

10

Privacy and security questions to ask your future data archiving partner to make sure your data is safe.

When going through a data migration, finding a legacy data archiving partner you can trust is a critical piece of the puzzle. We've put together a list of ten questions for you to ask during vendor selection that will make you feel certain you are investing in a partner that will protect you and your data.



1 Do you have a full time Privacy and Security Officer and/or Compliance Officer on staff?

With so much at stake, it is appropriate to expect and verify that a senior level resource is dedicated to managing security and privacy 100% of the time.

1

2

2 Will your ePHI and PII be stored within a Tier III (or higher) SOC 2-certified data center?

The classification of the data center is pertinent to data security but also to ensure the product will operate at the up-time levels a healthcare provider requires.



3 Have you committed to security excellence by obtaining a HITRUST or other CSF Certification?

This sort of credentialing is voluntary and can be indicative of their priorities when it comes to data security. Ask if they've taken the time and resources to achieve this certification.

3

4

4 Have you made a formal commitment to employee security training and awareness?

Ensuring protection against the latest threats to your healthcare data is a moving target. Ask how their workforce maintains its HIPAA knowledge base and stays ahead of the curve.



5 What is your process to maintain privacy and security policies and procedures?

Their policies and procedures should be reviewed and updated routinely in order to keep up with the changes in policy and risk management best practices.

5

6

6 Will our data be fully secure while in transit and at rest, with a framework in place to monitor endpoints and respond to threats?

With lots of data to manage, it is critical to protect it at every stage—24 hours a day, 365 days a year. Ask about their security framework for this process.



7 What are your data validation standards to ensure data retention requirements are met?

Ask your archiving partner about the process for ensuring 100% data integrity through automated and manual validation processes.

7

8

8 Do you offer features such as Single Sign-On and role-based security?

Features that allow easy clinical access to data and allow for monitoring of security enhance the overall security of your archive. Ask about break the glass.



9 Does your archive solution contain robust audit solutions like FairWarning® to monitor initial and ongoing access?

Push beyond the general assurances and ask about how data will be tracked at each stage of user access. Can they send their audit logs, automatically, to one integrated audit product?

9

10

10 Do you carry adequate Cyber Security Insurance to protect all parties involved?

As stewards of your data, a good data archiving vendor will be prepared to cover you and themselves in the event of a breach.

