VIRGINIA COMMUNITY HEALTHCARE ASSOCIATION™
45 YEARS 1980-2025

RAINTECH
Cloud. Security. Support. **Results.**

Resilience in the Face of a Crisis

Disaster Recovery for Health Centers

Andrew Jahnke

CEO & People Person,
Founder of RainTech

RAINTECH
Cloud. Security. Support. **Results.**

Our purpose is to cultivate experiences where individuals thrive, empowered to connect, grow, and lead together.

People ~~First~~, PERIOD.™

It’s Monday morning.

Ransomware has locked your EHR.

What happens next?

Disaster Scenario: Real World

- Is your DR plan accessible offline?
- What does it say to do first?
- Is your backup system protected/air-gapped from ransomware?
- How long will it take to restore your EHR?
- What about your ERP and other systems?
- How will you continue seeing patients and documenting care during downtime?
- Who communicates with internal teams, patients, and vendors during a ransomware event?

62%

of companies filed a cyber insurance claim in 2024

27%

filed 2 or more claims

Delinea 2024 State of Cyber Insurance Research Report

Disaster Scenario: By the Book

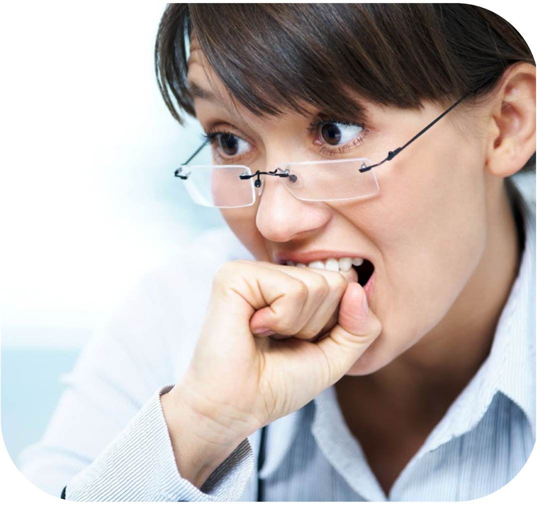
- Have you reviewed your cyber insurance policy and does your Incident Response plan align with their requirements?
- Is the Incident Response provided/required by your insurance carrier even adequate?
- Who is responsible for notifying HRSA and do they know the required timeframe?
- Do you monitor your disk reads and egress traffic to identify data exfiltration?
- How would you prove to an auditor that you’ve tested your DR plan?
- Have you done a tabletop exercise to simulate this exact scenario?

Disaster Recovery Drivers

Real World Risks

Natural Disasters

Cyber Attacks



Human Error

Theft

Disaster Recovery Drivers

Compliance & Regulatory

HIPAA Security Rule (45 CFR §164.308(a)(7))

Contingency planning, DR, data backup, and testing requirements

FTCA / CMS Conditions of Participation

Patient safety and continuity mandates

HRSA Program Requirements

Ensuring continuity of care and compliance with site visit protocols

Business Continuity

Beyond Servers and Data

- Patient Care Continuity
- Clinical Documentation and Reconciliation
- Communication Plans
- Workforce Management
- Facility Operations

- Supply Chain and Vendors
- Revenue Cycle and Billing
- Leadership and Decision-Making
- Offline Access to Critical Information
- Reputation Management

Common Challenges for Health Centers

Funding Gaps

Limited Time to Test

Lacking Skills/Expertise

Incomplete Infrastructure Backups

Take the Disaster Out of Your Recovery Plan

Overview

Disaster Recovery Approaches

On-Prem Secondary Site

Duplicate servers at another clinic or colocation site.

Third-Party Hosting/Vendor

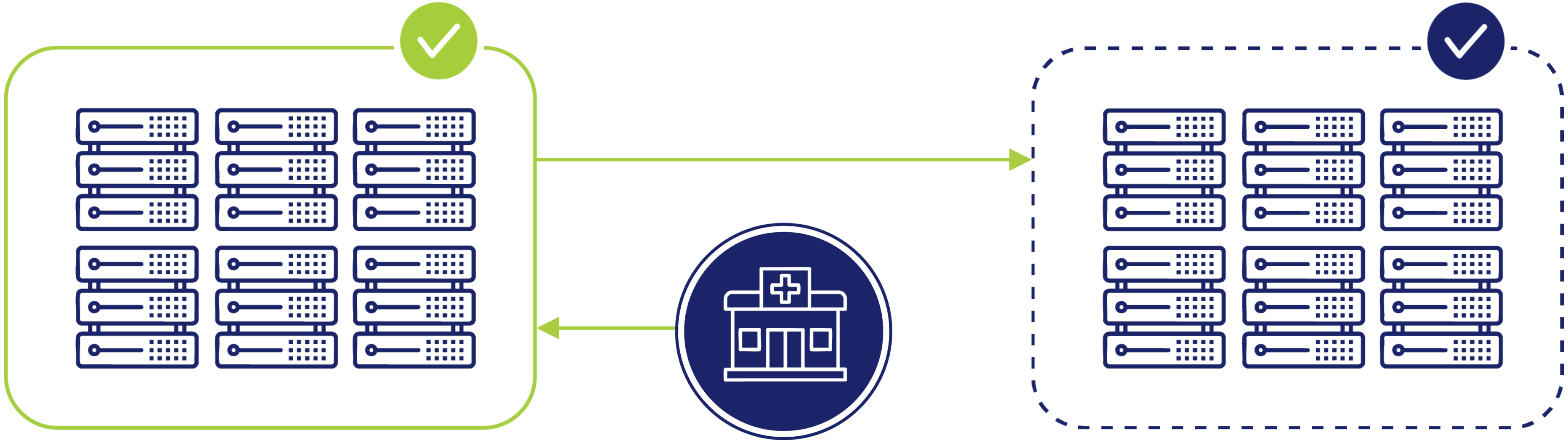
Partner with specialized service provider.

Cloud-Based (Azure Site Recovery)

Data and apps replicated to secure public cloud.

Overview

Disaster Recovery Process



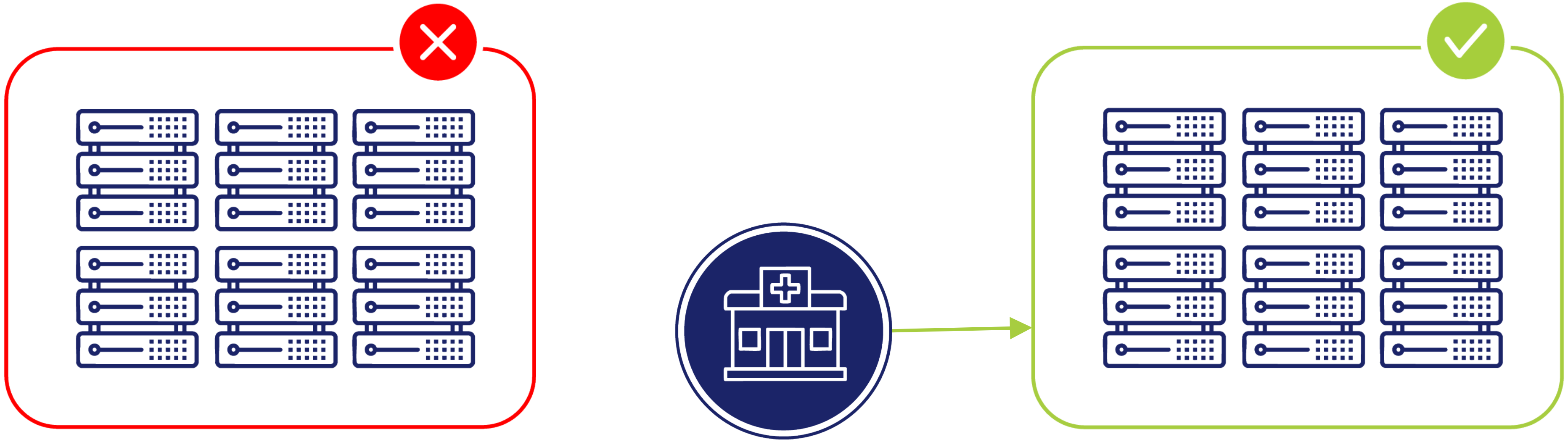
Production Servers

Customer Location

Disaster Recovery Infrastructure

Overview

Disaster Recovery Process



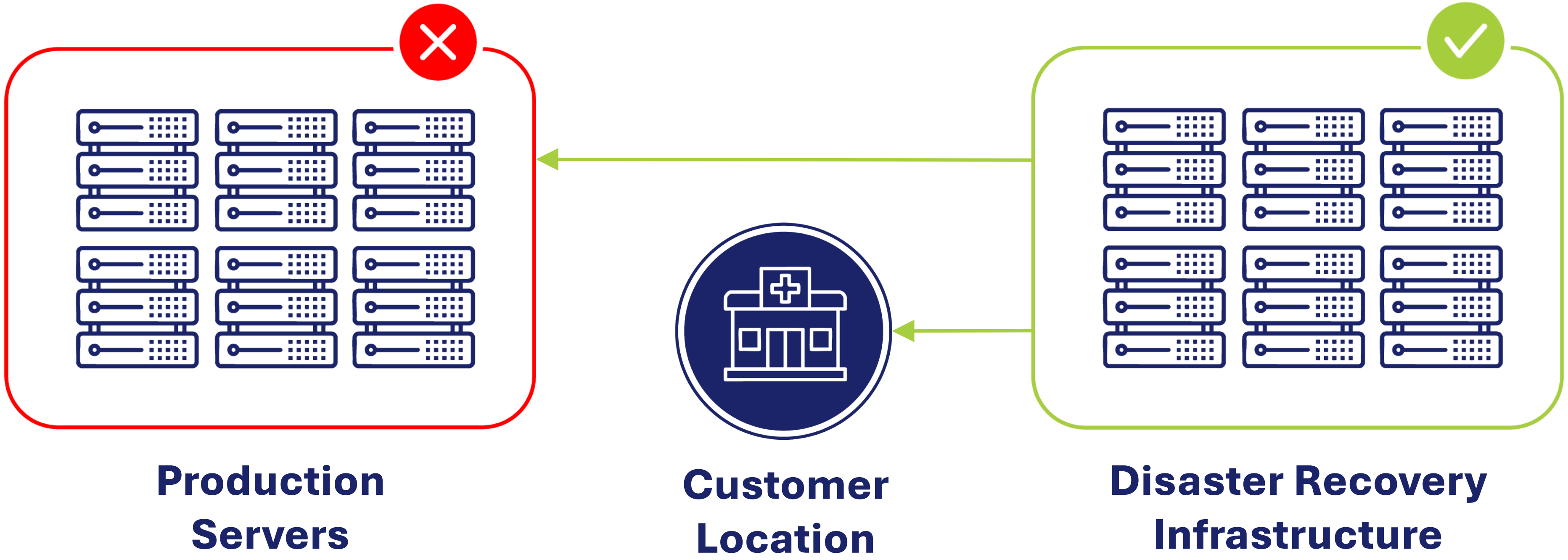
Production Servers

Customer Location

Disaster Recovery Infrastructure

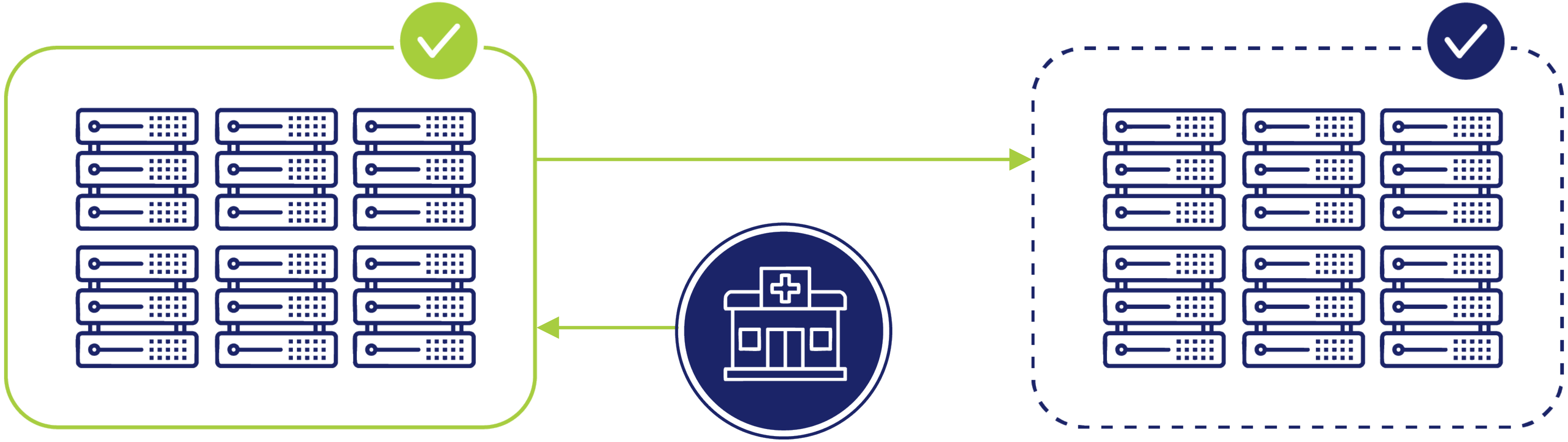
Overview

Disaster Recovery Process



Overview

Disaster Recovery Process



Production Servers

Customer Location

Disaster Recovery Infrastructure

Disaster Recovery Approaches

On-Premise Secondary Site

PROS

Covered by Capital Development Grants

Predictable performance

CONS

High capital cost

Ongoing maintenance

Very long-term skill requirements

Appliance-based solutions are limited in their ability to recover

COMPLIANCE TIE-IN

Must prove backup integrity and test and document annually (resource strain)

Why and When

On-Premise Secondary Site

- **Unreliable or limited internet access**
- Have **existing infrastructure** and want to maximize its use

- Have **dedicated internal IT team** capable of managing and testing DR in-house
- Finances dictate **CapEx investment** over recurring cloud OpEx

Disaster Recovery Approaches

Third-Party Hosting / Vendor

PROS

Professional support

Little to no capital cost

Often little to no third-party cost associated with DR testing

CONS

Vendor lock-in

Generally, not covered by capital development grants

COMPLIANCE TIE-IN

HIPAA requires BAA and documented recovery testing

Why and When

Third-Party Hosting / Vendor

- **Lack in-house resource availability** to configure and manage a DR environment themselves
- Want **expert guidance** on DR, compliance, and recovery planning
- Need a **"set-it-and-forget-it" approach** with clear SLAs and support
- Seeking **predictable monthly costs** and reliable vendor relationship
- Opt not to have duplicate onsite hardware, but **lack public cloud expertise and budget**
- Prefer to **outsource the complexity** of DR
- Want **automated testing and audit trails** to satisfy HRSA, HIPAA and cybersecurity insurance requirements

Disaster Recovery Approaches

Public Cloud-Based (Azure Site Recovery)

PROS

Scalable

Highly resilient

CONS

Subscription costs are expensive and can be unpredictable

Hiring Azure-certified staff is expensive

COMPLIANCE TIE-IN

Microsoft will sign a BAA

Why and When

Public Cloud-Based (Azure Site Recovery)

- Already in (or moving to) **Azure for other services**, making integration easier
- Need a **scalable, flexible DR solution** that grows with them
- Want to **reduce capital expenses** and only pay for what they use
- Need **geographic redundancy** to protect against regional outages
- Want **automated testing and audit trails** to satisfy HRSA, HIPAA and cybersecurity insurance requirements

DR-as-a-Service: Often the Best Fit

- Predictable OpEx vs. CapEx
- Includes Annual Testing and Documentation
- Specialized Expertise on Demand
- Scalable with Growth

Case Study

Third-Party Hosting DRaaS Solution

Case Study: Third-Party DRaaS

The Challenge

➡ **Legacy DR setup put patient care and compliance at risk**

- DR appliance was located on-site — vulnerable to physical disasters
- Could only virtualize a fraction of the FQHC's production servers
- Slow and partial failover risked major care disruptions
- No streamlined way to test DR — made HIPAA compliance harder
- Leadership needed a scalable, healthcare-aware partner

Case Study: Third-Party DRaaS

The Solution

➡ **MSP deployed a fully managed cloud-based DRaaS platform**

- Backups moved to secure, offsite cloud infrastructure
- Full environment failover in under two hours
- On-demand file and folder restoration — no hardware needed
- Network and VPN configurations replicated for seamless access
- Full failover test completed within 30 days; annual testing included

Case Study: Third-Party DRaaS

The Outcome

➡ **Modern, resilient DR with real peace of mind**

- Eliminated on-site hardware risk and single points of failure
- Significantly faster recovery during outages
- Simplified HIPAA compliance with built-in, documented testing
- Freed up internal IT to focus on strategic work
- Continuity of care delivery — even when disaster strikes

> Our previous Datto solution left us feeling uncertain about our disaster recovery readiness. We recognized that it would likely fall short in the event of a true emergency. Our MSP provided a seamless transition to a new solution that has exceeded our expectations. **The recovery process is now efficient, straightforward, and fully tested.** With no reliance on physical hardware and no compliance concerns, we have complete confidence in a solution that ensures business continuity.
>
> **— Vice President of Technical Services**

Key Takeaways

- A disaster recovery plan is not optional — compliance requires it
- Multiple approaches exist, each with challenges
- DRaaS offers best fit for most health centers' realities
- Annual testing and audit documentation are critical differentiators
- Alignment with cyber liability insurance

Thank You!

RAINTECH

Cloud. Security. Support. **Results.**

Andrew Jahnke

andrew@rain.tech
844.TEL.RAIN
www.rain.tech

VIRGINIA COMMUNITY HEALTHCARE ASSOCIATION™
45 YEARS 1980-2025