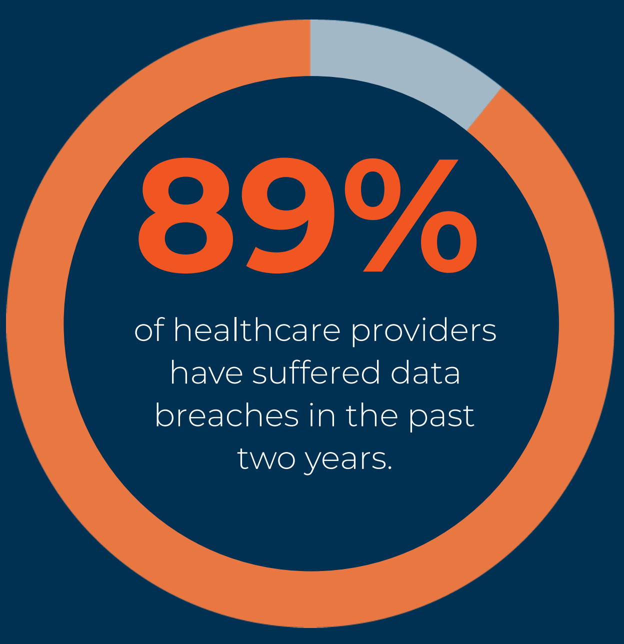
Bad actors and disruptions to your clinical documentation systems are inevitable. Are you resilient?

Clinical documentation is mission critical to revenue cycle, patient care and physician efficiency. Third-party partners that manage your clinical documentation must be reliable—even when hacks, upgrades and other disruptions occur.

If something disrupts your speech, scribing, dictation, or direct EHR input systems, are your business associates able to recover? Are they resilient?



1.76 Healthcare breaches of 500 or more records per day in December 2020, which is nearly double the rate from 2018. (HIPAA Journal)

$429 Amount healthcare institutions spend on average per stolen record.

$6.45M Amount data breaches cost healthcare providers on average.

42% 42% more healthcare hacking incidents in 2020 (Proteus, April 2021)

Five keys to clinical documentation resilience

Business continuity demands resilience. Clinical documentation data must be protected and accessible.

Clinical Documentation Security Index

Based on lessons from recent malware, ransomware and hacking events, here's a clinical documentation security index for your organization. Inspect what you expect from your clinical documentation partners.

- Cloud-based
- Azure-hosted security center
- Multi-tenant
- Data centers in multiple geographical regions
- Active-active failover with production testing

6 Tough Questions to Ask Your Clinical Documentation Partner

- What is your RTO/RPO guarantee?
- What is your business continuity management policy?
- How often do you perform fail over testing in a live environment?
- Is your system multi-tenant to ensure quick delivery of new features, upgrades and security updates?
- Are your data centers cloud-based, using tier 3+ security, and continually monitored and replicated?
- Can you redeploy compromised systems – servers, cloud native resources and networks – in minutes, not hours?

Protect Data + Access Data = Business Continuity

> "Effective busines continuity management reduces the likelihood of impact or significant business disruptive incidents, mitigates legal, compliance, regulatory and reputational risks, and helps to ensure the health and safety of employees."
>
> DeliverHealth Business Continuity Management Policy, July 2019

DeliverHealth's eSOne platform

Our platform provides exceptional security, data backup, protection, redundancy, and stability with robust functionality.

- Hosted in multiple geographical regions in active-active state
- Real-time monitoring, patching, updates and releases with no impact on customer uptime
- Weekly internal and external scanning to track deficiencies
- Regular and/or customer specific failover in production testing
- Regular and/or customer specific penetration tests
- Regular but no less then yearly updates to BC/DR plans
- Azure security centers with real-time monitoring and access control. Ask to see it in action.

We keep your clinical documentation safe so your organization stays on the path to uninterrupted patient care and proper, timely reimbursement.

Visit **deliverhealth.com** to learn more.

DeliverHealth

Sources: https://leftronic.com/healthcare-data-breach-statistics/
https://www.medicaleconomics.com/view/the-key-to-interoperability-safe-secure-access-to-patient-health-data