Data Protection For Microsoft (Office) 365 Subscription Users

Microsoft (Office) 365 is a suite of subscription products that include Word, Excel, PowerPoint, OneNote, Outlook, Publisher and Access. In addition, bundled into each subscription package is "cloud storage" generally known as Microsoft OneDrive (or SharePoint for Business).

Cloud storage is used to store documents online – making them accessible to any device connected to the Internet and authenticated to the subscription service. Cloud-based file synchronization makes thec combination of Microsoft 365 + OneDrive a widely-used tool for team collaboration.

Dr.Backup clients who are refreshing their technology platform and moving to this new subscription model should understand that:

1. **Microsoft standard service terms and conditions say explicitly that they are not liable** for any disruption or loss you may suffer as the result of an event (data loss) or outage. They explicitly instruct you to "**regularly backup your content and data on the services or store using third-party apps and services.**" (Microsoft Services Agreement - Service Availability, Section 6 – Ref: https://www.microsoft.com/en-us/servicesagreement)

2. Use of Microsoft 365/OneDrive **IS NOT A SUBSTITUTE FOR PROPER DATA PROTECTION AND BACKUP PROCESSES**. Relying solely on the cloud storage repository included in Microsoft 365 puts your business at serious risk and ignores the recommendations of the **U.S. CERT (Computer Emergency Readiness Team) – specifically the "Backup 3-2-1" rule for business.** This rule says always keep at least 2 different data backups stored in separate places with at least one offsite. Ref: https://drbackup.net/whitepapers/DrBackup-Data_Backup_Options-3-2-1.pdf

3. **If your organization is required to comply with HIPAA regulations and the HITECH Act,** there are multiple steps you must take before storing ePHI in Microsoft's 365 cloud storage -- including **execution and compliance with the Microsoft HIPAA Business Associate Agreement** (BAA). You must also implement appropriate privacy and security controls including access tracking, disabling of data sharing functions and the regular review of control reports. **Even with these features in place and properly configured and monitored, you still need to meet the business continuity requirements HIPAA outlines – which means securely back up your data.** Ref: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

IMPORTANT: For the above reasons (and more) when adopting Microsoft (Office) 365, the one thing you definitely **do NOT want to do is cancel your "Done-For-You" cloud and local backup services** provided by **Dr.Backup** – since the equivalent capabilities are NOT provided by Microsoft.