

HS2026-02 Alert for InterSystems HealthShare, IRIS for Health, and Health Connect

22-JUL-2026

Dear InterSystems Customer:

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

We have identified risks that may affect you when using:

- InterSystems IRIS® for Health
- InterSystems Health Connect™
- HealthShare® products

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 processes for cybersecurity, privacy, or product security, you can reach our Data Protection Officer, Ken Mortensen, at cyber@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,

Gokhan Uluderya
Director, Product Management

InterSystems
One Congress Street
Boston, MA 02114
TEL: +1.617.621.0600

Summary of Alerts

Alert	Product & Versions Affected	Risk Category & Score	Requirements
HS2026-02-01 Silent Upgrade Failure in Maintenance Versions of InterSystems IRIS for Health and Health Connect	Upgrades to version 2023.1.5 or 2023.1.6 of InterSystems: - Health Connect - IRIS for Health	Security: 3 – Medium Risk System Stability: 4 – High Risk	- Upgrading - Mirroring
HS2026-02-02 Synchronous Upgrade Step May Cause Additional Downtime	- InterSystems IRIS for Health: Version 2023.2 or earlier upgrading to any version up to and including 2026.1. - HealthShare Unified Care Record: Version 2023.1 or earlier upgrading to any version up to and including 2025.2.	System Stability: 3 – Medium Risk	- FHIR repository or ODS - Upgrading
HS2026-02-03 Consent Restrictions Not Applied to PIX Notifications and DSUB Subscriptions	HealthShare Unified Care Record: All versions	Privacy: 3 – Medium Risk	- MPI consent - External PIX notifications or DSUB subscriptions
HS2026-02-04 HealthShare Interoperability Deadlock Causes Fetch API Timeout	HealthShare Unified Care Record: 2024.2 through 2026.1	System Stability: 3 – Medium Risk	High-volume use of the Search and Fetch API

Detail of Alerts

HS2026-02-01 Silent Upgrade Failure in Maintenance Versions of InterSystems IRIS for Health and Health Connect

Issue date: 22-JUL-2026

Risk Category and Score:

Clinical Safety	Privacy	Security	Operational
Not Applicable	Not Applicable	3-Medium Risk	4-High Risk

Version and System Area Affected

Products and Versions:	InterSystems IRIS for Health and Health Connect when upgrading to version 2023.1.5 or 2023.1.6
Requirements:	Mirroring
System areas affected:	Upgrade
Reference:	IF-9148

Summary of Issue

Silent upgrade failures may be encountered in mirrored upgrades to InterSystems IRIS for Health or Health Connect 2023.1.5 and 2023.1.6.

Risk Assessment

The risk score and category were determined using the [InterSystems Risk Rating](#) process, and based on the following assessments:

Security:	3 – Medium Risk	
Operational:	4 – High Risk	Impact of typical adverse outcome = 4 out of 5 Likelihood of typical adverse outcome = 5 out of 5

Recommended Actions

For customers planning to upgrade to an InterSystems IRIS for Health or Health Connect 2023.1 maintenance release, InterSystems recommends waiting to upgrade using the 2023.1.7 release.

For customers that urgently need to upgrade to a 2023.1 maintenance release, please contact the WRC and reference IF-9023.

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference “Alert HS2026-02-01”.

– End of Alert HS2026-02-01 –

HS2026-02-02 Synchronous Upgrade Step May Cause Additional Downtime

Issue date: 22-JUL-2026

Risk Category and Score:

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

Version and System Area Affected

Products and Versions:	- InterSystems IRIS for Health: Version 2023.2 or earlier upgrading to any version up to and including 2026.1 - HealthShare Unified Care Record: Version 2023.1 or earlier upgrading to any version up to and including 2025.2
Requirements:	Unified Care Record ODS or InterSystems IRIS for Health FHIR repository
System areas affected:	FHIR, Upgrade, System Stability
Reference:	IF-9364

Summary of Issue

In InterSystems IRIS for Health 2023.3 and HealthShare Unified Care Record 2023.2, the `HardDelete()` method was corrected, preventing rows in FHIR tables from becoming orphaned. An upgrade step was added that deleted any orphaned rows in existing FHIR tables.

The upgrade step calls the `DeleteOrphanedRsrcRows()` method synchronously. On systems with very large tables of cached FHIR data, the method may take many hours to complete, causing extended downtime during the upgrade window.

A correction is available that can be requested as a full-kit ad hoc before the upgrade. With the ad hoc correction in place in the new kit, the upgrade will clean up orphaned rows as an asynchronous background job upon system startup (or when the instance becomes the primary), eliminating the upgrade delay.

Risk Assessment

The risk score and category were determined using the [InterSystems Risk Rating](#) process, and based on the following assessments:

Operational:	3 – Medium Risk	Impact of typical adverse outcome = 3 out of 5 Likelihood of typical adverse outcome = 3 out of 5
---------------------	-----------------	--

Recommended Actions

If you are planning an upgrade to an affected version, use the steps outlined in the technical addendum: [Determining Whether Your Upgrade Will Be Affected](#) to check for a large number of orphaned rows in your FHIR tables, and follow the recommendation there based on the number of rows identified.

A correction for this issue is available as a full-kit ad hoc. Customers who determine that they require a fix should contact the InterSystems Worldwide Response Center (WRC) and reference IF-9364.

This correction is included in the released HealthShare Unified Care Record 2026.1, and will be included in InterSystems IRIS for Health 2026.2.

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference “Alert HS2026-02-02”.

Technical Addendum for HS2026-02-02: Determining Whether Your Upgrade Will Be Affected

This issue only affects the following upgrade paths on systems with a FHIR Server or ODS:

- Upgrading from InterSystems IRIS for Health 2023.2 or earlier to any version up to and including 2026.1
- Upgrading from HealthShare Unified Care Record 2023.1 or earlier to any version up to and including 2025.2

Procedure to Determine the Number of Orphaned Rows in Your FHIR Tables

Use the steps outlined below to determine the number of orphaned rows in your FHIR tables:

1. In a terminal or the Management Portal, change to a namespace with a FHIR Server or ODS.
2. Run the following SQL query to identify your installed search and resource class packages:

```
SELECT r.ID, r.searchClassesPackage, r.resourceClassesPackage FROM
HS_FHIRServer.Repo r
  INNER JOIN HS_FHIRServer.RepoInstance i
    ON i.repo = r.ID
 WHERE i.IsDecommissioned = 0
```

Your query should return one or more results, where each result includes:

- a searchClassesPackage name ending with “.S”
- a resourceClassesPackage name ending with “.R”

For example:

ID	searchClassesPackage	resourceClassesPackage
1	HSFHIR.X0001.S	HSFHIR.X0001.R
2	HSFHIR.X0002.S	HSFHIR.X0002.R

3. For each result in Step 2, run the following SQL query, replacing the first italicized portion with the “S” package and the second italicized portion with the “R” package using underscore notation rather than dot notation (“HSFHIR.X0001.S” becomes “HSFHIR_X0001_S”):

```
SELECT COUNT(*) from <searchClassesPackage>.Rsrc WHERE Key NOT IN (SELECT
Key FROM <resourceClassesPackage>.Rsrc)
```

For example,

```
SELECT COUNT(*) from HSFHIR_X0001_S.Rsrc WHERE Key NOT IN (SELECT Key FROM
HSFHIR_X0001_R.Rsrc)
```

```
SELECT COUNT(*) from HSFHIR_X0002_S.Rsrc WHERE Key NOT IN (SELECT Key FROM
HSFHIR_X0002_R.Rsrc)
```

Requesting a Fix

Upgrading customers with more than a few hundred orphaned rows in their ODS or FHIR repository on their current version should use as their installation kit a full-kit ad hoc that includes the correction. Please request a kit that includes IF-9364 from the WRC.

With the correction in place, the upgrade will clean up orphaned rows as an asynchronous background job upon system startup (or when the instance becomes the primary), thereby eliminating the upgrade delay.

– End of Alert HS2026-02-02 –

HS2026-02-03 Consent Restrictions Not Applied to PIX Notifications and DSUB Subscriptions

Issue date: 22-JUL-2026

Risk Category and Score:

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

Version and System Area Affected

Products and Versions: All versions of HealthShare Unified Care Record

- Requirements:
1. MPI Consent (System, Facility, or Patient level) is configured to restrict patient search results.
 2. ...and at least one of the following is true:
 - PIX Notifications are configured for one or more external consumers.
 - DSUB Subscriptions exist in the Registry database.

System areas affected: Consent, IHE notifications

Reference: HSIEC-12464

Summary of Issue

Customers can configure consent restrictions at the MPI level. MPI consent prevents patient demographics from being returned to specific users, either for all records for a patient or only for records from a specific facility.

In affected versions, MPI consent is not being appropriately applied to outbound PIX notifications and DSUB subscription messages. As a result, patient demographic information that should be withheld from an external consumer or subscriber based on the patient's consent decisions is instead transmitted to that recipient.

For guidance on determining whether your environment is affected, refer to the technical addendum: [Assessing Potential Consent Impact from PIX Notifications and DSUB Subscriptions](#).

Risk Assessment

The risk score and category were determined using the [InterSystems Risk Rating](#) process, and based on the following assessments:

Privacy: 3 – Medium Risk

Impact of typical adverse outcome = 3 out of 5
Likelihood of typical adverse outcome = 4 out of 5

Recommended Actions

Refer to the technical addendum: [Assessing Potential Consent Impact from PIX Notifications and DSUB Subscriptions](#) to determine if you are affected by this issue.

A correction for this issue is available as an ad hoc patch.

Customers who determine they are impacted should contact the InterSystems Worldwide Response Center (WRC) and reference HSIEC-12464 to request the fix.

This correction will be included in Unified Care Record in version 2026.2.

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference "Alert HS2026-02-03".

Technical Addendum for HS2026-02-03: Assessing Potential Consent Impact from PIX Notifications and DSUB Subscriptions

Description of Issue

In an InterSystems HealthShare Unified Care Record environment where MPI consent policies are in use, certain conditions may cause PIX (Patient Identifier Cross-referencing) and DSUB (Document Metadata Subscription) notifications to be delivered without consent restrictions being applied to patient demographic data.

This issue only affects customers who use MPI Consent to restrict patient search results AND who either have PIX Notifications configured for one or more external consumers, or have DSUB Subscriptions present in the Registry database.

When these conditions are present, demographic updates for restricted patients may be sent to recipients who, based on the patient's consent decisions, should not receive them.

- If you have not configured MPI Consent (System, Facility, or Patient level), you are not affected.
- If you have not configured either PIX Notifications or DSUB Subscriptions, you are not affected.

Recommended Action

Use the steps outlined below to determine if your organization is affected by this issue:

1. Check if you have implemented MPI consent.

Only customers that have configured consent restrictions at the MPI level are affected. MPI consent prevents patient demographics from being returned to specific users, either for all records for a patient or only for records from a specific facility.

Have you configured system-wide, facility-level or patient-level MPI consent policies as described in the HealthShare documentation in [Consent in Unified Care Record](#)?

- **No.** You are not impacted. No further action is needed.
- **Yes.** You may be impacted. Continue to steps 2 and 3.

2. Check if you have implemented PIX notifications to external recipients.

Use the SQL Query below to evaluate what PIX notification consumers are defined, and whether they are internal or external. This query will display the host and port of the Service Registry entry that is linked to each PIX Notification item by the *ConsumerID*. Results will include both PIXv3 (SOAP) and PIXv2 (TCP) items.

Execute the following query in the Registry namespace:

```
SELECT oidmap.tcp->host,oidmap.tcp->Port,oidmap.OIDMapCode as ConsumerID
FROM HS_Registry_Service.tcp_OIDMapCode oidmap
inner join hs_ihe_pix_manager.domainsofinterest as domains
on oidmap.OIDMapCode = domains.consumerid
```

Some PIX consumers may be internal HealthShare applications (for example, Personal Community or Care Community). These can be ignored. This issue only impacts consumers sending PIX notifications to *external* organizations or communities.

Do the query results point to any hosts that are *external* to your Unified Care Record system?

- **No.** You are not impacted by external PIX notifications. Continue to step 3 to check for DSUB.
- **Yes.** You are impacted. External PIX notifications are in use. [Request an ad hoc correction](#).

3. Check if you have implemented DSUB subscriptions.

Perform the following query in your Registry database:

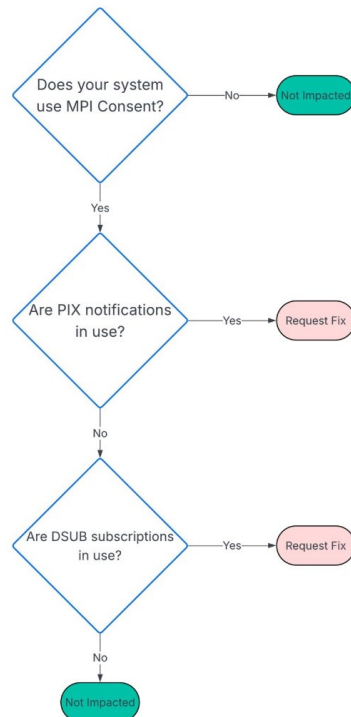
```
SELECT * FROM HS_IHE_DSUB_Subscriber.Subscription
```

Are any rows returned?

- **No.** You are not impacted by DSUB subscriptions. No action is required.
- **Yes.** You are impacted. DSUB subscriptions are in use. [Request an ad hoc correction.](#)

Note that the mere presence of HS.IHE.DSUB components in your productions does not indicate that DSUB is in use, as these components may exist because they are present in the default templates.

Decision Tree Diagram



Requesting a Correction

A correction for this issue is available as an ad hoc patch. Customers who determine they are impacted should contact the InterSystems Worldwide Response Center (WRC) and reference HSIEC-12464 to request the fix.

This correction will be included in Unified Care Record in version 2026.2.

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference "Alert HS2026-02-03".

– End of Alert HS2026-02-03 –

HS2026-02-04 HealthShare Interoperability Deadlock Causes Fetch API Timeout

Issue date: 22-JUL-2026

Risk Category and Score:

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

Version and System Area Affected

Products and Versions: HealthShare Unified Care Record: 2024.2 • 2025.1 • 2025.2 • 2026.1

Requirements: High-volume use of the Search and Fetch API for patient EPRs

System areas affected: HealthShare Interoperability

Reference: HSDD-6224 (no patch available)

Summary of Issue

In HealthShare 2024.2, as part of a larger change to increase search performance, the *INVOCATION* for the `HS.Gateway.Access.Manager` business operation was switched from *InProc* to *Queue*. When multiple `SearchAndFetch` requests are submitted to an Access Gateway, this can result in a deadlock, where requests from the front of the queue are waiting on responses that are stuck in the back of the queue.

Risk Assessment

The risk score and category were determined using the [InterSystems Risk Rating](#) process, and based on the following assessments:

Operational: 3 – Medium Risk

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

Recommended Actions

A two-part workaround has been identified. Both changes must be implemented in order to resolve the issue:

1. Add a second `HS.Gateway.Access.Manager` business operation to the production, and call it "FetchManager". Set the *FetchManager* property of the `HS.Gateway.Access.WebServices` business host to point to the new business operation.
2. Set the pool size the `HS.Gateway.Access.Manager` components to the expected number of simultaneous search requests plus some extra. If a queue develops, increase the value for the affected component.

If you have any questions regarding this alert, please contact the [Worldwide Response Center](#), and reference "Alert HS2026-02-04".

– End of Alert HS2026-02-04 –

– End of HS2026-02 Alert Communication –