

PHILIPS

HealthSuite Imaging



Data Protection

Safeguard your medical imaging data in the cloud

At the heart of every medical institution lies a wealth of diagnostic imaging data that serves as a historical record of a patient's health journey and informs current and future medical decisions. This patient care lifeline enables clinicians to make timely, accurate diagnoses, monitor treatment progress and ultimately, help improve patient outcomes.

Maintaining the security of this data is paramount, even in the face of unforeseen catastrophic events – like floods, fires and earthquakes – and ever-looming malicious cyberthreats. Ensuring the preservation and accessibility of medical imaging data is not merely a matter of operational continuity – it's a commitment to patient safety and the delivery of quality care.

Healthcare providers may not always have a proper backup process in place, or if they do, still often rely on on-site infrastructure to back up imaging data. This approach shows limitations that can include:



Medical imaging contributes a significant portion of healthcare data, and it's essential to maintain security during distribution and storage. The healthcare sector – and particularly medical imaging – has been the target of cyberattacks. A 2021 report found that 34% of healthcare organizations experienced a ransomware attack in a one-year span.¹

Cybersecurity breaches can lead to exposure of private patient health information on the internet and potentially harm patients if networked medical devices are compromised.²

HealthSuite Imaging Data Protection service

Offering unparalleled security and resilience against disasters of all kinds, Philips HealthSuite Imaging Data Protection is a cloud-based service designed to protect and preserve your medical imaging data and PACS system. It empowers your healthcare organization to mitigate risks, uphold regulatory compliance and most importantly, uphold your promise to patients to deliver care without compromise.

This software as a service is available to on-premises Philips PACS customers and uses the reliable and secure Philips Cloud solution that leverage AWS storage technology and security.

Philips leverages AWS Simple Storage Service (S3), designed to provide resiliency, availability and 99.999999999% durability. It's highly secure and guarantees encryption in transit and at rest. It also ensures specific healthcare regulatory compliance with:

- **50+ global compliance and certifications**
- **135+ HIPAA-eligible services**
- **137+ HITRUST certified services**



The data recovery process

If a disaster or cybersecurity threat causes partial or complete data loss:

- Philips will enable the data recovery from the cloud to the on-premises Philips PACS
- Recovery time will depend on physical damage (in case of natural disaster) integrity of the system (in case of virus cyberthreat), and extent of the data loss, the volume of lost data and the network characteristics between your organization and the cloud
- Data recovery will start 12-24 hours from when the request is made
- Recovery will be conducted according to the customer's priority order

Benefits of HealthSuite Imaging Data Protection

Gain the peace of mind that your medical imaging data will be protected and can be restored if necessary. Our goal is to help you:

- Trust the integrity of your cloud backed up data
- Free your organization from the cumbersome management and difficult testing of on-site backup solution
- Eliminate the need and related burden of procuring, sizing and maintaining local, long-term storage hardware
- Control costs and pay as you go, pay as you grow, for the volume of data you need to protect today

At a time when healthcare requires bolstered vigilance against cyberthreats, rely on Philips as your trusted partner for safeguarding your medical imaging data, while you focus on what matters most: patient care.

1. Global Cloud based Medical Imaging Informatics Market Forecast to 2026
2. The Diagnostic Imaging Equipment Service Outlook Report from 2020

