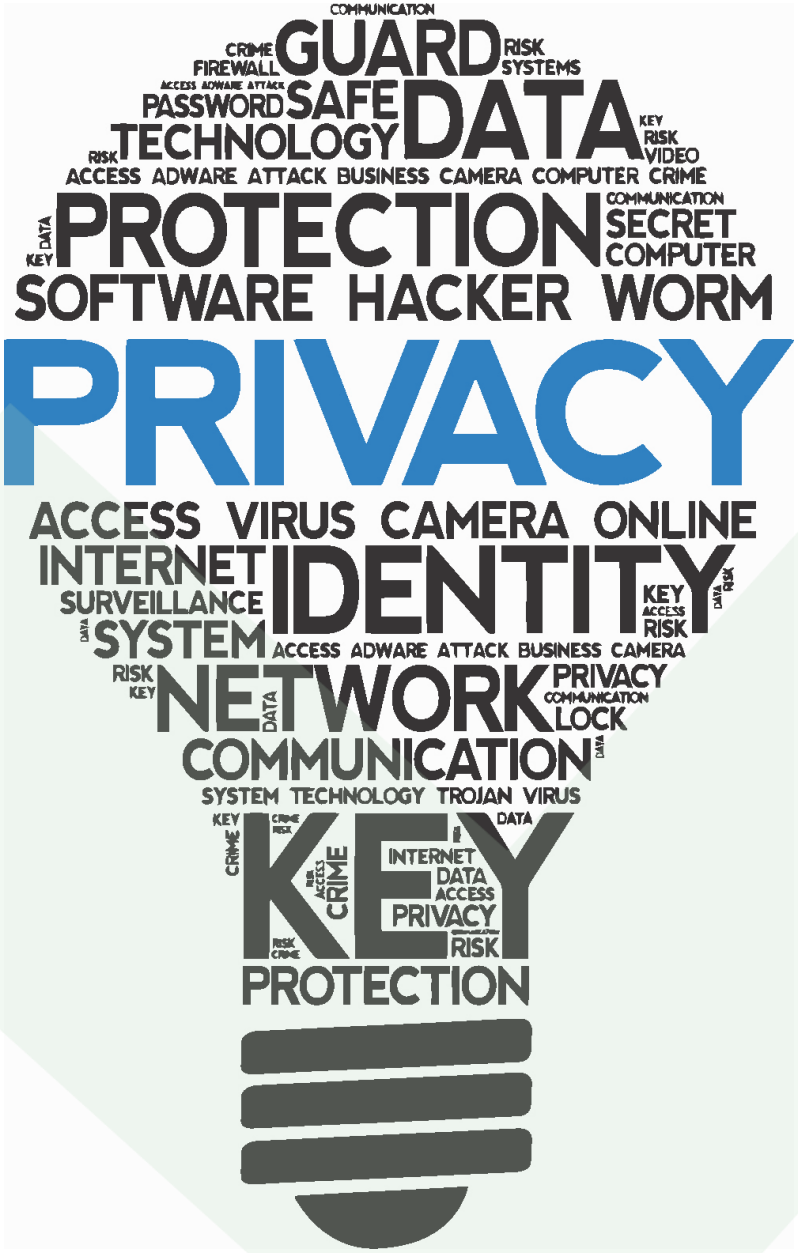
7 RECOMMANDATIONS ET BONNES PRATIQUES
POUR LES PRESTATAIRES DE SERVICES ICT DE SANTE

AGENCE eSanté LUXEMBOURG | Agence nationale des informations partagées dans le domaine de la santé

eQualis eHealth Qualification for Interoperability & Security

LHC Luxembourg House of Cybersecurity

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy



Les données de santé sont des données hautement sensibles qui doivent être traitées de façon sécurisée et conforme à la protection des données. En tant que prestataire de services ICT de santé, vous - et votre solution ICT - êtes un élément essentiel de la chaîne de sécurité des informations, avec les prestataires de services de santé.

Afin de vous soutenir dans ce rôle tout au long de vos interactions avec le système public de santé, l'Agence eSanté, le Ministère de l'Economie et Securitymadein.lu ont développé conjointement la présente directive qui contient ***7 RECOMMANDATIONS*** *dans le domaine de la sécurité des informations.*

Les recommandations contenues dans ce livret sont basées sur l'analyse d'entretiens avec des éditeurs de logiciel et des prestataires de services informatiques. Trouvez le contenu de ce livret et de plus amples informations en suivant ce lien ou avec le QR-code figurant sur la dernière page.

1 CHIFFREMENT

- ✓ Evitez de gérer les clés privées de vos clients et utilisateurs pour ne pas risquer de les perdre, de vous les faire voler ou que quelqu'un en fasse un mauvais usage. Le fait de gérer les clés privées de quelqu'un d'autre peut induire un risque de responsabilité en cas de litige.
- ✓ Chiffrez les sauvegardes et les données stockées dans votre système ou votre logiciel afin de les protéger contre tout risque de divulgation en cas de vol ou de perte et de corruption, en utilisant un logiciel de chiffrement de disque, un système de fichiers de chiffrement ou des bases de données chiffrées.
- ✓ Utilisez le chiffrement pour les données en circulation en configurant des connexions chiffrées.
- ✓ Utilisez une longueur de clé "optimale" pour votre algorithme de chiffrement, soit au moins 256 bits pour les clés des algorithmes symétriques et 2048 bits pour les algorithmes asymétriques. Suivez les dernières recommandations en termes de longueur de clés car il est important d'augmenter la longueur des clés pour assurer la sécurité du chiffrement.
- ✓ Pensez à utiliser à la fois les chiffrements symétriques et asymétriques. Pour le choix des algorithmes de chiffrement symétrique ou asymétrique, reportez-vous aux recommandations les plus récentes du BSI.

- ➔ Vous pouvez aider vos clients à créer des clés, mais jamais vous occuper des clés privées vous-même.
- ➔ Vous trouverez ici des informations utiles et une comparaison des logiciels de chiffrement de disque.
- ➔ Utilisez https, des connexions TLS valides et SFTP pour l'échange de données chiffrées.
- ➔ Pour les dernières recommandations concernant la longueur de clé pour le chiffrement, pensez à vérifier des sites tels que celui-ci ou celui-là à partir du BSI.

2 MISE A JOUR ET GESTION DES PATCHS

- ✓ Tenez-vous informé et appliquez les patchs de sécurité nécessaires au système d'exploitation et à l'environnement d'application sur votre système et sur les systèmes que vous gérez pour vos clients. A chaque fois que vous installez des patchs ou des mises à jour de sécurité, vous devez utiliser un compte ayant les privilèges minimum pour la tâche de mise à jour et de gestion des patchs.
- ✓ Automatisez les mises à jour logicielles plutôt que de compter sur les utilisateurs pour les effectuer ; informez et prévenez vos clients des mises à jour, et programmez celles qui doivent être effectuées en dehors des heures ouvrables courantes.

- ➔ Tenez-vous informé et appliquez des patchs de sécurité régulièrement.
- ➔ Respectez la recommandation concernant les privilèges minimum.
- ➔ Pensez à activer des mises à jour automatiques en dehors des heures ouvrables.

3 ACCES A DISTANCE AUX POSTES DE TRAVAIL

- ✓ Pensez aux risques d'exfiltration des données quand vous accédez à des ordinateurs distants. Reposez-vous toujours sur l'autorisation de l'utilisateur, évitez les connexions permanentes et assurez la journalisation et le traçage des activités effectuées.
- ✓ Reposez-vous toujours sur l'autorisation explicite de l'utilisateur pour toute session distante.
- ✓ Les sessions distantes pour la maintenance et l'assistance doivent être aussi brèves que possible.
- ✓ Ne demandez jamais les informations d'authentification de vos clients ; utilisez plutôt vos propres données.
- ✓ Assurez-vous que l'accès à distance est clos par l'utilisateur ou automatiquement une fois que la tâche est accomplie.

4 PROTECTION DES DONNEES A CARACTERE PERSONNEL

- ✓ Gardez à l'esprit quelques définitions de base :
  - Les données à caractère personnel (DCP) sont toutes les informations se rapportant à une personne physique identifiée ou identifiable (Art 4.1 RGPD). Les données à caractère personnel de santé sont des données sensibles relevant d'un régime spécial (Art 9.2 RGPD).
  - Le traitement des DCP est toute opération de manipulation de DCP (collecte, tri, consultation,...). Le traitement des DCP et des DCP de santé repose sur des bases légales.
  - Le responsable du traitement est l'entité qui détermine les finalités et moyens du traitement. Le responsable conjoint du traitement est une autre entité intervenant à des fins qui lui sont propres sur le traitement de DCP de sorte qu'elle soit déterminante dans l'orientation des finalités et des moyens du traitement.
  - Un sous-traitant est une entité qui traite des données pour le compte et sur instruction (par contrat) du responsable du traitement.
- ✓ Ne traitez pas inutilement des données à caractère personnel, pour éviter les risques potentiels de protection des données.
- ✓ Ne conservez pas de DCP inutilement, en particulier s'il s'agit de données médicales, pour éviter les risques de protection des données.
- ✓ Identifiez clairement le rôle et la fonction des intervenants et communiquez-les de manière transparente.
- ✓ Sécurisez le traitement des données à caractère personnel en appliquant des mesures élevées de sécurité physique, logique et organisationnelle.

5 GESTION DES INCIDENTS

Définissez un processus ou une procédure de traitement des incidents de sécurité. Voici quelques éléments à prendre en compte :

- exécuter les étapes classiques pour limiter les dommages
- isoler la source de l'incident
- prendre des mesures de rétablissement
- définir qui informer et quand
- garder une trace de chaque incident et de la manière dont il a été géré
- tirer des leçons des incidents précédents afin qu'ils ne se reproduisent plus

Si vous faites l'objet d'un incident de sécurité des informations (attaque, malware, etc.) et que vous avez besoin de l'avis d'un autre expert, vous pouvez toujours solliciter l'aide du service CIRCL de Security Made In Luxembourg (info@circl.lu).

6 GESTION DES RISQUES

- ✓ Evaluez la maturité de votre gestion des risques de sécurité des informations.
- ✓ Découvrez les faiblesses effectives de vos systèmes ou logiciels.
- ✓ Une bonne gestion des risques implique une préparation, mais aussi de la transparence vis-à-vis de vos clients. En matière de transparence, vous devez vous assurer que les contrats avec vos clients définissent quelles sont les responsabilités de chacun en matière de sécurité des informations.
- ✓ Si vous êtes en mesure de lister ces risques, vous devez aussi lister les actions que vous avez entreprises ou allez entreprendre pour traiter ces risques afin que leur impact soit minimal. Nous vous recommandons d'utiliser MONARC, un bon outil de gestion des risques qui est proposé gratuitement.

- ➔ Vous pouvez utiliser les outils Fit4Cybersecurity ou Fit4Privacy de CASES qui sont proposés gratuitement pour effectuer une auto-évaluation de votre maturité dans la gestion des risques.
- ➔ Informez-vous ici via l'outil de recherche des vulnérabilités courantes proposé par CIRCL.
- ➔ Accédez à l'annuaire Cybersecurity Ecosystem proposé par Security Made in Luxembourg si vous voulez sélectionner et contacter un expert pour effectuer cette analyse pour vous.
- ➔ Pensez à utiliser MONARC comme outil de gestion des risques .

7 PRINCIPES DE DEVELOPPEMENT ET DE CODAGE SECURISES

- ✓ Intégrez des exigences de complexité et de validité des mots de passe.
- ✓ Intégrez un accès à votre logiciel basé sur les rôles.
- ✓ Intégrez un chiffrement pour les données en transit ou stockées.
- ✓ Faites attention au jeu de données de test et à l'environnement de test.
- ✓ Utilisez des principes de codage sécurisé définis officiellement, gérez les codes et effectuez des revues de code.
- ✓ Utilisez un logiciel de gestion de code source.
- ✓ Sécurisez et chiffrez les sauvegardes de votre code source.
- ✓ Etablissez un processus de développement de logiciel approuvé et documenté.
- ✓ Pensez aux bonnes pratiques des tests de sécurité.
- ✓ N'utilisez pas de bibliothèques, de langages de programmation ou de systèmes d'exploitation périmés.
- ✓ Evitez les transferts de données avec des connexions sans fil non protégées ou publiques quand votre logiciel échange des données avec des machines extérieurs.
- ✓ Pensez à utiliser des langages de programmation modernes qui sont supportés par leur vendeur ainsi que par une vaste communauté et sont fournis avec des mises à jour régulières et des patchs de sécurité.

- ➔ Trouvez des recommandations plus précises sur la complexité des mots de passe ici ou reportez-vous aux recommandations sur les mots de passe du NIST.
- ➔ Pour les principes de codage sécurisés, reportez-vous aux recommandations OWASP, à la référence "Writing Secure Code" de M. Howard ou au livre "Software Security: Building Security In" de G. McGraw.
- ➔ Vous trouverez ici de plus amples informations sur les logiciels de gestion des codes sources tels que GIT, Subversion, etc.
- ➔ Pour le support de cycle de vie de votre système Windows, vous pouvez vous référer à cette page Microsoft.
- ➔ Cliquez ici pour trouver les bonnes pratiques de cybersécurité.

Agence nationale des informations partagées dans le domaine de la santé

eQualis eHealth Qualification for Interoperability & Security

Luxembourg House of Cybersecurity

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of the Economy

Des questions ou besoin d'assistance?

Contactez l'équipe eQualis de l'Agence eSanté

E-mail: eQualis@esante.lu

Plus d'infos?

Scannez ce code

https://gd.lu/3rQ56h