ChecklistGuro

Checkliste Für Die IT-Sicherheit Im Gesundheitswesen: Datenschutz Und Zugriffskontrolle

Datenverschlüsselung und -speicherung

Sicherstellung des Schutzes sensibler Patientendaten, sowohl im Ruhezustand als auch während der Übertragung.

Verwendete Verschlüsselungsmethode (gespeicherte Daten)

- [ ] AES-256
- [ ] Triple DES (oder 3DES)
- [ ] Sonstiges (bitte angeben)

Verwendete Verschlüsselungsmethode (Datenübertragung)

- [ ] TLS 1.2 oder höher
- [ ] SSL 3.0
- [ ] Sonstiges (bitte angeben)

Häufigkeit der Schlüsselrotation für die Verschlüsselung (in Tagen)

Eine Zahl eingeben...

Beschreibung der Datenspeicherorte

Etwas schreiben...

Datenmaskierung implementiert?

- [ ] Ja
- [ ] Nein
- [ ] Teilweise

Richtliniendokument für die Verwaltung von Verschlüsselungsschlüsseln

Upload File

Zugriffskontrolle und Authentifizierung

Verwaltung von Benutzerberechtigungen und Überprüfung von Identitäten.

Ist die Multi-Faktor-Authentifizierung aktiviert?

- [ ] Ja
- [ ] Nein.
- [ ] Teilweise Implementierung

Sind die Anforderungen an die Passwortkomplexität angewendet worden?

- [ ] Ja
- [ ] Nein
- [ ] Überprüfung erforderlich

Maximale Passwortlaufzeit (in Tagen)

Eine Zahl eingeben...

Häufigkeit der Überprüfung von privilegierten Zugriffsrechten

- [ ] Monatlich
- [ ] vierteljährlich
- [ ] Jährlich
- [ ] Ad-hoc

Rollenbasierte Zugriffskontrolle (RBAC) implementiert für:

- [ ] Elektronische Patientenakte/Elektronische Krankenakte
- [ ] Finanzsysteme
- [ ] Labormanagementsysteme
- [ ] Bildgebungssysteme
- [ ] Sonstiges (bitte angeben)

Datum der letzten Überprüfung der Zugriffskontrollen

Datum eingeben...

Hinweise zu Zugriffskontrollprozessen

Etwas schreiben...

Netzwerksicherheit

Schutz der Netzwerkinfrastruktur vor unbefugtem Zugriff und Bedrohungen.

Status der Firewall

- [ ] Aktiv
- [ ] Inaktiv
- [ ] Wartungsmodus

Anzahl der Firewall-Regeln

Eine Zahl eingeben...

Status des Intrusion Detection Systems (IDS)

- [ ] Aktiv
- [ ] Inaktiv
- [ ] Ausstehende Benachrichtigungen zur Überprüfung

Zusammenfassung der aktuellen Netzwerkaktivitätsprotokolle

Etwas schreiben...

VPN-Status

- [ ] Aktiviert
- [ ] Deaktiviert
- [ ] Aktive Verbindungen: 0

Datum der letzten Netzwerksicherheitsprüfung

Datum eingeben...

Wurde eine Netzwerksegmentierung implementiert?

- [ ] VLANs
- [ ] Mikrosegmentierung
- [ ] Firewall-Regeln
- [ ] Keine

Endgerätesicherheit

Sicherung der Geräte, die auf Gesundheitsdaten zugreifen, einschließlich Computern, Tablets und Mobiltelefonen.

Ist eine Endpoint-Schutzsoftware installiert?

- [ ] Ja
- [ ] Nein.
- [ ] Nicht zutreffend

Status der letzten vollständigen Scan-Durchführung (0 = fehlgeschlagen, 1 = erfolgreich)

Eine Zahl eingeben...

Datum der letzten Installation eines Sicherheitspatchs

Datum eingeben...

Wurde eine Lösung für die Verwaltung mobiler Geräte (MDM) implementiert?

- [ ] Ja
- [ ] Nein
- [ ] Nicht zutreffend

Welche der folgenden Sicherheitsmaßnahmen für Endgeräte sind implementiert?

- [ ] Antivirensoftware
- [ ] Firewall
- [ ] Datensicherheitsrichtlinien (Data Loss Prevention, DLP)
- [ ] Festplattenverschlüsselung
- [ ] Funktion zum Fernlöschen von Daten

Beschreiben Sie alle ungewöhnlichen Verhaltensweisen von Endgeräten, die kürzlich beobachtet wurden.

Etwas schreiben...

Schwachstellenmanagement

Identifizierung und Behebung von Sicherheitslücken in Systemen und Anwendungen.

Datum der letzten Schwachstellenprüfung

Datum eingeben...

Scan-Häufigkeit (in Tagen)

Eine Zahl eingeben...

Zusammenfassung der aktuellen Scan-Ergebnisse

Etwas schreiben...

Sind kritische bzw. schwerwiegende Sicherheitslücken entdeckt worden?

- [ ] Ja
- [ ] Nein.
- [ ] Ausstehender Scan

Beschreibung der Schritte zur Behebung von schwerwiegenden Sicherheitslücken

Etwas schreiben...

Geplantes Datum für den Abschluss der Fehlerbehebung

Datum eingeben...

Verwendetes Tool zur Schwachstellenanalyse

- [ ] Nessus
- [ ] Qualys
- [ ] Rapid7
- [ ] Sonstige

Anhang zum Scan-Bericht (optional)

Upload File

Reaktion auf Vorfälle und Wiederherstellung

Effektive Planung und Reaktion auf Sicherheitsvorfälle.

Datum/Uhrzeit des Beginns des Vorfalls

Datum eingeben...

Kurze Beschreibung des Vorfalls

Etwas schreiben...

Schweregrad des Vorfalls (gering, mittel, hoch, kritisch)

- [ ] Niedrig
- [ ] Mittel
- [ ] Hoch
- [ ] Kritisch

Geschätzte Anzahl der betroffenen Datensätze

Eine Zahl eingeben...

Betroffene Systeme (Bitte alle zutreffenden Optionen auswählen)

- [ ] Elektronische Patientenakte
- [ ] Abrechnungssystem
- [ ] Patientenportal
- [ ] Netzwerkinfrastruktur

Durchgeführte Maßnahmen zur Eindämmung

Etwas schreiben...

Durchgeführte Maßnahmen zur Beseitigung

Etwas schreiben...

Datum der Bestätigung der Wiederherstellung

Datum eingeben...

Datensicherung und Notfallwiederherstellung

Implementierung von Strategien, um die Datenverfügbarkeit im Falle von Systemausfällen oder Katastrophen sicherzustellen.

Häufigkeit der Datensicherung (z. B. täglich, wöchentlich)

Eine Zahl eingeben...

Datum der letzten erfolgreichen vollständigen Datensicherung

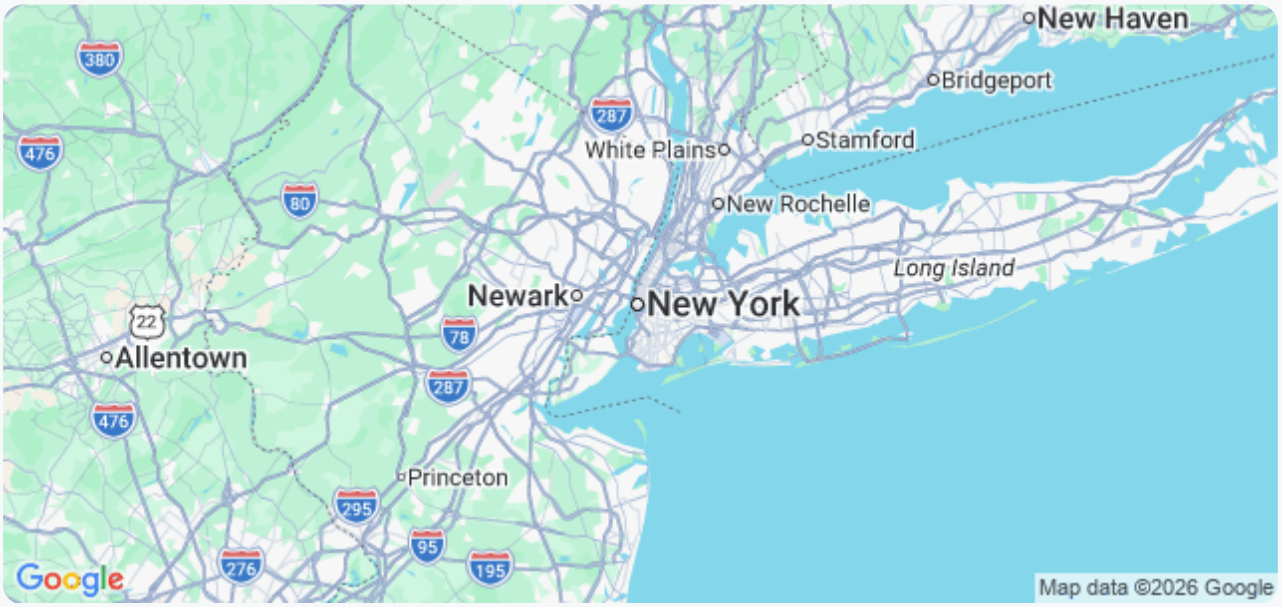
Datum eingeben...

Aufbewahrungsdauer für Backups (in Tagen)

Eine Zahl eingeben...

Standort für externe Datensicherung

Set My Current Location



Methode zur Überprüfung der Datensicherung (z. B. Testwiederherstellung)

- [ ] Testwiederherstellung
- [ ] Integritätsprüfung von Dateien
- [ ] Automatisierte Überprüfung

Datum der letzten Übung zur Notfallwiederherstellung

Datum eingeben...

Detaillierte Beschreibung des Disaster-Recovery-Plans

Etwas schreiben...

Schulung zum Thema Sicherheit und Sensibilisierung

Schulung der Mitarbeiter in Bezug auf bewährte Sicherheitsverfahren und potenzielle Bedrohungen.

Datum der letzten abgeschlossenen Schulung

- [ ] Innerhalb der letzten 3 Monate
- [ ] Vor 3–6 Monaten
- [ ] Vor 6–12 Monaten
- [ ] Vor über 12 Monaten

In der Schulung behandelte Themen

- [ ] Phishing-Erkennung
- [ ] Passwortsicherheit
- [ ] HIPAA-Konformität
- [ ] Schutz vor Schadsoftware
- [ ] Meldung von Datenschutzverletzungen
- [ ] Physische Sicherheit

Beschreiben Sie kurz, wie Sie sich Phishing-Angriffe vorstellen.

Etwas schreiben...

Wie melden Sie üblicherweise verdächtige Phishing-E-Mails?

- [ ] An die Abteilung für IT-Sicherheit
- [ ] An den Vorgesetzten
- [ ] Löschen und Ignorieren

Wie oft haben Sie in diesem Jahr die Sicherheitsrichtlinien der Organisation überprüft?

Eine Zahl eingeben...

Compliance- und regulatorische Anforderungen

Einhaltung der einschlägigen Gesetze und Vorschriften, wie beispielsweise HIPAA und HITECH.

Ist die Bewertung der HIPAA-Sicherheitsrichtlinien abgeschlossen?

- [ ] Ja
- [ ] Nein
- [ ] In Bearbeitung

Datum der letzten HIPAA-Risikobewertung

Datum eingeben...

Entspricht die Anwendung den geltenden Datenschutzgesetzen des jeweiligen Bundesstaates?

- [ ] Anwendbar – Ja
- [ ] Anwendbar - Nein
- [ ] Unbekannt

Zusammenfassung der relevanten Datenschutzgesetze der jeweiligen Bundesstaaten, die Anwendung finden

Etwas schreiben...

Einhaltung der Bestimmungen des HITECH-Gesetzes?

- [ ] Ja
- [ ] Nein.
- [ ] Nicht zutreffend

Frist für die Meldung von Datenschutzverletzungen (in Tagen)

Eine Zahl eingeben...

Ergänzende Dokumentation (z. B. Richtlinien, Vereinbarungen)

Upload File

Risikomanagement von Drittanbietern

Bewertung und Steuerung von Sicherheitsrisiken, die mit Drittanbietern verbunden sind.

Risikoeinstufung von Anbietern (hoch, mittel, niedrig)

- [ ] Hoch
- [ ] Mittel
- [ ] Niedrig

Vertragsbeginndatum des Anbieters

Datum eingeben...

Datum der letzten abgeschlossenen Risikobewertung

Datum eingeben...

Anzahl der vom Dienstleister verarbeiteten Patientendaten

Eine Zahl eingeben...

Zusammenfassung der Sicherheitsmaßnahmen des Anbieters

Etwas schreiben...

Vom Anbieter erbrachte Dienstleistungen (Bitte alle zutreffenden Optionen auswählen)

- [ ] Datenspeicherung
- [ ] Datenverarbeitung
- [ ] Softwareentwicklung
- [ ] IT-Support
- [ ] Andere

Bericht zur Sicherheitsbewertung von Anbietern

Upload File

Status der Einhaltung der Anforderungen durch den Anbieter (entspricht den Anforderungen, entspricht nicht den Anforderungen, in Bearbeitung)

- [ ] Konform
- [ ] Nicht konform.
- [ ] In Bearbeitung