ANHANG
FÜR AUDITRECHTE UND SICHERHEITSVORGABEN BEI GATEWAY-KUNDEN

Version: 1.0

Datum: 17.01.2024

1. Einleitung

Die Health Info Net AG (HIN) ist den Vorgaben für Datenschutz und Informationssicherheit in Gesetzen, Verordnungen, Normen und Verträgen verpflichtet. Dies sind unter anderem die Folgenden:

- Bundesgesetz über den Datenschutz (DSG), SR 235.1
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11
- Bundesgesetz über das elektronische Patientendossier (EPDG), SR 816.1
- Verordnung über das elektronische Patientendossier (EPDV), SR 816.11
- Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI), SR 816.111
- Anhang 2 der EPDV-EDI
- Anhang 8 der EPDV-EDI
- ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002, Information security, cybersecurity and privacy protection — Information security controls

HIN betreibt ein Managementsystem für Datenschutz und Informationssicherheit, welches unter anderem das Management der Risiken und der Konformität beinhaltet.

Dieses Managementsystem wird von definierten Lieferanten und Kunden beeinflusst, was deren Auditierung erfordert.

HIN wird regelmässig von akkreditierten Zertifizierungsstellen auditiert und ist bisher zertifiziert gemäss ISO/IEC 27001 und dem Anhang 8 der Verordnung des EDI über das elektronische Patientendossier. Die Zertifizierung des HIN IdP beinhaltet das Access Gateway.

2. Auditrechte der HIN

Ab dem Unterzeichnungsdatum räumt der Gateway-Kunde der HIN die im Folgenden beschriebenen Auditrechte ein.

Ausserdem beinhaltet dieser Anhang konkrete Sicherheitsvorgaben für Access Gateway (AGW) und Mail Gateway (MGW).

3. Verantwortlichkeiten für den Audit

Der Verantwortliche der HIN informiert den jeweiligen Gateway-Kunden mindestens einen Monat im Voraus über den anstehenden Audit und organisiert eine Vorbesprechung.

Der Gateway-Kunde definiert einen internen Verantwortlichen, welcher gemeinsam mit dem Auditor die Termine definiert, die notwendigen Dokumente bereitstellt, den Audit begleitet, die Ergebnisse entgegennimmt und die ggf. notwendigen Korrekturmassnahmen koordiniert.

4. Umfang des Audits

Abgeleitet von ISO/IEC 27001, Anhang 2 der EPDV-EDI und Anhang 8 der EPDV-EDI wird eine reduzierte Auswahl besonders kritischer Themen auditiert, auf Basis von Dokumenten, Interviews und Kontrollen an den relevanten Systemen:

1. Physische Sicherheit

- Richtlinie oder Konzept für physische Sicherheit
- Verantwortlichkeiten für physische Sicherheit
- Zonen und effektive Zutrittsberechtigungen
- Regelmässige Kontrollen der Zutrittsberechtigungen

2. Netzwerksicherheit

- Richtlinie oder Konzept für Netzwerksicherheit
- Verantwortlichkeiten für Netzwerksicherheit
- Netzwerkzonen
- Anbindung des Gateway an das ActiveDirectory
- Attribute der Server-Zertifikate
- Ggf. Cluster Konfiguration
- Regelmässige Kontrollen der Netzwerksicherheit

3. Logische Zugriffe

- Richtlinie oder Konzept für logische Zugriffe
- Verantwortlichkeiten für logische Zugriffe
- Privilegierte Zugriffsberechtigungen
- Regelmässige Kontrollen der Zugriffsberechtigungen

4. Protokollierung (Logging)

- Richtlinie oder Konzept für Protokollierung
- Verantwortlichkeiten für Protokollierung
- Quellen der Events
- Arten und Attribute der Events
- Regelmässige Kontrollen der Protokolle

5. Sicherheitsvorfallsmanagement

- Richtlinie oder Konzept für Sicherheitsvorfallmanagement
- Verantwortlichkeiten für Sicherheitsvorfallmanagement
- Arten und Bewertung von Sicherheitsvorfällen
- Regeln zur Notifizierung bei Sicherheitsvorfällen
- Ggf. Beispiele von Sicherheitsvorfällen

6. Managementsystem für Datenschutz und Informationssicherheit

- Leitlinie für Informationssicherheit
- Richtlinie für Risikomanagement
- Risiken mit Bezug zum Gateway

5. Ergebnisse des Audits und ggf. Korrekturmassnahmen

Die Ergebnisse des Audits werden dem Gateway-Kunden in tabellarischer Form über einen sicheren Kanal (z.B. HIN E-Mail) bereitgestellt. Sie dürfen weder durch HIN noch durch die Gateway-Kunden an Dritte offengelegt werden. Die einzige Ausnahme bilden dabei die akkreditierten Zertifizierungsstellen.

Im Falle notwendiger Korrekturmassnahmen wird gemeinsam ein Termin für deren Umsetzung definiert, welcher in der Regel 3 Monate nach dem Audit liegt.

Der Verantwortliche des Gateway-Kunden koordiniert diese Korrekturmassnahmen und meldet die Ergebnisse an HIN, welche diese überprüft.

6. Kosten der Audits

Die Kosten des Audits bei HIN und beim Gateway-Kunden werden gemäss Gebührentabelle dem Kunden verrechnet.

Für die Vorarbeit, Durchführung des Audits und Nacharbeit wird jeweils ein Aufwand eines halben Tages geschätzt.

SICHERHEITSVORGABEN

Die folgenden Sicherheitsvorgaben können aufgrund von geänderten oder neuen Gesetzen, Verordnungen, Normen oder sonstigen Vorgaben periodisch einseitig aktualisiert werden.

Der Kunde ist verpflichtet

- HIN Gateways in einer geschützten physischen Umgebung zu betreiben,
- HIN Gateways in einer geschützten logischen Umgebung zu betreiben,
- eine starke state-of-the-art Passwort-Policy umzusetzen (keine Accounts ohne Passwort, keine Default Passwörter, keine gleichen Passwörter für unterschiedliche Accounts, extra lange Passwörter für Service Accounts und privilegierte Accounts, usw.),
- Enduser und Service Accounts nach einer definierten Zahl (kleiner 20) fehlgeschlagener Anmeldeversuchen zu sperren,
- Idle-Timeouts umzusetzen,
- Software Updates, insbesondere die von HIN als kritisch deklarierten, so rasch wie möglich einzuplanen und zu implementieren,
- sicherheitsrelevante Ereignisse der HIN Gateways zu protokollieren (Audit Trail) und diese im Bedarfsfall der HIN zur Verfügung stellen oder der HIN Zugriff gewähren,
- Sicherheitsrisiken und Sicherheitsvorfälle in Bezug auf HIN Gateways umgehende an HIN zu melden.