

IGEL and Zscaler Healthcare Blueprints

Solutions for secure distributed care delivery

Table of Contents

Executive Summary 3

Protecting PHI Across Distributed Care Environments 4

Joint Healthcare Solution Blueprints 4

Blueprint 1: IRE Recovery Access Blueprint 5

Blueprint 2: Distributed Clinics Blueprint 6

Blueprint 3: Remote Clinician Access Blueprint 7

Architectural Characteristics 8

Cost and Operational Considerations 9

Summary 10



Executive Summary

Healthcare organizations are expanding how and where care is delivered. Outpatient clinics, imaging centers, virtual care platforms, and remote clinical workflows enable providers to improve access to care, support continuity, and scale services beyond the traditional hospital perimeter. At the same time, health systems are placing greater emphasis on operational resilience, ensuring that care can continue during disruptive events such as cyber incidents, infrastructure failures, or widespread endpoint compromise.

As care delivery becomes more distributed, the risk profile of the environment changes. More locations, more endpoints, and more access paths increase the potential attack surface and expand the number of systems that interact with electronic health records (EHRs) and other critical clinical applications. Without deliberate architectural controls, this distribution increases vulnerability and operational fragility. These conditions require architectures that control access precisely, limit exposure, and remain operational during disruption.

IGEL and Zscaler address these requirements through three joint healthcare solution blueprints. Each blueprint combines a secure endpoint foundation provided by IGEL and centralized access enforcement based on identity, policy and posture provided by Zscaler.

Together, these blueprints define endpoint to cloud access architectures that address two closely related requirements in modern healthcare environments. The first is resilient care delivery, supporting distributed clinics and remote clinicians with consistent, policy-controlled access. The second is resilient recovery, ensuring that critical systems such as Epic Isolated Recovery Environment (IRE) remain accessible even when endpoints or parts of the environment cannot be trusted.

With these solutions, organizations can simplify their security architecture by reducing the number of security tools, decreasing reliance on VPN infrastructure and branch security appliances, and consolidating overlapping secure access capabilities, while improving operational consistency and resilience.

Implementing these solutions allows organizations to simplify their IT infrastructure by consolidating security tooling, reducing bespoke tools, and eliminating legacy remote access solutions such as VPN, while improving security posture and operational efficiency.

Protecting PHI Across Distributed Care Environments

Securing protected health information (PHI) is a core requirement across all healthcare organizations. As endpoints and access paths multiply, PHI risk increasingly shifts away from centralized data centers and toward the edge of the environment.

The joint IGEL and Zscaler architecture addresses PHI protection across the full access path. At the endpoint, IGEL OS™ is immutable and read-only, with no local persistence of PHI. Devices reset to a known-good state on every boot, reducing residual data risk. A device that is lost, stolen, or compromised carries no locally stored patient data, eliminating a significant HIPAA exposure vector.

In transit and during access, Zscaler Private Access (ZPA) enforces identity- and policy-based access to clinical applications by brokering direct user-to-application connections rather than granting network-level access. No inbound ports are exposed, and access is evaluated per session based on identity, device posture, and policy—ensuring that only authorized users reach specific applications, never the broader network. All access activity is centrally logged, providing the auditability across user activity and application access required to support continuous risk assessment and documented ePHI data flow mapping under the proposed 2025 HIPAA Security Rule updates.[1]

By combining an endpoint that carries no patient data locally with per-session, identity-verified access enforcement, PHI handling is constrained end to end.

Joint Healthcare Solution Blueprints

Each blueprint describes a joint IGEL and Zscaler architecture that combines endpoint integrity with Zero Trust application access. The intent is to show how the two platforms work together to support specific healthcare workflows rather than to sequence one before the other.



Blueprint 1: IRE Recovery Access Blueprint

Context



Isolated Recovery Environments (IREs) are designed for the most disruptive operational scenarios, including destructive cyber incidents. Epic's IRE provides the application and data architecture required to continue care during a crisis. Effective use of an IRE depends on two conditions being met simultaneously:

1. The endpoints used for access must be trusted and operational.
2. Access to the recovery environment must be tightly controlled.

In actual ransomware incidents, traditional Windows endpoints are frequently compromised, encrypted, removed from service, or placed under quarantine for forensic investigation. Even when an IRE environment is available, clinical access is severely delayed because endpoint trust cannot be established quickly. Exposing an IRE to the public internet or relying on legacy VPN-based access introduces severe risk, potentially allowing malware to propagate from compromised endpoints into the pristine recovery environment.

Joint Architecture

This blueprint combines a recoverable, known good endpoint state with application-level access brokering so that recovery workflows do not depend on endpoint remediation or network trust.

IGEL provides a secure endpoint foundation for recovery operations. IGEL OS is immutable and does not depend on the local Windows installation. Existing endpoints can be configured for IGEL Dual Boot™ or IGEL USB Boot™ to load IGEL OS at startup, bypassing the installed Windows partition entirely during operation. Endpoints are centrally managed using IGEL Universal Management Suite™ (UMS) or UMS as a Service, typically hosted outside the impacted environment to ensure continued control during recovery. Access to the IRE is delivered through a minimal, purpose-built IGEL OS configuration that includes the IGEL OS base image, an approved Chromium-based browser, approved virtual desktop or Desktop-as-a-Service (DaaS) clients supporting Citrix, Omnissa, and Microsoft platforms, and required identity and authentication components. No PHI is stored locally, and endpoints return to a known-good state on every reboot.

Zscaler provides controlled, zero trust access to the IRE. Zscaler Private Access (ZPA) brokers access to the IRE as a private application rather than exposing it to the public internet. Access is established outbound only and evaluated per request based on identity, context and policy. Access paths bypass potentially compromised internal networks by brokering sessions directly to the IRE through ZPA under centralized policy enforcement. No inbound listeners or VPN gateways are required, and all access activity is centrally logged and visible for audit and investigation.

Combined Operational Result

The IRE is not reachable from the public internet. Recovery access does not depend on trusted Windows endpoints. Compromised internal networks are bypassed during recovery access. Endpoint integrity and access control are enforced independently but coherently. Clinical recovery can proceed in parallel with forensic investigation and system remediation.

Blueprint 2: Distributed Clinics Blueprint

Context

Outpatient clinics and imaging sites allow healthcare organizations to deliver care closer to patients and reduce reliance on centralized facilities. These environments introduce distributed endpoints, limited on site IT resources, increased dependence on remote access to hospital hosted systems, and greater exposure to physical risks such as device loss, theft, or unauthorized local access.

Traditional clinic architectures often rely on local security appliances, costly WAN connections or VPN backhaul, and heterogeneous endpoints. As clinic footprints grow, this model becomes increasingly inefficient, complex, and costly to operate.

Joint Architecture

This blueprint establishes a standardized clinic access model built on controlled endpoints and centralized policy enforcement.

IGEL provides a standardized endpoint platform across all clinics. Endpoints are centrally configured, updated, and managed via the IGEL UMS, reducing the need for local IT staff. IGEL OS supports clinical peripherals, avoids any local persistence of PHI, and removes the need for local administrative access, dramatically lowering the local device attack surface.

Zscaler enforces cloud-delivered security controls for all traffic. Zscaler Zero Trust Branch (ZTB) secures traffic between clinics and hospital data centers removing the need for dedicated WAN circuits or VPN backhaul. This is ideal for securing devices that cannot host the Zscaler agent (such as medical devices, IOT, and IoMT. Zscaler Private Access (ZPA) enforces granular, policy-based access to private clinical applications and PHI, while Zscaler Internet Access (ZIA) applies consistent, high-performance web security, inline data protection, and cloud application control (SaaS) for clinical staff.

Combined Operational Result

Clinics share a consistent, repeatable endpoint and access model regardless of location. Reliance on traditional branch security appliances and VPN hardware is eliminated. IGEL enables cost optimization across new and existing facilities by extending endpoint life, simplifying the endpoint software stack, and lowering operational overhead. Zscaler reduces cost and complexity by consolidating secure access, remote connectivity, and branch security capabilities into a single cloud delivered platform. Together, these efficiencies improve the return on investment for distributed clinic deployments while maintaining consistent security and operational control.

Blueprint 3: Remote Clinician Access Blueprint

Context

Remote and hybrid clinical work is now a permanent component of healthcare delivery, driven by the expansion of telehealth, home health, remote diagnostics and administrative flexibility. Clinicians require fast, seamless access to clinical systems from home and other remote locations. Legacy VPN based approaches typically extend broad network access to remote devices without sufficient control over endpoint state or session context, dramatically widening the attack surface and increasing the risk of lateral threat movement.

Joint Architecture

This blueprint applies the same endpoint and access controls used in clinical facilities to remote environments.

IGEL provides a controlled endpoint state for remote clinicians. Endpoint configuration remains consistent regardless of location, endpoint attack surface is reduced outside hospital networks, and no PHI persists locally. Optionally, IGEL USB Boot can be used to provide a secure, managed IGEL OS environment on clinician owned devices, enabling remote access without relying on the underlying operating system.

Zscaler enforces policy-based access to clinical applications regardless of user location. The Zscaler Client Connector (ZCC) agent running on the IGEL endpoint enforces access and security policies directly at the endpoint edge. ZPA and ZIA apply rigorous identity and context-based controls to private applications, SaaS services, AI services, and internet access. Security policies are continuously evaluated and enforced, independent of user location or network.

Combined Operational Result

Clinicians experience consistent access behavior across hospital, clinic, and home environments, reducing login friction and enhancing user experience. Reliance on insecure VPN infrastructure is eliminated. Security teams gain centralized visibility, auditability, and control over all remote access activity and internet security policy is consistently enforced regardless of location.

Secure IRE with Zscaler and IGEL

Epic Isolated Recovery Environment

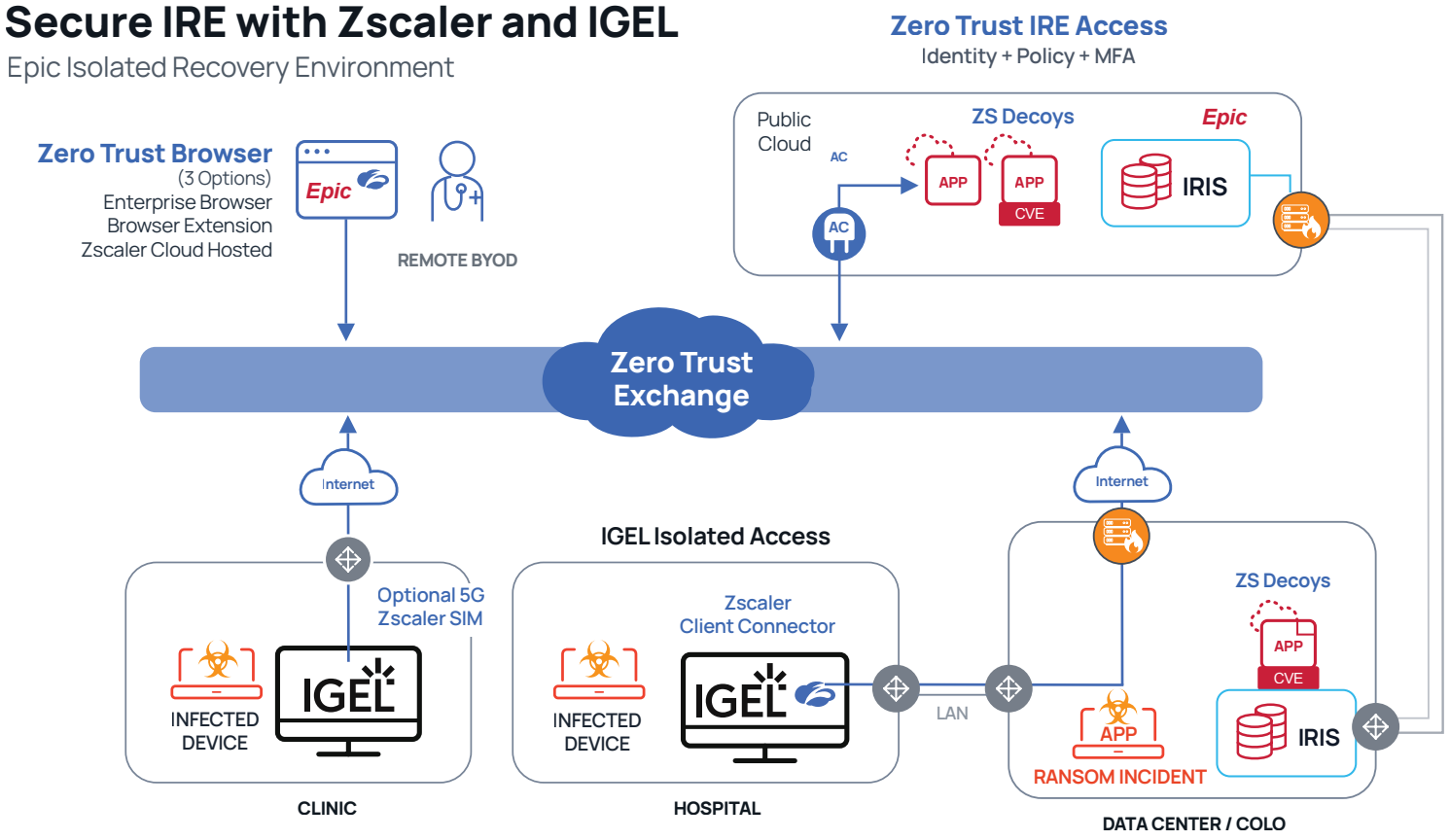


Figure 1. Secure IRE with Zscaler and IGEL

Architectural Characteristics

Across all three blueprints, endpoint attack surface and PHI persistence are minimized through IGEL's Preventative Security Model®. Access is enforced through identity and policy-based controls rather than network location. Endpoint integrity and access control are treated as coordinated but independent concerns. These architectures apply Zero Trust design principles such as explicit verification, least privilege access, and reduced implicit trust across endpoint and access workflows.

Cost and Operational Considerations

The joint IGEL and Zscaler approach significantly reduces capital and operational expenditures across all three clinical use cases by standardizing endpoint and access architectures rather than relying on disparate point solutions.

Cost and Operational Considerations

The joint IGEL and Zscaler approach significantly reduces capital and operational expenditures across all three clinical use cases by standardizing endpoint and access architectures rather than relying on disparate point solutions.

Hardware

Endpoint hardware life is extended for both new and existing devices, increasing typical usable life from approximately three to five years to six to eight years and helping offset rising hardware costs. The need for emergency endpoint sourcing during recovery scenarios is reduced, as existing devices can be repurposed using IGEL OS. Dependence on branch security appliances and VPN hardware is also eliminated.

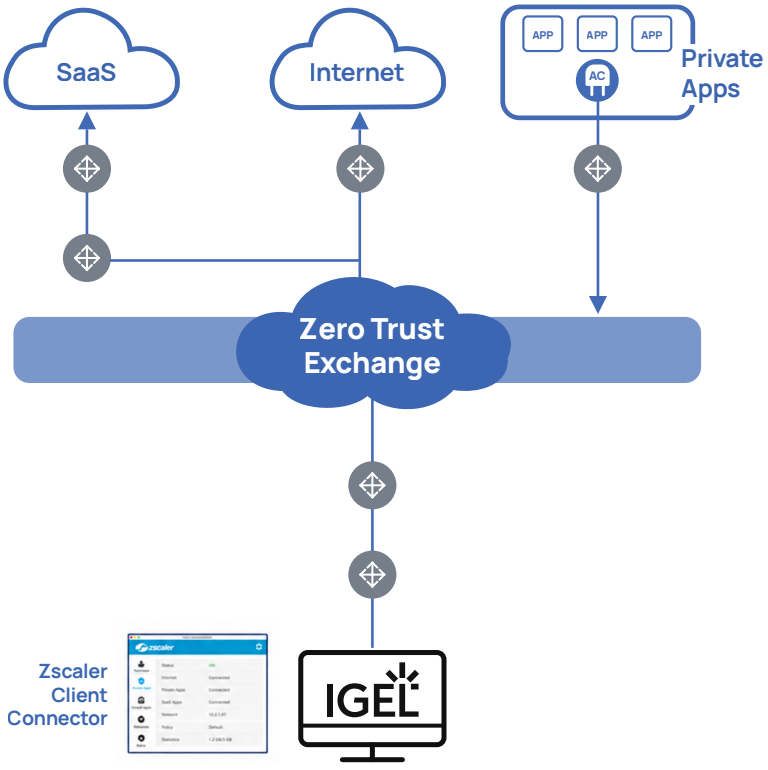


Figure 2. Zscaler Client Connector

Software

Large portions of the traditional endpoint security stack are eliminated through IGEL's Preventative Security Model, reducing the need for multiple endpoint security agents. Overlapping secure access, VPN, and other remote connectivity tools are consolidated by standardizing on Zscaler for private application access and internet and internet/SaaS security. The endpoint software footprint is simplified through use of a single secure endpoint operating system across multiple workflows.

Operations

Operational burden on lean healthcare IT teams reduced through centralized endpoint management combined with Zscaler's global cloud admin console. Device configuration, security patching, and policy updates are executed globally in minutes.

Summary

Healthcare organizations are redesigning their IT environments to support care delivery that is more distributed, more flexible, and more resilient. This shift introduces new risk as endpoints, access paths, and locations multiply, but it also creates an opportunity to modernize security and operations in ways that better align with how care is delivered today. The joint IGEL and Zscaler architectures described in this paper address both sides of that equation. Together, they provide a secure endpoint and access foundation that supports day to day distributed care delivery while also enabling recovery when systems, networks, or endpoints cannot be trusted. These architectures apply across normal operations, expansion into new outpatient facilities, and worst case recovery scenarios.

Within the hospital, IGEL and Zscaler function as core components of a modern security strategy by reducing endpoint attack surface, enforcing identity and policy-based access, and improving visibility. Beyond the hospital perimeter, the same capabilities extend robust security controls and operational consistency to clinics, remote clinicians, and recovery environments without reintroducing legacy VPN or branch centric models.

By standardizing on a secure endpoint platform and a cloud-delivered access and security layer based on Zero Trust, organizations can reduce architectural complexity, consolidate overlapping tools, and achieve measurable cost savings across hardware, software, and operations. At the same time, they improve resilience and maximize the return on investment in distributed care models.

Collectively, these blueprints demonstrate how IGEL and Zscaler enable healthcare teams to extend secure access to care wherever it's needed, stay resilient during disruption, and reduce operational complexity with a streamlined, sustainable approach.

References

1. HHS Office for Civil Rights. "HIPAA Security Rule — Notice of Proposed Rulemaking." Federal Register, January 6, 2025.

Key provisions include mandatory MFA, universal ePHI encryption, 72-hour restoration requirement, and elimination of "addressable" safeguard category. Finalization targeted mid-2026; 240-day enforcement grace period.

Contact your IGEL Representative to arrange your free trial.

IGEL is a registered trademark of IGEL Technology GmbH. All hardware and software names are registered trademarks of the respective manufacturers.
Errors and omissions excepted. Subject to change without notice. © 11/2026