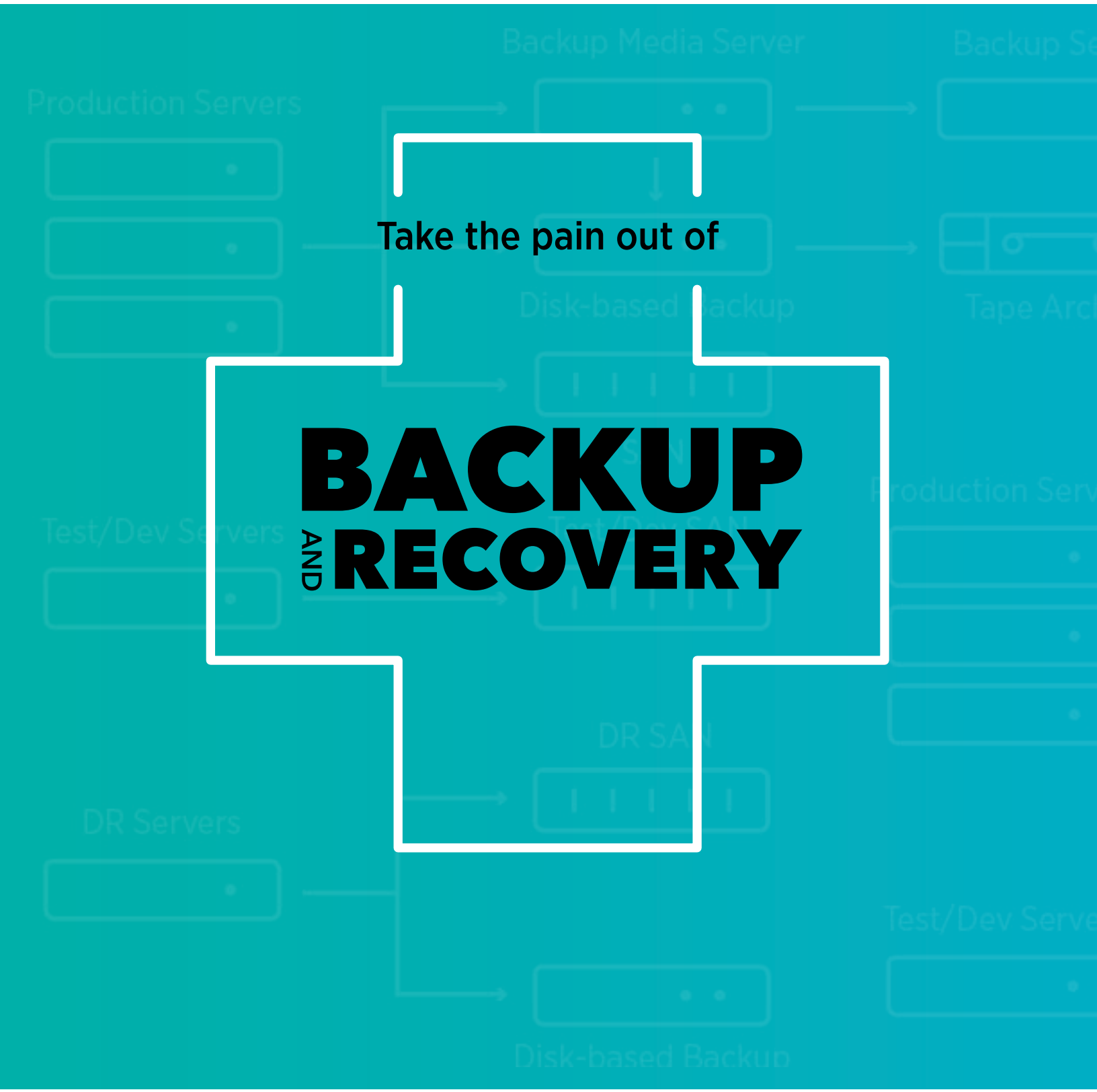

Take the pain out of

BACKUP AND RECOVERY

rubrik

Tell the doctor where it hurts.

Treating patients is a healthcare provider's primary purpose, and technology plays a mission-critical role in that contract. Equipment like MRI and heart-lung machines, infusion pumps, medical monitors, ventilators, and incubators help healthcare professionals (HCPs) save lives. HCPs electronically chart patient records on PCs, tablets, and smartphones, and they have the medical Internet of Things with its assortment of wearables and mobile apps to gather additional patient data.[1]

As you're well aware, all of these machines create mountains of data that become part of a patient's digital health record.

You've always protected your company's digital financial and business data. When healthcare shifted from paper to digital charts, you protected those too. Now with health information technology's move from electronic medical records (EMR) to electronic health records (EHR), you're responsible for collecting, maintaining, and protecting a huge volume of unstructured patient data. And this avalanche of data is only going to grow.[2]

Your reputation relies on the ability to collect and access patient data quickly, accurately, and securely. Data failures can result in significant financial losses[3] and damage to your company's reputation. Data failures pose greater risks for healthcare companies than for those in other industries; you may incur hefty HIPAA fines[4] as well as threaten the trust your patients have that you can protect their privacy.

Worst of all, data failures could cost patient lives.

How long have you been feeling this way?

Until now, preserving your growing amount of data required not only ballooning amounts of storage, but also implementation of four or more products—sometimes from four or more different companies—to back up both cloud data and on-premises data originating from your increasingly heterogeneous ecosystem of devices. Those products included, but weren't limited to, storage, backup software, back-end databases, replication software, and archiving software to name a few. Putting those disparate products together meant weeks of installing, setting up, integrating, testing, and tweaking, especially if you're trying to protect branch clinics and offices. Add to that the manual effort you needed to fulfill new user requests and ensure the protection of new assets.

You may even have stored your backups on the same system where the vast majority of your data lived, and allowed client administrators full backup access. This approach could cost you dearly, and because it left your backups vulnerable to exactly the same attacks as your underlying data, it could also result in lost data—rendering all the time and money you spent on backup plans worthless.

One ransomware attack could cost days of effort and productivity, not to mention data loss-- especially if your most recent backups were compromised along with your data. If you were lucky, you could restore from a backup. If you weren't, you paid the ransom and hoped that the attacker would actually give you the password to unlock your data.

So despite your best efforts, your data may still be at risk.

[1] Mobile Devices and Apps for Health Care Professionals" Uses and Benefits, US National Library of Medicine, National Institute of Health, 2014 May.

[2] A 2012 International Data Corporation study anticipates a 48% annual increase in the amount of stored health data, from 153 exabytes in 2013 to 2,314 exabytes by 2020. (How CIOs Can Prepare forHealthcare 'Data Tsunami,' CIO Magazine, 12/16/2014).

[3] The Ponemon Institute calculates that organizations face average costs of $740,357 per outage or about $9,000 per minute per incident, roughly a 38 percent increase since its original 2010 study. (2016 Cost of Data Center Outages, Ponemon Institute, 01/19/2016).

[4] HIPAA settlements hit record levels in 2016. The Department of Health and Human Services' Office for Civil Rights collected more than $22.8 million in 2016 to resolve alleged HIPAA violations. Seven settlements were in excess of $1,500,000. (OCR HIPAA Enforcement: Summary of 2016 HIPAA Settlements, HIPAA Journal, 01/12/2017).

A prescription for backup and recovery.

Here's your regimen for successful data backup and management:

Regularly back up and be able to dependably restore clinical and business data from devices in both physical and virtual environments at a moment's notice. Your data is an irreplaceable asset that must be reliably and securely preserved with decreasing daily operational overhead.

Minimize restoration time. Successful disaster recovery means having globally searchable secure data as well as fast restores so that you can quickly find and deploy the data you need.

Make data unassailable by thinking ahead about format. Backups are your safety net in case of an attack on your company's system, so they must be stored in a guaranteed immutable format.

Validate critical data every day. Rather than relying on validation sampling, which may require using stale or incomplete data in a restoration, critical data should be validated daily.

Reduce manual effort. Every time a solution is manual, it not only takes time, but it also risks human error... and repetitive tasks are the most prone to that error.

Make storage system updates and data maintenance as easy as possible. Without meeting each of these challenges, your company's data and reputation are at risk.

Rubrik: Just what the doctor ordered.

Rubrik is disrupting the data backup and recovery industry. We give you the peace of mind that your mission critical data is fully protected and accessible at all times so that you can focus on quality patient care. In fact, customers typically achieve an immediate 30-50% capex savings by dumping unnecessary hardware and software solutions.

Rubrik is a single, scalable platform for backup to disaster recovery that securely manages and safeguards data.

Rubrik manages heterogeneous physical devices without vendor-specific plug-ins, methods, or storage formats in both physical and virtual environments through one HTML5-based, responsive interface.

Rubrik Edge extends data protection and management to your remote and branch health clinics. Satellite facilities can deploy the software to backup locally, replicate to a central data center, and archive to the cloud.

Rubrik secures globally searchable data using a Google-like predictive search feature as well as the management of data to protect from data incursions. This allows data to be easily and instantly accessible as well as secure.

Rubrik's declarative policy engine dramatically reduces ongoing manual effort by allowing administrators to create service level agreements (SLAs) that easily define data protection frequency, retention, archiving, and more in far fewer steps than previous alternatives, reducing your Recovery Time Objectives (RTOs) from hours to just minutes.

Save lives. Rubrik's got your back(up). Learn more about the technology and our products on our website.