SECUREPOINT

IT-SICHERHEITS-CHECKLISTE

SICHERE PRAXIS-IT

IT-SICHERHEITS-CHECKLISTE

NACH PRAXISGRÖSSE

Mögliche Konsequenzen bei Nicht-Beachtung der Sicherheitsrichtlinie

- **Bußgelder und Honorarabzug**: Obwohl derzeit keine spezifischen Honorarkürzungen bei Nichtbeachtung der IT-Sicherheitsrichtlinie vorgesehen sind, können Verstöße gegen die Richtlinie dennoch Konsequenzen haben, insbesondere im Hinblick auf Datenschutzverletzungen und die damit verbundenen Haftungsrisiken. Es wird daher dringend empfohlen, die Anforderungen der IT-Sicherheitsrichtlinie fristgerecht umzusetzen. (§ 390 SGB V).
- **Datenschutzrechtliche Folgen**: Kommt es zu einem Datenschutzverstoß (z. B. durch ungesicherte IT oder Datenlecks), können zusätzliche Bußgelder durch Aufsichtsbehörden nach der DSGVO verhängt werden – diese können empfindlich hoch ausfallen (bis zu 20 Mio. € oder 4 % des Jahresumsatzes).
- **Haftung bei Schäden**: Sollte es z. B. durch mangelnde IT-Sicherheit zu einem Datenverlust, einem Hackerangriff oder einer Betriebsunterbrechung kommen, haftet die Praxis zivilrechtlich – etwa bei Schäden gegenüber Patient:innen oder Kooperationspartnern.
- **Strafrechtliche Relevanz**: Bei grober Fahrlässigkeit oder Vorsatz – etwa dem bewussten Ignorieren gesetzlicher Anforderungen – kann auch eine strafrechtliche Verfolgung (z. B. wegen Verletzung von Berufsgeheimnissen oder unterlassener Hilfeleistung im organisatorischen Sinne) nicht ausgeschlossen werden.

Persönliche Haftung
Die Verantwortung für die Einhaltung der IT-Sicherheitsrichtlinie in einer Arztpraxis liegt grundsätzlich bei der Praxisinhaberin bzw. dem Praxisinhaber – unabhängig davon, ob IT-Aufgaben an einen Dienstleister ausgelagert wurden.

SECUREPOINT

IT-SICHERHEITS-CHECKLISTE

NACH PRAXISGRÖSSE

Die folgende Checkliste basiert auf den KBV-Sicherheitsrichtlinien nach § 390 SGB V (ehemals §75b), Version 1.1, abgerufen am 24.06.2025. In den Klammern () finden Sie den jeweiligen Verweis auf den Punkt der Richtlinie, auf den sich die Frage der Checkliste bezieht.

Nr.	Frage	Erklärung	Hinweis in KBV-Richtlinien	Ja	Nein
Kleine Praxen (bis 5 Personen) Folgende Punkte sind von Praxen aller Größen zu beachten:					
1	**Firewall – Wird eine Firewall genutzt?**	Eine Firewall überwacht und kontrolliert den Datenverkehr zwischen Ihrer Praxis und dem Internet. Sie blockiert unbefugte Zugriffe und schützt Ihre Systeme vor Angriffen von außen.	Anlage 1 Punkt 11		
2	**Firewall Status – Ist diese Firewall nach dem aktuellen Stand der Technik eingerichtet?**	Updates und die passende Konfiguration machen den vollen Funktionsumfang der Firewall nutzbar. Dies betrifft z.B. die Aufteilung von Netzwerken, die Zuweisung von Nutzerrechten und die Einrichtung von Authentisierungsverfahren.	Anlage 1 Punkt 11		
3	**Netzplan – Gibt es eine Dokumentation des Netzwerks?**	Ein Netzplan zeigt, welche Geräte und Systeme miteinander verbunden sind. Er hilft IT-Dienstleistern bei Wartung, Fehlersuche und bei der Einhaltung von Sicherheitsvorgaben. Ohne Dokumentation fehlt Transparenz über kritische Verbindungen.	Anlage 1 Punkt 12		
4	**Einarbeitung – Gibt es eine geregelte Einarbeitung neuer Mitarbeitender?**	Neue Mitarbeitende sollten zu Beginn ihrer Tätigkeit über sichere Arbeitsweisen und interne IT-Regeln informiert werden. Das verhindert versehentliche Sicherheitsvorfälle und sorgt dafür, dass neue Mitarbeitende verantwortungsvoll handeln.	Anlage 1 Punkt 1		

Nr.	Frage	Erklärung	Hinweis in KBV-Richtlinien	Ja	Nein
5	**Engagement der Praxisleitung – Unterstützt die Praxisleitung aktiv die Sensibilisierung für Informationssicherheit?**	Die Praxisleitung trägt Verantwortung dafür, dass IT-Sicherheit ernst genommen wird. Wenn sie Schulungen unterstützt, Sicherheitskampagnen initiiert und selbst mit gutem Beispiel vorangeht, steigt die Wirksamkeit aller Schutzmaßnahmen deutlich.	Anlage 1 Punkt 8		
6	**Anleitungen – Werden Mitarbeitende regelmäßig im sicheren Umgang mit IT geschult?**	Mitarbeitende müssen wissen, wie sie sicher mit IT-Komponenten arbeiten, beispielsweise wie E-Mails signiert werden oder wie man das VPN aktiviert.	Anlage 1 Punkt 9		
7	**Awareness Schulungen – Gibt es regelmäßige Schulungen zur IT-Sicherheit?**	Mitarbeitende müssen wissen, wie sie z. B. Passwörter schützen, Phishing erkennen und Datenverlust vermeiden. Diese Schulungen sind verpflichtend – auch für kleine Praxen.	Anlage 1 Punkt 10		
8	**Updates – Werden regelmäßig alle wichtigen Updates installiert?**	Sicherheitsupdates für Betriebssysteme und Programme schließen bekannte Sicherheitslücken. Ohne regelmäßige Updates steigt das Risiko für Viren und Angriffe erheblich.	Anlage 1 Punkt 14		
9	**Update-Verantwortung – Ist festgelegt, wer für Updates zuständig ist?**	Ein klar Verantwortlicher – ob intern oder extern – sorgt dafür, dass Updates tatsächlich und zeitnah eingespielt werden. Nur so bleibt die IT-Sicherheit gewährleistet.	Anlage 1 Punkt 15		
10	**Altsysteme – Werden Systeme ohne fortlaufende Updates ersetzt oder isoliert?**	Geräte oder Programme, die Seitens der Hersteller keine Sicherheitsupdates mehr erhalten, stellen ein hohes Risiko dar. Sie sollten entweder ersetzt oder so betrieben werden, dass sie vom restlichen Netzwerk getrennt sind.	Anlage 1 Punkt 17		
11	**Virenschutz – Gibt es einen aktuellen Virenschutz auf allen Geräten?**	Antivirensoftware erkennt und blockiert bekannte Schadprogramme. Ein aktueller Schutz auf jedem Gerät ist ein grundlegendes Sicherheitsmerkmal jeder Praxis-IT.	Anlage 1 Punkt 20		
12	**Backups – Werden regelmäßig Sicherungskopien wichtiger Daten gemacht?**	Nur mit regelmäßigen Datensicherungen können Informationen nach einem Vorfall wie einem Systemabsturz oder einem Angriff wiederhergestellt werden.	Anlage 1 Punkt 21		
13	**Backup-Schutz – Ist die Sicherung vor unbefugtem Zugriff geschützt?**	Backups sollten verschlüsselt und gegen physischen Zugriff geschützt aufbewahrt werden, z. B. in einem Tresor oder in einem Cloud-Speicher.	Anlage 1 Punkt 22		

IT-SICHERHEITS-CHECKLISTE

NACH PRAXISGRÖSSE

Nr.	Frage	Erklärung	Hinweis in KBV-Richtlinien	Ja	Nein
14	**Backup-Test – Werden Backups regelmäßig getestet?**	Ein Backup ist nur dann hilfreich, wenn es im Ernstfall auch korrekt funktioniert. Regelmäßige Tests stellen sicher, dass sich die Daten wiederherstellen lassen.	Anlage 1 Punkt 25		
15	**Mobile Sicherheit – Sind mobile Geräte mit PIN oder Code geschützt?**	Mobile Geräte wie Tablets oder Smartphones müssen gegen unbefugten Zugriff gesichert sein – besonders, wenn sie Patientendaten enthalten oder Zugang zum Praxissystem haben.	Anlage 1 Punkt 32		
16	**App-Rechte – Sind App-Zugriffe auf Daten eingeschränkt?**	Viele Apps fragen unnötige Berechtigungen an. Diese sollten so restriktiv wie möglich vergeben werden, um den Datenschutz zu wahren.	Anlage 1 Punkt 33		
17	**Sperrung bei Verlust – Können Sie Mobilgeräte aus der Ferne sperren?**	Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden, um Missbrauch vorzubeugen.	Anlage 1 Punkt 34		
18	**USB-Kontrolle – Werden Wechseldatenträger geprüft und gelöscht?**	USB-Sticks und externe Festplatten können Schadsoftware enthalten oder versehentlich vertrauliche Daten transportieren. Sie sollten bei Verwendung mit einem gezielten Scan durch das Antiviren-Programm geprüft und nach Gebrauch gelöscht werden.	Anlage 1 Punkt 36		
19	**E-Mail-Schutz – Wird E-Mail-Verkehr durch Viren- und Spamfilter geschützt?**	Bei der Konfiguration von E-Mail-Clients sollten Dateianhänge vor dem Öffnen auf Schadsoftware geprüft, die automatische Interpretation von HTML-Code und aktiven Inhalten deaktiviert und für die Kommunikation über unsichere Netze eine sichere Transportverschlüsselung verwendet werden.	Anlage 1 Punkt 40		
20	**Spamverhalten – Werden verdächtige E-Mails ignoriert und gelöscht?**	Mitarbeitende sollten keine Links oder Anhänge aus unbekannten E-Mails öffnen. Diese Sensibilisierung ist ein wesentlicher Teil der IT-Sicherheitskultur.	Anlage 1 Punkt 41		

Nr.	Frage	Erklärung	Hinweis in KBV-Richtlinien	Ja	Nein
Mittlere Praxen (6 bis 20 Personen) Zusätzlich zu den Fragen der kleinen Praxen sind folgende Punkte zu beachten:					
21	**Verschlüsselte Kommunikation – Werden E-Mails oder Datenübertragungen verschlüsselt?**	Die Übertragung sensibler Daten sollte stets verschlüsselt erfolgen – z. B. per TLS bei E-Mail-Kommunikation. Nur so ist sichergestellt, dass keine Dritten mitlesen können.	Anlage 2 Punkt 2		
22	**Zugriffsrechte – Sind Zugriffsrechte klar geregelt und beschränkt?**	Jede Person sollte nur Zugriff auf die Daten erhalten, die sie wirklich benötigt. Diese Beschränkung reduziert das Risiko von Fehlern und Datenmissbrauch.	Anlage 2 Punkt 2		
23	**Mobile-Richtlinie – Gibt es eine Nutzungsrichtlinie für mobile Geräte?**	Einheitliche Regeln für mobile Endgeräte helfen dabei, Sicherheitslücken zu vermeiden und den Umgang mit dienstlichen Informationen klar zu regeln.	Anlage 2 Punkt 5		
Große Praxen (über 20 Personen oder umfangreiche Datenverarbeitung) Zusätzlich zu den Fragen der kleinen und mittleren Praxen sind folgende Punkte zu beachten:					
24	**Netzsegmentierung – Ist das Netzwerk in Sicherheitsbereiche unterteilt?**	Eine Trennung sensibler Datenbereiche vom restlichen Netzwerk stellt sicher, dass im Fall eines Angriffs nicht alle Systeme betroffen sind. Dies ist insbesondere bei großen Praxen mit komplexen IT-Strukturen wichtig.	Anlage 3 Punkt 2		
25	**Mobile Device Management (MDM) – Werden mobile Geräte zentral verwaltet?**	Ein Mobile Device Management erlaubt es, Richtlinien zentral durchzusetzen, Geräte bei Verlust aus der Ferne zu sperren und Updates automatisch zu verteilen.	Anlage 3 Punkt 7		
26	**Zertifikatsverwaltung – Werden Zertifikate für Mobilgeräte zentral verwaltet?**	Zentrale Verwaltung von digitalen Zertifikaten für Dienste wie E-Mail oder VPN auf mobilen Geräten verhindert Manipulation und sorgt für eine sichere, einheitliche Infrastruktur.	Anlage 3 Punkt 9		

SECUREPOINT UNIFIED SECURITY

Cyberkriminalität entwickelt sich ständig weiter. Neue Angriffsvarianten, menschliches Fehlverhalten und technischer Fortschritt stellen Unternehmen und öffentliche Einrichtungen vor immer neue Herausforderungen.

Um den unterschiedlichsten Bedrohungen wirksam zu begegnen, setzt Securepoint auf das Prinzip der „Unified Security". Das bedeutet: Verschiedene, sich ergänzende und verstärkende Schutzmaßnahmen werden Schicht für Schicht kombiniert, sodass ein ganzheitlicher Abwehrmechanismus entsteht.

UTM-Firewalls
Das Fundament der Netzwerksicherheit
- Exzellenter Content-Filter
- Schutz vor Viren und Trojanern
- Anti-Spam-Funktionen
- Modelle für 1–2.000 User
- Zum Kauf oder „as a Service"

Antivirus Pro
Der Antivirus für Unternehmen
- Hochleistungsfähige Scan-Engine
- Schnell und ressourcenschonend
- Verwaltung aus der Cloud

Mobile Security &
Device Management
- Sicherheit für Smartphone und Tablet
- Volles Mobile Device Management
- Verschlüsselte Verbindungen

Awareness Next
Das Cybersecurity-Training
- Macht Mitarbeitende zur „Human Firewall"
- KI-basierte Phishingvorlagen
- Individuelles E-Learning
- Datenschutzkonforme Auswertung

Cloud Shield
Schutz für Netzwerke und Geräte
- Schutz für Netzwerke und Geräte
- DNS-Check und verschlüsselte Verbindungen
- Firewall, Filter und Geo-IP-Blocking
- Jugendschutz und Sperrfunktionen
- Verwaltung über Online-Portal

SCHICHT FÜR SCHICHT ZU MEHR SICHERHEIT

SecurITy made in Germany

SecurITy Trust Seal www.teletrust.de/itsmie made in EU

Änderungen und Irrtümer vorbehalten. Stand: 10.07.2025

Securepoint GmbH
Bleckeder Landstraße 28
21337 Lüneburg

Tel.: +49 (0)4131 / 24010
info@securepoint.de
www.securepoint.de

SECUREPOINT