Checklist for

MINIMIZING RISK OF DATA BREACHES IN YOUR HEALTHCARE ORGANIZATION

Use this checklist to make sure your data isn't left vulnerable to the increasing number of risks hospitals and health systems will continue to face in 2021 and for years to come.

- □ Regularly analyze risk factors present in your organization and create strategies for both prevention and response.
- □ Choose only trusted third party vendors with serious precautions against data breaches in place across their organization.
- □ Archive legacy data with a solution that enables payment collection, access to data, and long-term storage.
- □ Secure your IT infrastructure with updated hardware or, if no security patches are available, a new system that is on par with current security standards.
- □ Provide ongoing training to all staff to keep them updated with current HIPAA regulations—and the consequences of violating them. Staff should also be taught to keep devices and paper records out of the wrong hands, log on and off of shared devices, and recognize and report potential security threats.
- □ Restrict access to private data from anyone that doesn't need it to do their job. This is an often overlooked but essential component of data protection.
- □ Keep your organization's internet connection secure by creating a separate wireless network for guests.

Retiring data is a simple but essential part of a data security strategy in 2021. With patient data volumes increasing rapidly, more and more data will be at risk. Whether you need to archive now or your best next step is to outline a strategy for six to twelve months from now will depend on a unique combination of factors.

Not sure what your next move is? Take our quiz to find out when you should implement data archival at your healthcare organization.

TAKE THE QUIZ AT
www.legacydataaccess.com/quiz

Legacy Data Access