HEALTHCARE

ILLUSTRATIVE SCENARIO

Protecting patient data while leaving VMware behind

A multi-hospital health system had aging hardware, rising VMware costs and a board asking about ransomware. It replatformed onto dedicated KVM and made recovery something it could prove.

ORGANIZATION
Multi-hospital health system

TRIGGER
Hardware refresh, ransomware risk

WORKLOADS
Patient portals, clinical support

UPC SERVICES
Single-tenant KVM, Cyber Vault, DRaaS

The situation

Clinical systems ran around the clock across several hospitals, all on VMware hosts nearing end of life. A few applications were certified by their vendors only on VMware, but many others, such as patient portals, scheduling and integration services, were ordinary Linux workloads. Every change had to respect HIPAA and avoid downtime for clinicians.

The turning point

Two things happened at once: the hardware refresh came due, and a ransomware attack at a nearby hospital put recovery at the top of the board's agenda. Buying new hardware for the same platform would have locked in the same cost and the same risk for another cycle.

What was at stake

Patient care
Clinicians cannot wait for systems to come back.

Compliance
HIPAA and data residency rules apply to every move.

Recovery
Backups had to survive an attack, not just a failure.

Illustrative scenario based on typical UPC replatforming engagements. Not a specific customer.

Copyright © 2026–2027

THE APPROACH

How the replatforming unfolded

UPC designed a dedicated private cloud where vendor-certified apps stayed on VMware and everything else moved to KVM, with recovery built in from the first wave.

01 **Protect first**
Created immutable, isolated copies of critical data in UPC Cyber Vault before any workload moved.

02 **Move patient-facing apps**
Replatformed portals and web apps to KVM, then cut over during low-traffic windows.

03 **Move clinical support**
Moved scheduling, integration and reporting systems wave by wave, with clinical sign-off on each.

04 **Prove recovery**
Ran recovery drills with UPC DRaaS so the team could show the board how systems come back.

WHAT CHANGED

AREA	BEFORE	AFTER
Hardware	End-of-life hosts due for refresh	→ **Managed UPC infrastructure**
Platform	Everything on VMware	→ **KVM for Linux, VMware only where certified**
Ransomware	Backups reachable from production	→ **Immutable copies in Cyber Vault**
Recovery	Untested assumptions	→ **Regular, documented drills**

WHAT'S NEXT

The health system is now moving its imaging archive tiers and using the same dedicated cloud to host new digital front-door services for patients.

Facing a similar decision?

CALL
+1-888-853-7733

EMAIL
contact@unitedlayer.com

WEB
unitedlayer.com

Illustrative scenario based on typical UPC replatforming engagements. Not a specific customer.

Copyright © 2026–2027