UMB

creating time®

Sicherheitsaspekte im HealthCare-Umfeld:
Wechselwirkung von Datenschutz, Security und Cloud

UMB für Information Security in Healthcare
Markus Kaegi und Roger Moor

Zwei Denkanstösse:

1. Umgang mit AI ChatBots
2. Umgang mit Public Cloud Anbietern

Umgang mit AI ChatBots (ChatGPT, CoPilot, BARD)

ChatBots liefern keine Wahrheiten

ChatBots unterliegen Datenschutzrichtlinien

(z.B OpenAI: https://openai.com/policies/privacy-policy)

Hinweis 1

Vermeiden von personenbezogenen Daten

Hinweis 2

Nur generische oder sogar fiktive Informationen

Hinweis 3

Vorsicht bei vertraulichen Daten (Passwörter, Bankdaten, medizinische Daten)

Hinweis 4

Chatverläufe überprüfen (vor dem Teilen oder speichern)

Hinweis 5

Lokale Datenschutzgesetze beachten

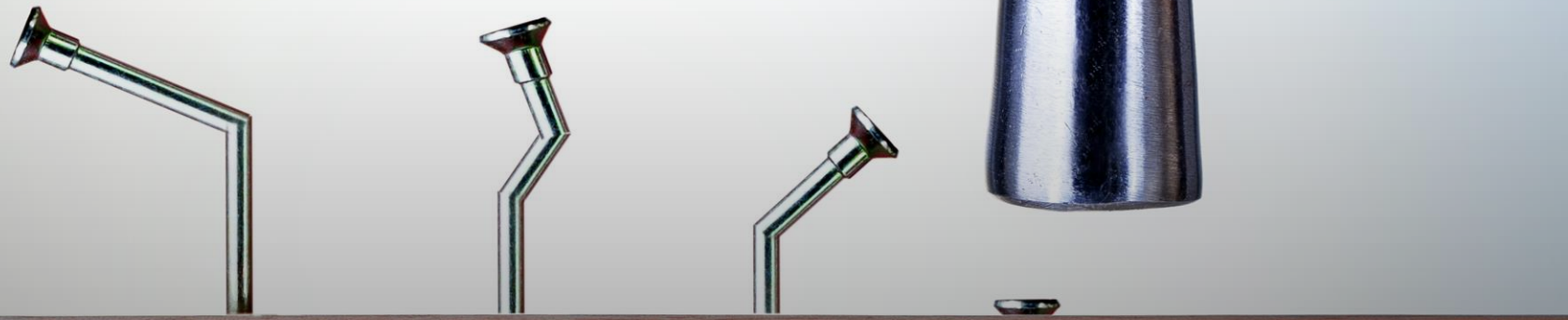
Hinweis 6

Keine Rechtsschutz- oder Datenschutz-Beratung

Und im Gesundheitswesen?

Hinweis 7

Die Risiken und Gefahren sind die gleichen, die Einsatzmöglichkeiten, die Daten und Informationen sind andere !



Fehldiagnosen und Behandlungsfehler
Haftungsfragen
Ethik und Transparenz

Beispiel aus Forschung, Entwicklung und Praxis:

Standford University – interdisziplinäres Lernen

Standford School of Medicine
Standford Center for Health Education
Standford School of Engineering

Artificial Intelligence in Healthcare | Program | Stanford Online

Umgang mit Public Cloud Anbietern

Neue Technologien bieten neue Möglichkeiten

Public Cloud Anbieter unterliegen Schweizer Datenschutzrichtlinien

Hinweis 1

Interoperabilität und Daten Portabilität richtig nutzen

Hinweis 2

Datenhoheit und Kontrolle sicherstellen


stay_safe

Folgen Sie uns umb-ag umb1978 umb1978 umb_ag

Danke für Ihre Zeit

Koordinaten für weitere Informationen:

Markus.Kaegi@UMB.ch
+41 79 286 88 17

UMB

creating time®

UMB

creating time®

BACKUP

revDSG Anforderungen und Möglichkeiten in Cloud-Services von Microsoft (Top 6)

Anforderung revDSG	Microsoft Funktionalität	Beschreibung der Funktionalität
Art. 6 Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit (CIA)	MS 365 IAM & Privileged Access Management Conditional Access	– aktive Verwaltung von privilegierten Zugriffen – Einschränkung von ständigem Zugriff auf sensible Daten oder Zugriff auf kritische Konfigurationseinstellungen
Art. 7 Datenschutz durch Technik & Voreinstellung	Verschlüsselung & Schlüsselmanagement	– kein Zugang zu hochsensiblen Daten für Unbefugte (inkl. Microsoft) – Schlüssel bleiben innerhalb einer geografischen Grenze und unter Ihrer eigenen Kontrolle

revDSG Anforderungen und Möglichkeiten in Cloud-Services von Microsoft (Top 6)

Anforderung revDSG	Microsoft Funktionalität	Beschreibung der Funktionalität
Art. 12 Verzeichnis der Bearbeitungstätigkeiten	Microsoft Information Protection	– Compliance-Beauftragte kennen die Speicherorte sensibler Informationen – Sicherheitsadministratoren setzen Richtlinien für den Datenzugriff und den Schutz vor Datenverlusten (DLP) auf der Grundlage von Labels um
Art. 6 Abs 5. Auf Risiken abgestimmte Massnahmen	Privacy Management & Compliance Manager	– Identifizierung kritischer Datenschutzrisiken und Konflikte

revDSG Anforderungen und Möglichkeiten in Cloud-Services von Microsoft (Top 6)

Anforderung revDSG	Microsoft Feature	Beschreibung der Funktionalität
Art. 25 Auskunftsrecht (Data Subject Request)	Microsoft Priva & Pureview	– Identifizierung der personenbezogenen Daten, die Gegenstand der Anfrage sind – Identifizierung kritischer Datenschutzrisiken und Konflikte – Automatisierung von Datenschutzmassnahmen und Beantwortung von Anfragen der Betroffenen
Art. 22 Datenschutz-Folgeabschätzung	Microsoft 365 Compliance Center	Microsoft unterstützt das Erstellen einer Datenschutz-Folgenabschätzung für Vorgänge, die "wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen.“