ANNEXE
DROITS D'AUDIT ET EXIGENCES DE SÉCURITÉ POUR LES CLIENTS GATEWAY

Version: 1

Date: 17.01.2024

1. Introduction

Health Info Net AG (HIN) s'engage à respecter les directives relatives à la protection des données et à la sécurité de l'information énoncées notamment dans les lois, ordonnances, normes et contrats suivants:

- Loi fédérale sur la protection des données (LPD), RS 235.1
- Ordonnance relative à la loi fédérale sur la protection des données (OLPD), RS 235.11
- Loi fédérale sur le dossier électronique du patient (LDEP), RS 816.1
- Ordonnance sur le dossier électronique du patient (ODEP), RS 816.11
- Ordonnance du DFI sur le dossier électronique du patient (ODEP-DFI), RS 816.111
- Annexe 2 de l'ODEP-DFI
- Annexe 8 de l'ODEP-DFI
- ISO/IEC 27001, Sécurité de l'information, cybersécurité et protection de la sphère privée — Systèmes de management de la sécurité de l'information — Exigences
- ISO/IEC 27002, Sécurité de l'information, cybersécurité et protection de la sphère privée — Contrôles de sécurité de l'information

HIN exploite un système de gestion pour la protection des données et la sécurité de l'information, qui comprend entre autres la gestion des risques et de la conformité.

Ce système de gestion est influencé par des fournisseurs et des clients définis, ce qui nécessite leur audit.

HIN est régulièrement auditée par des organismes de certification accrédités et est actuellement certifiée selon la norme ISO/IEC 27001 et l'annexe 8 de l'ordonnance du DFI sur le dossier électronique du patient. La certification de l'IdP HIN inclut l'Access Gateway.

2. Droits d'audit de HIN

À compter de la date de signature, le client Gateway accorde les droits d'audit décrits ci-dessous à HIN.

En outre, cette annexe contient des exigences de sécurité concrètes pour Access Gateway (AGW) et Mail Gateway (MGW).

3. Responsabilités en matière d'audit

Le responsable de HIN informe le client Gateway concerné de l'audit à venir au moins un mois à l'avance et organise une réunion préliminaire.

Le client Gateway définit un responsable interne qui, avec l'auditeur, définit les délais, fournit les documents nécessaires, accompagne l'audit, reçoit les résultats et coordonne toute mesure corrective nécessaire.

4. Étendue de l'audit

Dérivée de la norme ISO/IEC 27001, annexe 2 de l'ODEP-DFI et annexe 8 de l'ODEP-DFI, une sélection réduite de sujets particulièrement critiques est auditée sur la base de documents, d'entretiens et de contrôles des systèmes concernés:

1. Sécurité physique

- Directive ou concept de sécurité physique
- Responsabilités en matière de sécurité physique
- Zones et autorisations d'accès effectives
- Contrôle régulier des autorisations d'accès

2. Sécurité du réseau

- Directive ou concept de sécurité du réseau
- Responsabilités en matière de sécurité du réseau
- Zones de réseau
- Connexion du Gateway à l'ActiveDirectory
- Attributs des certificats de serveur
- Év. configuration du cluster
- Contrôle régulier de la sécurité du réseau

3. Accès logiques

- Directive ou concept d'accès logiques
- Responsabilités en matière d'accès logiques
- Autorisations d'accès privilégiées
- Contrôle régulier des autorisations d'accès

4. Journalisation (logging)

- Directive ou concept de journalisation
- Responsabilités en matière de journalisation
- Sources des événements
- Types et attributs des événements
- Contrôle régulier des protocoles

5. Gestion des incidents de sécurité

- Directive ou concept de gestion des incidents de sécurité
- Responsabilités en matière de gestion des incidents de sécurité
- Types et évaluation des incidents de sécurité
- Règles de notification des incidents de sécurité
- Év. exemples d'incidents de sécurité

6. Système de gestion pour la protection des données et la sécurité de l'information

- Ligne directrice pour la sécurité de l'information
- Directive de gestion des risques
- Risques liés au Gateway

5. Résultats de l'audit et mesures correctives éventuelles

Les résultats de l'audit sont fournis au client Gateway sous forme de tableaux via un canal sécurisé (p. ex.: e-mail HIN). Ni HIN ni les clients Gateway ne sont autorisés à les divulguer à des tiers. La seule exception à cette règle concerne les organismes de certification accrédités.

Si des mesures correctives sont nécessaires, une date de mise en œuvre est définie conjointement, généralement trois mois après l'audit.

Le responsable du client Gateway coordonne ces mesures correctives et en communique les résultats à HIN, qui les examinera.

6. Coûts de l'audit

Les coûts de l'audit pour HIN et pour le client Gateway sont facturés au client conformément au tableau des frais.

La durée du travail de préparation, de l'audit et du suivi est estimée à une demi-journée.

EXIGENCES DE SÉCURITÉ

Les exigences de sécurité suivantes peuvent être mises à jour périodiquement de manière unilatérale en raison de modifications ou de nouvelles lois, ordonnances, normes ou autres exigences.

Le client est tenu

- d'utiliser HIN Gateway dans un environnement physique protégé,
- d'utiliser HIN Gateway dans un environnement logique protégé,
- de mettre en œuvre une politique de mot de passe «state of the art» solide (pas de comptes sans mot de passe, pas de mots de passe par défaut, pas de mots de passe identiques pour différents comptes, mots de passe très longs pour les comptes de service et les comptes privilégiés, etc.),
- de bloquer les utilisateurs finaux et les comptes de service après un nombre défini (inférieur à 20) d'échecs de connexion,
- de mettre en œuvre des idle timeouts,
- de planifier et d'implémenter le plus rapidement possible les mises à jour logicielles, en particulier celles déclarées comme critiques par HIN,
- de consigner les événements liés à la sécurité des HIN Gateways (audit trail) et, en cas de besoin, de les mettre à la disposition de HIN ou accorder l'accès à HIN,
- de signaler immédiatement à HIN les risques et incidents de sécurité concernant les HIN Gateways.