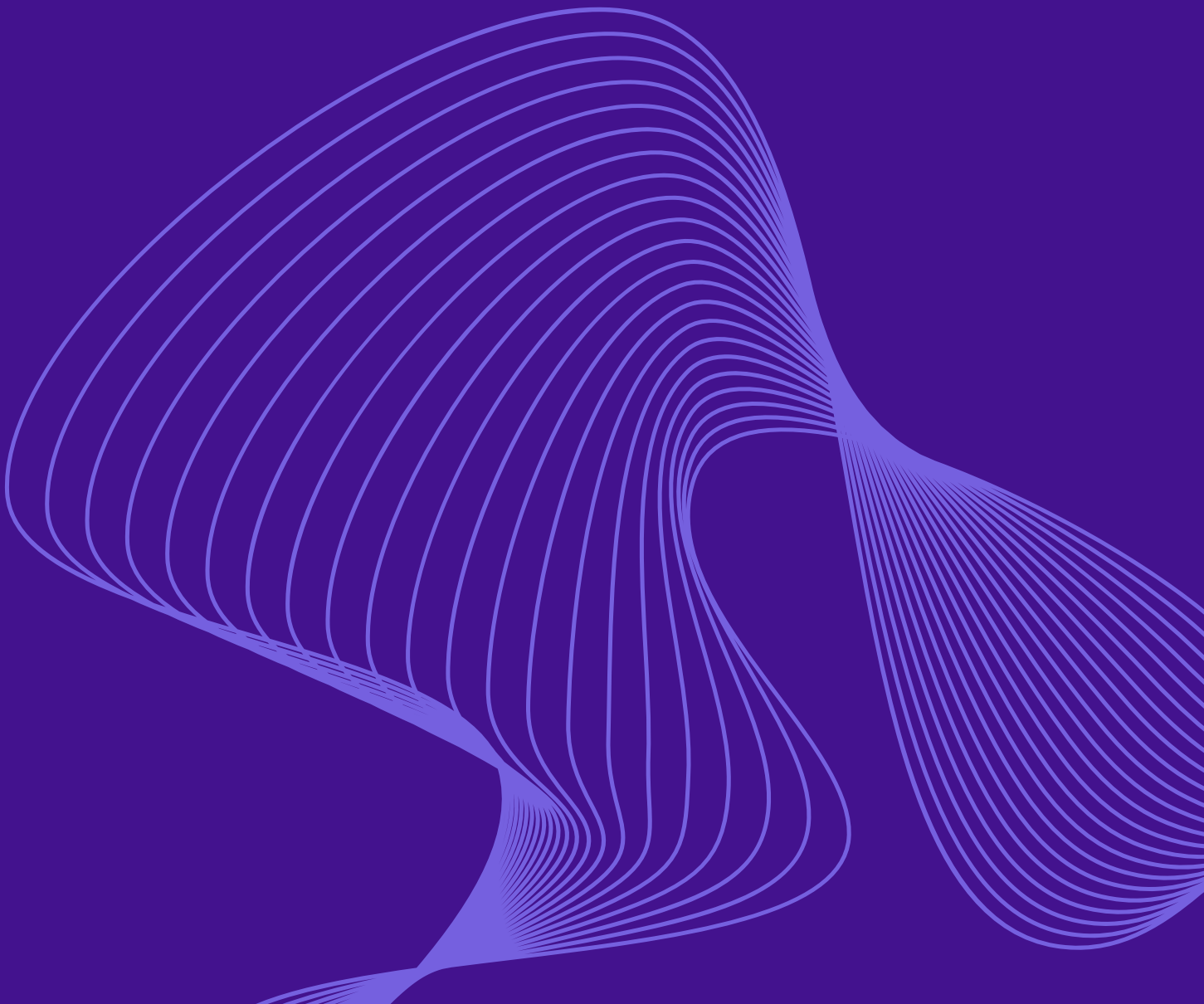





Data Protection Checklist

for Healthcare IT Professionals





As an IT administrator, director, or manager in the healthcare industry, protecting sensitive patient data across both on-premises and cloud environments is crucial. This checklist will help you prepare for potential data loss scenarios and implement a robust backup and recovery strategy.

01 STEP

Map Your Healthcare Data Ecosystem and Identify Risks

Healthcare organizations often utilize a hybrid infrastructure with both on-premises and SaaS applications. Follow these steps to gain visibility into your entire data estate:

- Catalog all on-premises systems, including legacy applications and databases
- Map out all SaaS applications and cloud services used across your healthcare facility
- Examine platforms like AWS or Azure to identify all associated healthcare apps
- Categorize applications by hospital departments (e.g., radiology, pharmacy, billing)
- Identify both on-prem and cloud-based apps and their shared responsibility model
- Address shadow IT by requiring staff to register all applications in use

02 STEP

Implement Comprehensive Data Protection and Recovery Measures

To protect against data breaches, ransomware attacks, or accidental deletions, ensure your data is recoverable across all environments:

- Schedule frequent backups: Implement daily backups at minimum for both on-premises and cloud systems, considering more frequent backups for critical patient data
 - Enable granular restore capabilities: Ensure you can recover specific configurations or user data without full system rollbacks, regardless of data location
 - Implement post-restore security measures: Reset all passwords after a restore to maintain data integrity across all systems
 - Maintain comprehensive audit trails: Keep 24/7 logs and event tracking for all healthcare applications, both on-premises and in the cloud
 - Set up alerting systems: Enable notifications for all activities, especially those involving sensitive patient information, across your entire infrastructure
 - Establish access controls: Implement role-based access control (RBAC) for backup and recovery operations to limit exposure in all environments
 - Conduct regular recovery drills: Test your recovery process frequently for both on-premises and cloud systems to ensure it meets healthcare compliance standards and minimizes downtime
-

03

STEP

Healthcare-Specific Considerations

- **HIPAA Compliance:** Ensure your backup and recovery solutions meet HIPAA requirements for data protection and privacy across all environments
- **Electronic Health Records (EHR) Systems:** Pay special attention to EHR systems, whether on-premises or cloud-based, as they contain critical patient data and require stringent protection
- **Telemedicine Platforms:** Include telemedicine applications in your protection strategy, considering both on-premises infrastructure and cloud-based solutions
- **Medical Imaging Systems:** Implement backup solutions for medical imaging data, which can be large in size and may reside on local servers or in the cloud
- **Pharmacy Management Systems:** Protect pharmacy systems, both on-premises and cloud-based, to ensure continuity of medication management and prevent prescription errors.


04

STEP

Best Practices for Healthcare IT Data Resilience

- **Data Encryption:** Implement end-to-end encryption for all backed-up healthcare data, both in transit and at rest, regardless of storage location
- **Disaster Recovery Planning:** Develop a comprehensive disaster recovery plan that addresses both on-premises and cloud-based systems
- **Staff Training:** Regularly train healthcare staff on data protection best practices for both local and cloud-based applications
- **Vendor Assessment:** Evaluate the data protection capabilities of your IT vendors, ensuring they meet healthcare industry standards for both on-premises and cloud solutions
- **Compliance Monitoring:** Continuously monitor and audit your data protection measures across all environments to ensure ongoing compliance with healthcare regulations

By following this checklist, healthcare IT professionals can significantly improve their organization's resilience against data loss across both on-premises and cloud environments, ensuring uninterrupted patient care and maintaining the integrity of critical healthcare information systems.





Take control of your data



GET STARTED