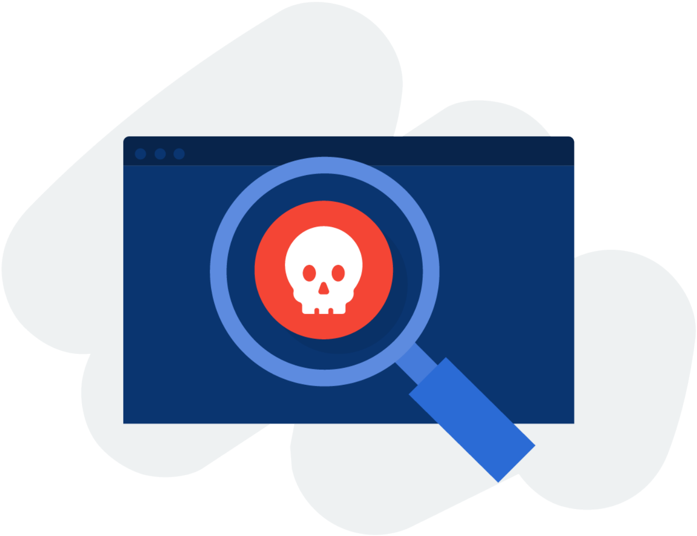
Like preventing an illness rather than curing it, planning for business continuity beats improvising in the face of a hack or disaster

As a healthcare company, your patients are your number one priority. Part of your obligation to them is to keep their health-related information secure and protected.

This information can include the patient's health history, insurance details, and financial information. Recent waves of government regulation have strongly encouraged the digitization of medical records, while at the same time threatening severe penalties for any healthcare organization that fails to protect the confidentiality of that information. While fines and damage to your business and its reputation resulting from a breach would be a nightmare, you should be equally concerned about the loss of access to this data, which would cripple your ability to provide healthcare services. Given that lives could hang in the balance for lack of access to a patient's medical history, there is no time to waste.

Unfortunately, because the healthcare industry is considered so vulnerable, it is a target for cyber attacks. One of the most pernicious tactics, ransomware, doesn't necessarily steal data but encrypts it in place with a key only the attacker possesses. By depriving you of your own data, and that of your patients, the attackers seek to extort you into paying whatever they demand.

For all of these reasons, some of the same regulations that penalize healthcare data breaches also spell out the need for healthcare business continuity and disaster recovery plans, including technologies to backup, secure, and restore data. Loss of healthcare data is simply unacceptable. That's as true in the event of a fire, flood, or natural disaster as it is for cyber attacks.



On the other hand, keeping your patient data properly backed up and protected will help you focus on what matters – the patients you care for.

A False Sense of Security

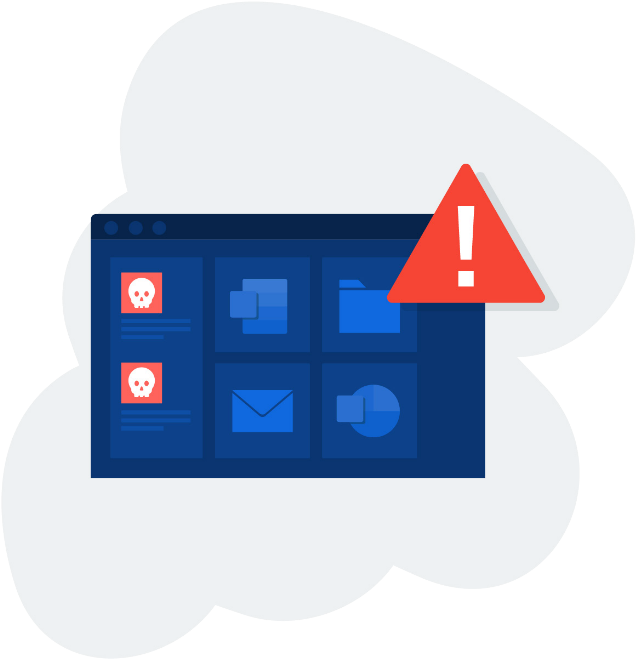
While you may be taking some precautions, such as making a daily backup, that's not enough. Years ago, sure, backing up data once a day was the best practice. Today, it's outdated, partly because businesses rely so much more on computerized data and partly because better options are available. Instead, data should be backed up on an ongoing basis, many times throughout the day.

There are several reasons a daily backup is inadequate:

- If you forget to perform the backup or the backup process fails, you're not protected.
- If you back up your files only once a day, you're left vulnerable to the loss of an entire day's work.
- If you don't properly validate your backup files, you could be in for an unpleasant surprise when you try to restore your company's operational systems from corrupted or incomplete backups.
- If you back up your files to an on-site location only, you could lose them too – leaving you with no with no recourse.
- *What* you backup is critical, too. If you back up only documents and data, rather than all your application and server configuration files, it could take days to restore your business or practice after a disaster or major system

failure. That is because you will also have to rebuild your servers, operating systems, applications, and so on. Even frequent, incremental backups may not be trustworthy if their integrity hasn't been verified. If only 9 out of 10 snapshot backups are correct, having nine-tenths of the puzzle won't be good enough to restore a critical workstation
or server.

Because there's a lot that can be missed when implementing a backup strategy, it's important to get it right the first time.



In 2020, a healthcare data breach cost $7.13 million USD, on average

How Vulnerable Are You?

If your company identifies as a business that doesn't have the IT resources to recover effectively from a major outage, make sure you weigh all the factors around the costs of downtime.

Consider these facts:

- A 2020 study by IBM and the Ponemon Institute1 found, for the 10th year in a row, that healthcare organizations incur the highest cost from a data breach, averaging $7.13 million.[1] Despite reporting in US dollars, the study was global, finding that the cost of a breach was particularly high in the U.S. — averaging $8.64 million, across all industries. However in 12 of 16 countries studied, the cost of a breach was higher than it was the year before — with Brazil experiencing a hefty 29 percent increase.
- Attacks involving ransomware or data-destroying malware were even more costly than the average breach because of the cost of lost business, according to the IBM/Ponemon researchers.

- A National Cyber Security Alliance report found that for businesses with fewer than 500 employees that suffered a data breach, 10 percent went out of business, 25 percent had to file for bankruptcy and 37 percent experienced a financial loss.[2]

Best Practices for Healthcare IT

Whether ransomware, natural disasters, fires, or corrupt employees deleting or altering data to cover up fraud worry you the most, you can take basic precautions to safeguard your data:

- Outsource your company's IT to an expert who has experience in the healthcare industry.
- Find a company educated in HIPAA with a team that's dedicated to security and compliance.
- Ask for references so you can hear from fellow healthcare professionals about their experience with the company.

Any company that has not recently re-assessed its backup and disaster recovery procedures should do so to conform to the industry-standard best practices.

- Don't sacrifice quality to save money when choosing a backup and recovery solution. In the long run, it will benefit you (and your bottom line) to have strong technology.
- Perform timely hardware and software updates, maintenance, and backups.
- Establish, review, and maintain system security of all practice technology.

If you can't attend to these details yourself, make sure you hire an IT service provider you trust to obsess over them on your behalf.

The Better Way: Business Continuity

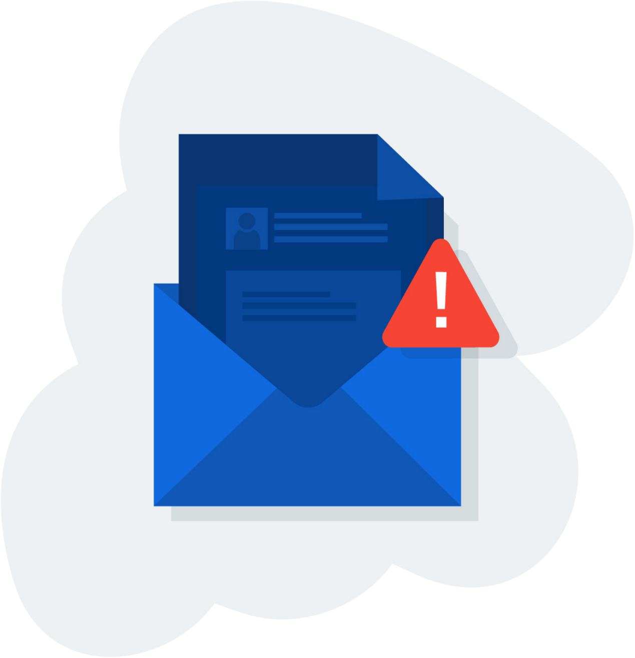
Business continuity describes a complete solution for backup and disaster recovery. A true business continuity and disaster recovery (BCDR) solution protects data on-premises and in the cloud. Whether data is on servers or in SaaS applications, it must be backed up. Business continuity goes a step further and offers you the ability to restore your data quickly, to a different location or the cloud if necessary.

Whether a business is faced with a natural disaster or one that is man-made, a strong solution will have you up and running in minutes. Solutions with a hybrid cloud design — including both local and remote virtual computing resources — can guarantee a quicker restore time as well.

Why? Local backups are great to keep data close at hand and ready to restore to local systems. However, if something happens to that local backup, then what? Cloud backup adds the protection of moving your backups to an offsite location, but bandwidth issues mean retrieving data from a cloud backup can be time consuming. A hybrid cloud backup solution takes an initial backup on a local device and then replicates the backup to a cloud server for a best-of-both-worlds solution. That's intelligent business continuity.

Because we serve healthcare businesses that are increasingly digital, under attack, and potentially vulnerable to disaster, we have partnered with Datto, a specialist in hybrid cloud BCDR. The Datto Cloud is immutable, protected against ransomware as well as accidental or malicious deletion of important files and emails.

Take it from a healthcare company that survived a data crisis that could have been fatal to its business. When their pharmacy fell victim to a destructive robbery, the team at Complete Pharmacy Care was able to get back to business thanks to their Datto business continuity solution.



> **Because of the physical damage, had we not been on the cloud we absolutely would have gone bankrupt because it would have taken us six weeks to rebuild all of the equipment. But because we could get on the cloud, we brought in laptops and dialed into the cloud and were able to start servicing patients by Tuesday. We were only down one day. Had we not had a second copy of our data already up in the cloud, we would not be having this conversation."**
>
> – Leonard Lynskey, CEO, Complete Care Pharmacy

Want to learn more about how we can protect your data, your business, and your patients? **Contact us today.**

1. IBM and the Ponemon Institute, available at https://www.ibm.com/security/services
2. Small Business Cybercriminal Target Survey Data, National Cybersecurity Alliance https://staysafeonline.org/small-business-target-survey-data/