

Checkliste: IT-Datensicherheit in der Medizin

1. Datenschutz & DSGVO-Konformität

- ☐ Haben Sie ein vollständiges Verzeichnis der Verarbeitungstätigkeiten für alle IT-Systeme?
- ☐ Sind Ihre Mitarbeitenden regelmäßig zu Datenschutzthemen geschult?
- ☐ Liegen aktuelle AV-Verträge mit Microsoft und anderen IT-Dienstleistern vor?
- ☐ Existiert ein dokumentiertes Löschkonzept mit definierten Fristen?
- ☐ Werden Patienten schriftlich über die Datenverarbeitung informiert (Datenschutzerklärung)?

2. E-Mail-Sicherheit & Archivierung

- ☐ Nutzen Sie einen professionellen Spam- und Phishing-Filter für eingehende E-Mails?
- ☐ Ist Ihre E-Mail-Kommunikation standardmäßig TLS-verschlüsselt?
- ☐ Archivieren Sie E-Mails revisionssicher und gesetzeskonform nach GoBD?
- ☐ Gibt es automatisierte Prüfungen auf gefährliche Anhänge oder Links?
- ☐ Werden kritische E-Mails in Quarantäne verschoben und zentral geprüft?

3. Backup & Wiederherstellung

- ☐ Sichern Sie automatisch alle M365-Daten (Exchange, OneDrive, SharePoint, Teams)?
- ☐ Haben Sie einen Notfall- und Wiederherstellungsplan für IT-Ausfälle?
- ☐ Testen Sie regelmäßig, ob Backups korrekt wiederhergestellt werden können?
- ☐ Speichern Sie Ihre Sicherungen zusätzlich außerhalb der Microsoft-Cloud?
- ☐ Sind Ihre Wiederherstellungszeiten (RTO/RPO) klar definiert und dokumentiert?

4. Technische & organisatorische Maßnahmen (TOM)

- ☐ Ist Multi-Faktor-Authentifizierung (MFA) bei allen Nutzern verpflichtend aktiviert?
- ☐ Werden alle administrativen Aktivitäten protokolliert und regelmäßig überprüft?
- ☐ Arbeiten Sie mit einem Rollen- und Rechtekonzept nach dem Prinzip „Least Privilege“?
- ☐ Werden sicherheitsrelevante Updates regelmäßig installiert?
- ☐ Schränken Sie den Zugriff auf sensible Systeme standort- oder IP-basiert ein?

5. Integration & Benutzerfreundlichkeit

- ☐ Ist Ihre Sicherheitslösung vollständig in Microsoft 365 integriert?
- ☐ Nutzen Sie ein zentrales Dashboard zur Übersicht über alle sicherheitsrelevanten Vorfälle?
- ☐ Ist die Benutzerverwaltung über Azure AD oder ähnliche Dienste automatisiert?
- ☐ Erhalten Sie deutschsprachigen Support, der den medizinischen Bereich kennt?
- ☐ Können Sie mehrere Standorte oder Praxen (Mandanten) zentral verwalten?