SB-2026-002 — Multi-Site Reversible Pseudonymization (Solution Brief)

Document number: DOC-2026-430 **Solution brief:** SB-2026-002 **Version:** 2 **Category:** Marketing Material **Product family:** fleet (XyDromatics Router) **Owner:** Synthology Healthcare Solutions Group, LLC (SHSG) **Audience:** Prospective customers, design-partner candidates, and health-system imaging IT evaluating Synthology's site-to-site imaging exchange. **Regulatory posture:** Non-device software under **FD&C Act §520(o)(1)(D)**. No clinical or diagnostic function; nothing in this brief describes a medical device. **Companion:** Renders on the marketing site at `/whitepaper/multi-site-pseudonymization`. **Cross-references:** SB-2026-001 (AI-Vendor Egress with Pseudonymization); RI-2026-277 / RI-2026-279 (Router on-prem de-pseudonymization).

---

1. The claim, in one line

If you pseudonymize a study on the way out of your Router at one site and send it to your Router at another site — for the same customer — the destination Router can **restore full PHI**, because the reversible re-identification map travels **sealed inside the study** and the key is **already at the destination**. The wire never carries plaintext identity, and the key never rides with the study.

2. The problem — two compromises multi-site imaging makes today

Moving a study from one of your facilities to another is routine — and a routine place for patient identity to end up somewhere you did not intend. The two common approaches each give something up:

- **Ship PHI in the clear.** Send the study site-to-site with full identity intact, trusting the transport (VPN, private circuit, TLS) to protect it in flight. Identity is exposed to every hop, appliance, and log on the path. The blast radius of a misconfigured tunnel or a captured backup is the patient's name, MRN, and dates — in the clear.
- **Anonymize and lose the thread.** Strip identity before it leaves Site A. The wire is safe — but so is the study, uselessly: the far site receives an anonymous image it cannot reconcile with the patient, order, or prior. Irreversible de-identification is the right tool for research; it is the wrong tool for moving a clinical study between two of your own facilities.

The study needs to stay clinically whole **at the destination** — without patient identity riding across the network **in between**.

3. The approach — reversibility is a property of the study, not the network

On export, the Router pseudonymizes every PHI element and seals the **bidirectional re-identification map** — the table mapping each pseudonym back to its original value, plus the per-patient date-shift offset — **inside**

the study, encrypted under your customer key. The map travels with the pixels. Nothing at the far site phones home to the origin to reverse it; it needs only your key, which is already there.

The customer keypair lives **only in your environment**, at each of your sites, on the Router host. A site that does not hold your key receives a pseudonymized study and **cannot re-identify it**. That is not a limitation to work around; it is the access-control guarantee: the set of places that can restore identity is exactly the set of your sites you provisioned with your key — not an intermediary on the wire, and not Synthology.

4. How it works — four steps

1. **Pseudonymize on export (Site A).** A routing rule marked *anonymize-on-export* replaces PHI elements with deterministic pseudonyms, applies a per-patient date shift, and writes the reversible map.
2. **Seal the map inside the study.** The map is encrypted with **AES-256-GCM** under the customer keypair and embedded in a **DICOM private group** (not the File Meta header), carrying the customer id and key version. The study now self-describes how to be restored — to anyone holding the key.
3. **Travel over your existing transport.** DIMSE C-STORE or DICOMweb STOW-RS, your choice. The envelope lives in the PS3.3 data set, which both transports carry intact, so behavior is identical on either.
4. **Restore at the destination (Site B).** A single **restore rule** (*deanonymize-on-export*) on the Site B Router — matching the inbound studies — reads the envelope, resolves the customer keypair by the embedded customer id and key version, decrypts the map, substitutes every original value back, and reverses the date shift, then strips the envelope. Plaintext is delivered to the Site B PACS or workstation. **One rule is the whole control:** every inbound path — DIMSE C-STORE, DICOMweb STOW-RS, or a pull from the cloud exchange — is restored by the same rule, so there is no second switch to set or forget.

5. Fail-closed, and never silent

If the destination Router does not hold the key — or holds only a newer, rotated version the study predates — or the envelope is malformed, it **fails closed**: it refuses to re-identify and routes the study to its failed queue with the fixed reason *"Key missing or envelope is bad,"* recording the event. It never forwards an un-restored study, and never fails silently. Every automated reverse event is written to the SHA-256 **hash-chained audit log**, with a `verify` endpoint that walks the chain and surfaces tamper detection.

6. Why both transports behave the same

The DICOM standard separates the file-on-disk format (PS3.10, which includes a File Meta header) from the message-exchange protocol (PS3.7, the C-STORE wire). The File Meta header is reconstructed by the receiver and does **not** survive a C-STORE hop, so anything a sender writes there is lost in transit. The re-identification envelope is deliberately kept **out** of File Meta and placed in the **PS3.3 data set** instead. Both DIMSE and DICOMweb carry the full data set — so the same study restores identically over either transport.

7. The untrusted-recipient case

Send the same pseudonymized study to a recipient that does **not** hold your key — an external reviewer, an AI vendor, a partner site you have not provisioned — and they receive a clinically-usable but **de-identified** study. They cannot reverse it. Re-identification is gated entirely by key possession, which you control.

8. Shipping status (truthful-claims note)

Reversible DICOM pseudonymization, the per-customer keypair, the AES-256-GCM re-identification envelope in a DICOM private group, per-patient date-shifting, rule-driven restore on receive, fail-closed behavior, and hash-chained audit are **shipping in production**. Multi-site provisioning — distributing one customer keypair to a second on-prem site — is an **operational onboarding step**, not a software gap. Any claim in this brief traces to shipped, measured behavior.

Non-device software under FD&C Act §520(o)(1)(D). Not a medical device; no clinical or diagnostic function. © Synthology Healthcare Solutions Group, LLC.

> **Regulatory classification.** All Synthology and XyDromatics software described here is non-device software under the FD&C Act §520(o)(1)(D) software exclusion — not a medical device, and no clinical diagnostic function. Published by Synthology Healthcare Solutions Group, LLC as a controlled document; the authoritative version is the approved record in the Synthology quality-management system.