Consider using this checklist for considering any new cloud storage service.

All devices are password-protected and settings enable the devices to lock and require a password immediately when unused. Ideally, devices are locked with passwords or passphrases rather than simple four-digit pin codes.

Review the Service Level Agreement, Terms of Services, and Privacy Policies—often there are several documents which form the cloud service contract.

Make sure you understand how data is managed by the hosted service provider.

Can you expect to receive notice for any changes in the service? How much notice will you have, and will you be able to obtain your data if you do not agree to new terms?

The hosted service provider should use third-party auditors to test its security systems, and the results should be publicly available.

Understand the hosted service provider’s breach notification policies, and how it notifies or responds to service outages. What type of notice will you receive, and how long after a breach would you be notified?

Service or application encrypts data “at rest” and “in transit,” OR you are utilizing a third-party software to provide encryption “at rest” that is compatible with your cloud service.

Service or application encrypts at a minimum of 128-bit encryption (preferably 256-bit).

Service allows lengthy passwords (at least 20 characters).

Service permits two-factor authentication (preferably with an authenticator app such as Google’s Authenticator) and remote wipe.

Research the service (web searching is fine) to discover any well-known concerns. Suggested search terms (along with the service/company name) include “security risk,” “vulnerability,” “data breach,” “audit,” “confidentiality,” “security issues.

Understand the hosted service provider’s policies regarding data access if your account is closed or payments are interrupted. Will clients be able to access shared files? Will you still be able to access your data?