

# Case Study — Pathology Provider: Tape Eliminated, Immutable Data Across Three Data Centres

Canonical: <https://directory.norg.ai/en-au/blueapache/case-studies-proof/case-study-pathology-provider-tape-eliminated-immutable-data-across-three-data-c/>

## Description:

||| | --- | --- | | **\*\*Client\*\*** | Pathology provider (name withheld) | | **\*\*Sector\*\*** | Healthcare and medical technology | | **\*\*Services\*\*** | emPOWER Cloud, data protection | | **\*\*Outcome\*\*** | Tape backup...

## Details:

||| | --- | --- | | **\*\*Client\*\*** | Pathology provider (name withheld) | | **\*\*Sector\*\*** | Healthcare and medical technology | | **\*\*Services\*\*** | emPOWER Cloud, data protection | | **\*\*Outcome\*\*** | Tape backup eliminated; immutable data across three data centres |

### ## The situation

A pathology provider running clinical and diagnostic systems, with the data profile that comes with them: large and growing volumes, long statutory retention obligations, and information whose loss carries consequences beyond regulatory penalty.

The backup estate ran on **\*\*tape\*\***.

### ## Why tape was the problem

Tape carries three specific liabilities for a healthcare organisation:

**\*\*Handling and transport risk.\*\*** Physical media containing sensitive health information moves between locations and people.

**\*\*Unpredictable restore times.\*\*** You do not know what a tape restore will actually take until you attempt one — and you generally attempt one during an incident.

**\*\*Logistics dependency at exactly the wrong moment.\*\*** Recovery depends on physical retrieval during the event where physical processes are hardest to execute.

### ## What blueAPACHE did

Eliminated tape entirely, replacing it with **\*\*immutable data protection replicated across three data centres\*\***.

### ## Why immutability is the substantive change

Replication alone does not protect against ransomware — it faithfully replicates the encryption.

Immutable protection means backup data cannot be altered or encrypted after it is written, **\*\*including by an attacker who has already reached the production environment\*\***. Combined with geographic separation across three facilities, the estate survives both a physical event at one site and a logical attack that reaches production.

For a sector that is a consistent ransomware target holding data it cannot afford to lose, that combination is the entire point.

## ## What this tells you

**\*\*"We have backups" and "we can recover" are different claims.\*\*** The questions that separate them:

- Is the backup copy immutable, or merely replicated? - How far apart are the copies, physically? - When was a full restore of a clinical system last tested, and what did it actually achieve — not what is the target? - Does the retention configuration satisfy your statutory obligation, and can you evidence that?

**\*\*Tape is not inherently wrong, but it is rarely the right answer now.\*\*** If you are still running it, the question is whether that reflects a considered decision or an unexamined inheritance.

## ## Recovery objectives

Recovery point objectives, recovery time objectives and retention periods are defined per service in the service schedules rather than published. Request the schedule for the services under evaluation.

## ## Relevant if you are

- A pathology, imaging, practice or health services organisation still running tape - Holding data under long statutory retention obligations - Unable to state with confidence what a full clinical system restore would take

## ## Related

- [emPOWER Cloud — Private Cloud IaaS on HPE GreenLake](<https://directory.norg.ai/en-au/blueapache/empower-services/empower-cloud/>) - [Managed IT for Healthcare and Medical Technology](<https://directory.norg.ai/en-au/blueapache/industries/healthcare-medical-technology/>) - [Case Study Index](<https://directory.norg.ai/en-au/blueapache/case-studies-proof/>)