare versions

Change the *External Authentication Logout URL* setting from:

```
/csp/healthshare/hsviewer/web/HS.UI.ClinicianPortalV2.Launch.cls
```

to:

```
csp/healthshare/hsviewer/web/HS.UI.ClinicianPortalV2.Launch.cls?CacheLogout=end
```

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-07”.

End of Alert HS022-01-07

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.

HS2022-01-08: Access Gateway Aggregation Cache Grows over Time

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	HealthShare Unified Care Record
Versions:	2020.1, 2020.2, 2021.1, and 2021.2
System areas affected:	Access Gateway
Reference:	HSIEO-5562

Summary of Issue

InterSystems has detected a system stability concern in HealthShare Unified Care Record systems that have been upgraded from version *2019.2 or earlier* to version *2020.1 or later*.

Streamlets in the aggregation cache of Access Gateway namespaces are not purged correctly during routine operation. This will cause the storage on the Access Gateway's server to grow slowly over time. If the server disk space becomes full, the system will stop. The streamlets are purged if the Access Gateway is reset.

- For customers who have upgraded and are impacted by this issue, a workaround is described below.
- For customers who are planning an upgrade, the relevant Terminal command is now detailed in the upgrade documentation for each affected version.

The fix for this issue will also be included in all future versions of HealthShare, beginning with HealthShare Unified Care Record 2022.1.

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

Recommended Action

For customers who have upgraded and are impacted by this issue, run the following Terminal command on each Access Gateway namespace. This will ensure that routine purging of the streamlets executes successfully:

```
k ^rINDEXEXT("F")

Do $System.OBJ.RebuildExtentIndex(0,1)
```

Routine monitoring of disk space helps to reduce the likelihood of encountering system stability issues. For information on monitoring disk space, see the HealthShare Monitoring and Operations Guide.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-08".

End of Alert HS022-01-08

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.

HS2022-01-09: Incompatibility in HL7toSDA3 Customizations when Upgrading from HealthShare 15.03 or earlier

Issue date: 1-MAR-2022

Risk Category and Score:

As this issue involves overriding standard code with custom code, it did not receive a risk score.

Version and System Area Affected

HealthShare® Products:	Information Exchange
Versions:	Upgrades from Information Exchange 15.03 or earlier to a later version of Information Exchange or Unified Care Record
System areas affected:	Data Transformations
Reference:	HSIEC-4291

Summary of Issue

HealthShare transforms patient data that it receives into an internal data format called SDA (Summary Document Architecture). Customers may extend or modify the standard transformations to fit their needs.

InterSystems has received reports of an incompatibility between *custom* and *standard* HL7 to SDA transformations that may cause the custom transformation to mix data from separate HL7 v2 messages. This may result in error messages that cause HL7 v2 messages to fail to save correctly or result in data being stored incorrectly. The exact results of this issue depend on the details of the custom transformation.

This issue is caused by a change to a method in the standard transformation that occurred in version 2018.1 of Information Exchange. InterSystems recommends that customers review their custom code against standard transformations for any differences when they perform an upgrade. Customers should also thoroughly test all functionality impacted by custom code at each upgrade.

Full details of the identified issue appear in the Technical Addendum for HS2022-01-09.

Risk Assessment

As this issue involves overriding standard code with custom code, it did not receive a risk score.

Recommended Action

InterSystems strongly recommends that customers who have upgraded or are planning an upgrade from HealthShare Information Exchange 15.03 review their custom *HS.Gateway.HL7.HL7ToSDA3* class to determine if they are affected by this issue and update the class if needed.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-08".

– Additional details for this issue appear in the Technical Addendum below –

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 HS2022-01-09

Description of Issue

In HealthShare Information Exchange 15.03 and earlier, the *GetSDA()* class method in *HS.Gateway.HL7.HL7ToSDA3* referenced a global named `^||d`. This global was renamed to `^||HS.Data` in version 2018.1 of Information Exchange (and in all versions of Unified Care Record).

Customers who copied the *HS.Gateway.HL7.HL7ToSDA3* class to create a custom class may still be attempting to reference the `^||d` global and therefore will not kill the `^||HS.Data` global when needed. As a result, `^||HS.Data` may contain data from both the current HL7 message and previous HL7 messages. This can trigger error messages that cause HL7 v2 messages to fail to save correctly or may result in data being stored incorrectly. The exact results of this issue depend on the details of the custom transformation. Affected customers are encouraged to test their transformations to determine how they are impacted by this issue.

This issue only impacts customers who meet the following criteria:

- Have upgraded or are planning an upgrade from HealthShare Information Exchange 15.03 or earlier to a later version of HealthShare Information Exchange or Unified Care Record.
- Implemented a custom transformation of the *HS.Gateway.HL7.HL7ToSDA3* class by copying the class.
- Did not review the changes made to the *HS.Gateway.HL7.HL7ToSDA3* class when upgrading and did not update the global name from the `^||d` to `^||HS.Data`.

Recommended Action

InterSystems recommends that customers who have upgraded or are planning an upgrade from HealthShare Information Exchange 15.03 review their custom *HS.Gateway.HL7.HL7ToSDA3* class to determine if `^||d` is used and update all instances to `^||HS.Data`.

As a general principle, InterSystems recommends that customers always review their custom code against standard transformations for any differences when they perform an upgrade. Customers should also ensure they thoroughly test all functionality impacted by custom code at each upgrade.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-09”.

End of Alert HS022-01-09

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.

HS2022-01-10: IHE Endpoints should use Appropriate Credentials

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Information Exchange and Unified Care Record
Versions:	All versions
System areas affected:	IHE Endpoints (PIX, PDQ, XDS.b, XCPD, XCA, DSUB)
Reference:	HSIEO-4036

Summary of Issue

When you configure an IHE endpoint, you must provide third parties with credentials so they can access that endpoint.

The user credential for your IHE endpoints should:

- include a resource specific to IHE transactions and include no other resources.
- not be the same credential used for other purposes in your HealthShare system, such as the "HS_Services" credential used to access API endpoints.

User credentials that provide access to a broader range of resources than are required to complete IHE transactions present a potential security vulnerability.

Complete details on how to identify if your IHE credentials are secure and how to remediate the issue if they are not, appear in the Technical Addendum for HS2022-01-10.

Risk Assessment

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

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

Recommended Action

If you are using IHE and any of the following are true about your endpoint credentials, then follow the instructions in the Technical Addendum for HS2022-01-10 to remediate the issue:

- The IHE credential is the HS_Services user and password.
- The IHE credential is a custom user that has the `%HS_WebServices` resource.
- The IHE credential is a custom user with no resources.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-10".

– Additional details for this issue appear in the Technical Addendum below –

Technical Addendum for HS2022-01-10

Description of Issue

In order to provide third parties with access to IHE endpoints in a secure manner, you should:

1. Create a resource specific to IHE.
2. Require that resource in order to access your IHE endpoints.
3. Create a user and password that has privileges only for that resource, and distribute those credentials to third parties.

You *should not* distribute to third parties the credential for the HS_Services user or any other user that has privileges for the `%HS_WebServices` resource.

If any of the following are true about the IHE credentials that you have distributed to third parties:

- The IHE credential is the HS_Services user and password
- The IHE credential is a custom user that has privileges for the `%HS_WebServices` resource
- The IHE credential is a custom user with no resource privileges

then follow the instructions below to create new a new resource and credentials that you can safely distribute to third parties.

Creating a New Resource, Role, and User for IHE

Follow the steps below to secure your IHE endpoints:

1. Create a new resource that is specific to IHE endpoints, for example `%HS_IHEWebServices`.
2. Create a new role, for example, `%HS_IHEServices`.
3. Add privileges for the `%HS_IHEWebServices` resource to the `%HS_IHEServices` role.
4. Create a new IRIS user, for example “HS_IHEServices”, and add that user to the `%HS_IHEServices` role.
5. Modify each public-facing IHE endpoint to require the new `%HS_IHEWebServices` resource by setting it as the *ResourceRequired* in each IHE production web service business host.
6. Distribute the new credentials to any third-party systems that require access your IHE endpoints.

For a list of potential IHE endpoint names, see the section “Securing IHE Endpoints” in the “Setting Up Unified Care Record to Use IHE” chapter of the book *Setting Up Unified Care Record*.

Changing the HS_Services Password, if necessary

Once you have properly secured your IHE endpoints, if you previously distributed the HS_Services password to third parties, change the HS_Services password as described in the section “Change HS_Services Password” in the “Things to Check Before you Deploy” chapter of *Roadmap to Implementing Unified Care Record*.

Modifying Existing IHE User Credentials

- If the credential that you previously distributed was a custom user with privileges for the `%HS_WebServices` resource, modify that user to have the new IHE-specific role you created above, and remove the role that granted them the `%HS_WebServices` resource.
- If the credential that you previously distributed was a custom user with no resource privileges, modify that user to have the new IHE-specific role you created above.

Recommended Action

Follow the instructions above to remediate the issue.

Please contact InterSystems’ Worldwide Response Center (WRC) with any questions or for additional information.

End of Alert HS022-01-10

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.

HS2022-01-11: ODS Namespace Reactivation Can Result in Prolonged Downtime

Issue date: 1-MAR-2022

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
1-Very Low Risk	Not Applicable	Not Applicable	4-High Risk

Version and System Area Affected

HealthShare® Products:	Unified Care Record
Versions:	2019.1, 2019.2
System areas affected:	ODS, FHIR Gateway
Reference:	IF-1028 (HSIEC-6189)

Summary of Issue

This issue impacts only customers who meet all of the following criteria:

- You are using version 2019.1 or 2019.2 of Unified Care Record.
- You have deployed the Operational Data Store (ODS) component.
- You have enabled a FHIR Gateway endpoint on the ODS.

You can experience a prolonged downtime if you reactivate an existing ODS namespace.

In versions 2019.1 and 2019.2, the activation task erroneously re-indexes the FHIR resources on the server. For customers with a large set of FHIR resources on the ODS, this can take a significant amount of time. While this re-indexing is occurring, the ODS will be offline. If you do start a reactivation, *you must wait for the process to complete*.

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:	1-Very Low Risk	Severity of typical adverse outcome = 2 out of 5 Likelihood of typical adverse outcome = 1 out of 5
Operational:	4-High Risk	Severity of typical adverse outcome = 5 out of 5 Likelihood of typical adverse outcome = 2 out of 5

Recommended Action

Two options are available to resolve this issue:

1. Apply the ad hoc patch for IF-1028 (HSIEC-6189) and follow the instructions provided by the WRC.
2. If you are on version 2019.1, you may upgrade the ODS to Version 2020.2. The ODS component can be upgraded without upgrading the entire Unified Care Record system. Please contact the WRC for instructions on how to use a 2020.2 ODS with version 2019.1 of Unified Care Record.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-11".

End of Alert HS022-01-11

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.

HS2022-01-12: Upgrade of ODS may Require Manual Intervention to Complete

Issue date: 1-MAR-2022

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:	Upgrades from version 2020.1 to version 2020.2
System areas affected:	Upgrades, ODS
Reference:	IF-1770 (HSIEC-6166)

Summary of Issue

If a 2020.1 Operational Data Store (ODS) had a FHIR endpoint that was later decommissioned, it will fail to properly upgrade to version 2020.2. During the upgrade, the system will be left in a state that requires manual intervention before the upgrade can succeed.

Because this issue will lead to extended system downtime during an upgrade, it presents an operational risk.

This issue has been fixed in versions 2021.1 and later. An ad hoc patch is available for upgrades to version 2020.2.

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 Action

ODS customers on version 2020.1 who plan to upgrade to 2020.2 should obtain and apply an ad hoc patch for IF-1770 (HSIEC-6166) prior to performing the upgrade.

If a customer has upgraded and encounters a system stuck mid-transaction, they should WRC to obtain manual recovery steps, and then obtain the ad hoc patch before upgrading again.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-12".

End of Alert HS022-01-12

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.

HS2022-01-13: ODS Audit Data Inaccessible after Upgrade to Version 2020.1

Issue date: 1-MAR-2022

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:	Unified Care Record
Versions:	• Upgrades from 2019.1 to version 2020.1 • Upgrades from 2019.2 to version 2020.1
System areas affected:	Upgrades, ODS
Reference:	IF-1320 (HSIEC-6248, IF-1219)

Summary of Issue

This issue impacts customers who have upgraded from Unified Care Record 2019.1 or 2019.2 to version 2020.1 and use the Operational Data Store (ODS).

In the upgrade, audit data for user access events was not properly migrated to a new storage location in the ODS. While no data is lost, existing ODS user access event audit data is inaccessible until the issue is fixed, making it difficult to report on user access events for patient data in the ODS from before the upgrade.

Full details of the identified issue appear in the Technical Addendum for HS2022-01-13.

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 = 1 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Action

- If you upgraded from version 2019.1 or 2019.2 to version 2020.1, request and apply the correction, IF-1219, from the WRC, and follow the ad hoc instructions.
- If you are planning to upgrade from 2019.1 or 2019.2 of Unified Care Record, upgrade to a version later than 2020.1 in order to avoid the issue.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-13".

– Additional details for this issue appear in the Technical Addendum below –

Technical Addendum for HS2022-01-13

Description of Issue

Some audit data related to user access events was not properly migrated to a new storage location in the upgrade steps from Version 2019.1 and 2019.2 of the Operational Data Store (ODS) to version 2020.1. While no data is lost, this audit data is inaccessible until the issue is fixed, making it difficult to report on user access events for patient data in the ODS from before the upgrade.

In version 2020.1 of the ODS, the global `^HS.Flash.AccTS` was renamed to `^HS.ODS.AccTS`. This global is responsible for helping track when to purge data from the ODS and is also used to audit the data that was sent to requesting systems. While this issue may temporarily prevent the ODS from purging some data, this is not considered an operational risk.

The old global is still present after the upgrade and all new data is written to the correct global. No data is lost as a result of this issue, but audit reports and purging will not work for the data referred to by the old global until the data is migrated. The correction correctly maps the data.

Recommended Action

- If you upgraded from version 2019.1 or 2019.2 to version 2020.1, request and apply the correction, IF-1219, from the WRC, and follow the ad hoc instructions.
- If you are planning to upgrade from 2019.1 or 2019.2 of Unified Care Record, upgrade to a version later than 2020.1 in order to avoid the issue.

Please contact InterSystems' Worldwide Response Center (WRC) with any questions or for additional information.

Information about the Correction

The correction IF-1219 will be included in all future releases and is available as an ad hoc distribution from the Worldwide Response Center (WRC).]

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-13".

End of Alert HS022-01-13

HS2022-01-14: System-wide and Facility-level Clinical Consent Policies Ignore Event Dates

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Information Exchange and Unified Care Record
Versions:	All versions (through 2021.1)
System areas affected:	Consent
Reference:	HSIEC-5062

Summary of Issue

There are two kinds of consent policies in Unified Care Record:

- *MPI Consent* - These policies determine whether a patient appears in the search results.
- *Clinical Consent* - These policies control what data appears in the clinical record.

A consent policy may be applied at one of three levels:

- System-wide
- Facility level
- Patient level

The issue in this advisory applies only to *clinical* consent policies that are applied *system-wide* or at the *facility* level.

Clinical consent policies specify a *Clinical Information Type (CIT)*. A clinical consent policy may optionally specify an *event start date* and *event end date* which should block or show data for events defined in the CIT based on those dates.

- When a clinical consent policy is configured at the *patient level*, the event start and event end dates for the CIT are respected.
- When a clinical consent policy is configured at the *system-wide* or *facility* level, event start and event end dates for the CIT may be specified, but those dates are ignored when the consent policy is evaluated.

An example scenario is as follows:

- A system-level clinical consent policy is set to “Default Block” a CIT for diagnosis data.
- A facility-level clinical consent policy for facility X is set to “Show” the CIT for diagnosis data with an Event Start Date of 2020-01-01.

The expected result is that only diagnoses occurring after January 1, 2020 at facility X will be shown. The actual result is that all diagnoses from facility X, regardless of the date they occurred, will be shown, because the *event start date* is ignored.

This issue has been identified as a patient privacy concern as it could result in *inappropriate* access to patient data by an *authorized* HealthShare user. This issue does not cause an increased risk of disclosure outside of HealthShare. A fix is not yet available for this issue.

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 = 2 out of 5

Recommended Action

InterSystems recommends that customers review their consent policies to determine whether they use *event start date* or *event end date* in clinical consent policies at the system-wide or facility level.

As a remediation, customers may choose to configure patient-level clinical consent policies to produce the correct behavior and should consider removing or modifying system-wide and facility-level policies clinical consent policies that rely on event start and event end dates.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-14".

End of Alert HS022-01-14

HS2022-01-15: FHIR Requests Not Being Evaluated Properly for Consent

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	Unified Care Record
Versions:	2020.1
System areas affected:	ODS, FHIR Gateway, Consent
Reference:	IF-1218 (HSIEC-6257)

Summary of Issue

This issue impacts only customers who meet all of the following criteria:

- You are using version 2020.1 of Unified Care Record.
- You have deployed the Operational Data Store (ODS) component.
- You have enabled a FHIR Gateway endpoint on the ODS.
- You use consent policies to grant or restrict access to PHI.

This alert and the associated correction address two related issues:

1. FHIR clients that send “patient search” requests to the FHIR Gateway will receive search results that do not follow consent policies defined in the system. This is a concern if a patient's address also discloses information about their care, such as a nursing home, prison, substance abuse, or mental health facility address.
2. When FHIR clients “read” resources from the FHIR Gateway, role-based consent policies that are intended to block or grant access to clinical data are not executed. This can result in FHIR clients either receiving or not receiving data erroneously due to consent policies.

Because these issues can result in improper disclosure of PHI to the requesting application, they are considered a privacy risk.

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

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.

Recommended Action

Two options are available to resolve this issue:

1. Obtain the ad hoc patch for IF-1218 (HSIEC-6257) and follow the WRC instructions for installation of the patch.
2. Upgrade the ODS to Version 2020.2. The ODS component can be upgraded without upgrading the entire Unified Care Record system. Please contact the WRC for instructions on how to use a 2020.2 ODS with version 2020.1 of Unified Care Record.

In addition, there are several immediate courses of action available to customers to prevent the improper disclosure of PHI related to this issue:

1. To prevent leakage of search demographics due to failure to evaluate consent, customers may disable the FHIR endpoint until the issue is resolved with a patch or upgrade.
2. To prevent disclosure (or lack of disclosure) of patient data due to lack of role-based consent evaluation, customers may temporarily implement a more restrictive consent model to avoid accidental disclosure of sensitive information such as protected mental health data.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-15”.

End of Alert HS022-01-15

HS2022-01-16: FHIR “$everything” Operation Can Return Unconsented Demographics

Issue date: 1-MAR-2022

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:	Unified Care Record
Versions:	2018.1, 2019.1, 2019.2, 2020.1, 2020.2
System areas affected:	Consent, FHIR API on ODS
Reference:	IF-1667 (HSIEC-6186)

Summary of Issue

The Unified Care Record Operational Data Store (ODS) provides an API to retrieve FHIR resources. Consent is applied to FHIR resource requests. However, when a FHIR query specifies the `$everything` operation, consent is ignored for “Organization” resources. The Organization resource indicates the healthcare facility that contributed the clinical data. While the actual clinical data is properly blocked by consent, the Organization resource is not.

A user of a client application that performed a `$everything` query would have an indication that the patient had received care from a sensitive facility such as a mental health or substance abuse facility where the clinical data had been blocked by consent rules.

If you have a HealthShare Unified Care Record version mentioned above that meets all of the following criteria, you are impacted by this issue:

- You have deployed the Operational Data Store component.
- You have enabled a FHIR endpoint on the Operational Data Store.
- You have facilities that are blocked by facility-based consent policies.

Full details of the identified issue appear in the Technical Addendum for HS2022-01-16.

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 = 3 out of 5 Likelihood of typical adverse outcome = 3 out of 5

Recommended Action

The correction, IF-1667 (HSIEC-6186), will be included in all future releases and is available as an ad hoc distribution from the Worldwide Response Center (WRC). Affected customers should request and apply the correction and may choose to apply the short-term mitigation actions described in the technical addendum.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-16”.

– Additional details for this issue appear in the Technical Addendum below –

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 HS2022-01-16

Description of Issue

When querying for a patient using the FHIR `$everything` operation, consent is ignored for Organization resources. The Organization resource is populated from SDA data and indicates the healthcare facility that contributed the data. While the actual clinical data is properly blocked by consent, the Organization resource is not. The unconsented Organization data would allow a user of a client application to infer that a patient had received care from a sensitive facility such as a mental health or substance abuse facility for which the clinical data was blocked by consent.

If you have a HealthShare Unified Care Record version mentioned above that meets all of the following criteria, you are impacted by this issue:

- You have deployed the Operational Data Store component.
- You have enabled a FHIR endpoint on the Operational Data Store.
- You have facilities that are blocked by facility-based consent policies.

Patient streamlets are the only type of streamlet where data is combined from multiple source records into a single record. This facilitates activities such as aggregating all Telecom contacts into a single record. It was discovered that the *Patient.EnteredAt* value was being included in the aggregated *Patient* streamlet, if the source streamlet was deemed the best record, even if facility-level consent resulted in that streamlet being excluded. This results in that data leaking out in a FHIR Organization resource when the FHIR `$everything` operation is used.

Recommended Action

If you are affected by this issue, request and apply the correction, HSIEC-6168, from the WRC.

As a workaround for this issue before you apply the correction, you may choose to:

- Ensure that any facility with facility-level consent in place is not the highest ranked facility by lowering the facility tier ranking for sensitive facilities in the facility registry.
- Deauthorize applications or users from using the `$everything` operation
- Limit access to the FHIR endpoint.

Please contact InterSystems' Worldwide Response Center (WRC) with any questions or for additional information.

Information about the Correction

The correction, IF-1667 (HSIEC-6186), will be included in all future releases and is available as an ad hoc distribution from the Worldwide Response Center (WRC).

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-16".

End of Alert HS022-01-16

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.

HS2022-01-17: FHIR Index Performance Issue Can Cause ODS Instability

Issue date: 1-MAR-2022

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 and Information Exchange
Versions:	2018.1, 2019.1, 2019.2
System areas affected:	ODS, FHIR Gateway
Reference:	IF-971

Summary of Issue

Operational Data Store (ODS) performance will degrade over time as the amount of data in the FHIR Gateway grows, due to an incorrect implementation of indexing on FHIR Resources that are shared between patient records, such as Practitioner resources.

Eventually, the number of shared FHIR Resources could grow to the point where excessive table scanning effectively takes the ODS offline.

This issue is corrected in version 2020.1 and later.

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 Action

There are three resolutions available for this issue:

1. Apply the ad hoc patch for IF-971 and follow the instructions provided by the WRC.
2. Upgrade the Unified Care Record deployment to version 2020.1 or later.
3. If you are on version 2019.1, you may alternatively upgrade only the ODS component to Version 2020.2. The ODS can be upgraded without upgrading the entire Unified Care Record system. Please contact the WRC for instructions on how to use a 2020.2 ODS with version 2019.1 of Unified Care Record.

As interim mitigation steps, customers may:

- Disable the FHIR endpoints on the ODS.
- Limit the growth of the FHIR Gateway by turning off the auto-load feature.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-17".

End of Alert HS022-01-17

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.

HS2022-01-18: Security Vulnerability in FHIR Gateway/FHIR Server

Issue date: 1-MAR-2022

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	Medium Risk CVSS 5.9	Not Applicable

Version and System Area Affected

HealthShare® Products:	Unified Care Record and InterSystems IRIS for Health
Versions:	2021.1
System areas affected:	FHIR, Security
Reference:	IF-2099

Summary of Issue

A security vulnerability has been found in the FHIR Gateway and FHIR Server that allows an *authorized system user with administrative privileges* to view information that should be hidden.

Risk Assessment

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

Security:	Medium Risk	CVSS 5.9

Recommended Action

InterSystems recommends that you obtain and apply the ad hoc correction for IF-2099 if you use the FHIR Gateway or FHIR Server in an affected version. This correction is also included in all later versions.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-18".

End of Alert HS022-01-18

HS2022-01-19: FHIR Server Does Not Verify Token Revocation

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products: Unified Care Record, Health Connect and InterSystems IRIS for Health

Versions:

- Unified Care Record: 2020.1, 2020.2, 2021.1
- Health Connect: 2020.4, 2021.1
- InterSystems IRIS for Health: 2020.4, 2021.1

System areas affected: FHIR Server and FHIR Gateway

Reference: IF-2103

Summary of Issue

The FHIR Server and FHIR Gateway properly validate an access token on initial requests. However, subsequent requests do not properly check for access token revocation. This could allow an attacker with access to a recently used FHIR session to access the server for a period of time even if the original client had properly logged out.

This could result in a revoked token being used by a malicious attacker.

Token expiration is properly handled and is part of the recommended mitigation.

Risk Assessment

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

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

Recommended Action

Affected customers should request and apply an ad hoc patch for IF-2103 from the Worldwide Response Center (WRC). The correction will be included in all future releases.

Customers may choose pursue the following short-term mitigation as well:

- Decrease the expiration time on tokens to reduce the risk of a revoked token being used.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-19".

End of Alert HS022-01-19

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.

HS2022-01-20: OAuth Token Scope Not Applied in FHIR Batch Transaction Bundles

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	InterSystems IRIS for Health
Versions:	2021.1
System areas affected:	FHIR Server, Security
Reference:	IF-1855

Summary of Issue

When the FHIR Server receives a batch transaction bundle, the OAuth2 token is validated; but when the FHIR Server processes the individual transactions contained within, the OAuth2 token scope is not evaluated against each individual interaction.

For example, a valid OAuth token that is scoped only for read access would allow write-based interactions if they were sent in a batch transaction bundle.

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

Recommended Action

A correction for the issue, IF-1855, is available as an ad hoc distribution from the Worldwide Response Center (WRC). The correction will be included in all future releases.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-20".

End of Alert HS022-01-20

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.

HS2022-01-21: FHIR Server Interoperability REST Client does not Properly Clean Up Data

Issue date: 1-MAR-2022

Risk Category and Score:

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

Version and System Area Affected

HealthShare® Products:	HealthShare Health Connect and InterSystems IRIS for Health
Versions:	2020.2, 2020.3
System areas affected:	FHIR Server
Reference:	IF-982

Summary of Issue

A potential stability issue has been identified for customers developing on some versions of InterSystems IRIS for Health and Health Connect who use the FHIR Server “interoperability REST client” class. Because this class does not properly clean up temporary data, the IRISTEMP global can continue to grow and could potentially consume all available storage.

Full details of the identified issue appear in the Technical Addendum for HS2022-01-21.

Risk Assessment

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

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

Recommended Action

Several options are available to remediate this issue. Please refer to the Technical Addendum for HS2022-01-21.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-21”.

– Additional details for this issue appear in the Technical Addendum below –

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 HS2022-01-21

Description of Issue

Developers who use the *HS.FHIRServer.RestClient.Interop* class to carry out write interactions such as Create and Update can see rapid growth in the IRISTEMP global. This happens if the input payload is supplied as a string or as any type of stream that *is not* a QuickStream. *HS.FHIRServer.RestClient.Interop* creates a QuickStream from the input and places a pointer to it in the *HS.FHIRServer.Interop.Request* object, but fails to clean up the QuickStreams in IRISTEMP after completing the call to the Business Host.

This poses a potential stability issue for customers developing on InterSystems IRIS for Health or Health Connect and using the functionality described. IRISTEMP will continue to grow and could potentially consume all available storage.

Recommended Action

The following actions can resolve the issue:

1. Restarting the impacted IRIS or Health Connect instance will clear the IRISTEMP database.
2. Developers should update their code to manually manage the creation and cleanup of QuickStreams and supply a QuickStream to the *RestClient.Interop* class.
3. Upgrade to InterSystems IRIS for Health or HealthShare Health Connect version 2020.4 or later.
4. Request an ad hoc patch for IF-982 and follow the instructions provided by the WRC to apply the patch.

Please contact InterSystems' Worldwide Response Center (WRC) with any questions or for additional information.

Information about the Correction

The correction, IF-982, will be included in all future releases and is available as an ad hoc distribution from the Worldwide Response Center (WRC).]

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference "Alert HS2022-01-21".

End of Alert HS022-01-21

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.

HS2022-01-22: Security Issue in Patient Index

Issue date: 1-MAR-2022

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	High Risk CVSS: 8.7	Not Applicable

Version and System Area Affected

HealthShare® Products:	Patient Index
Versions:	All versions: 15, 15.02, 15.03, 2018.1, 2019.1, 2019.2, 2020.1, 2021.1, 2021.2
System areas affected:	Security
Reference:	HSPI-2329

Summary of Issue

All versions of Patient Index through version 2021.2 contain a vulnerability described by this CVSS vector.

Risk Assessment

Security:	High Risk	CVSS: 8.7

Recommended Action

HealthShare Patient Index customers should obtain and apply the corrections, HSPI-2329 and HSPI-2258, as an ad hoc distribution from the Worldwide Response Center (WRC). These corrections will be included in all future releases of HealthShare Patient Index, beginning with version 2022.1.

If you have any questions regarding this alert, please contact the Worldwide Response Center, and reference “Alert HS2022-01-22”.

End of Alert HS022-01-22

– End of HS022-01 Alerts –

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.

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

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.

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

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.

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 HS2022-01 Alert Communication –