Exigences techniques et organisationnelles pour les services sur le cloud

Sommaire

Introduction

Au cours des dernières années, les progrès réalisés dans l'utilisation partagée des ressources au sein de réseaux a entraîné un déplacement des capacités de calcul, de l'espace de stockage et des applications vers le cloud. Ces déplacements s'accompagnent non seulement d'avantages en termes de coûts, mais aussi de gains de productivité sous forme d'une modularité améliorée, d'une maintenance du système simplifiée et généralement d'une plus grande fiabilité. Outre les avantages, on se trouve aussi face à des défis dans le domaine de la sécurité de l'information. Il s'agit notamment de tirer au clair des questions concernant le cryptage, le contrôle des accès, la gouvernance et le support, la performance, la disponibilité, la sauvegarde et la reprise sur sinistre (disaster recovery). En particulier dans le domaine des rôles et compétences, il faut définir quelles tâches sont assumées par les utilisateurs des services sur le cloud (les médecins) et les prestataires informatiques des cabinets médicaux, et lesquelles par les services sur le cloud. La responsabilité pour la protection des données incombe toujours aux médecins.

Objectif

Les exigences techniques et organisationnelles qui suivent ont été élaborées pour garantir la protection et la sécurité des données lors du traitement de données de patients sur le cloud. Ces exigences visent à réduire les risques associés à l'utilisation de services sur le cloud et à garantir une utilisation sûre de ces services pour les médecins.

Les présentes exigences s'appliquent d'une manière générale à tout système basé sur le cloud dans lequel sont traitées des données sensibles. Pour chacun des services sur le cloud dépassant le cadre des applications pour cabinets médicaux mentionnées, il faut donc vérifier, avant son utilisation, si ce service traite des données de patients. Si le service ne contient que des données personnelles sans besoin de protection accru, les exigences sont en conséquence moins élevées.

Groupe cible

Les exigences techniques s'adressent aux prestataires TIC et fournisseurs de services sur le cloud pour les médecins. Cela inclut aussi les fabricants de dispositifs médicaux qui proposent des services sur le cloud pour les médecins dans le cadre de leurs prestations.

Caractère obligatoire

Les exigences techniques et organisationnelles de ce document ont valeur de recommandations. Il relève de l'appréciation des médecins responsables ou de leurs prestataires TIC mandatés de définir le caractère obligatoire des exigences.
Pour appuyer ce processus décisionnel, les mesures sont divisées en deux groupes:

1. Exigences obligatoires (**M**): une exigence obligatoire signifie que l'exigence doit être remplie au sens de cette recommandation. Cela vaut pour les données personnelles sensibles et les données personnelles sans besoin de protection accru. Il est recommandé de refuser la réception si cette exigence n'est pas remplie.
2. Exigences standard (**S**): une exigence standard signifie que l'exigence doit en règle générale être remplie au sens de cette recommandation. Le prestataire de services sur le cloud ou le prestataire TIC doit justifier le non-respect de cette exigence pour des données personnelles sensibles. Ces exigences peuvent être supprimées pour les données personnelles sans besoin de protection accru.

Délimitation

Le présent document est soumis aux délimitations suivantes:

Portée

- Les recommandations portent essentiellement sur le traitement électronique de données personnelles dans le système de santé, au sens de la section 3 de la loi fédérale sur la protection des données (LPD), par des personnes privées en rapport avec l'utilisation de services sur le cloud. Le traitement de données personnelles par des organismes officiels tels que des hôpitaux publics n'est pas visé par ces recommandations. Les informations au format papier ou d'autres informations analogues ne sont pas concernées par les exigences.
- Les exigences pour les prestataires de services sur le cloud sont indépendantes des exigences en matière de sécurité en rapport avec le dossier électronique du patient (DEP).
- Les exigences pour les prestataires de services sur le cloud ne sauraient prétendre être exhaustives ni donner un aperçu complet des thèmes traités. La mise en œuvre de toutes les exigences ne garantit pas une sécurité absolue.

Bases

- Les exigences techniques et organisationnelles pour les prestataires de services sur le cloud ont été définies en référence à la Security Guidance – for Critical Areas of Focus in Cloud Computing V 4.0 de la Cloud Security Alliance (CSA).
- Les exigences s'appuient sur le profil de risque des données sensibles selon l'art. 3, let. a, LPD.

Service sur le cloud

L'informatique sur le cloud est un modèle dans lequel des ressources informatiques configurées conjointement, par exemple un réseau, un serveur, une mémoire, des applications ou services, peuvent être sollicitées par l'intermédiaire d'un réseau.

Dans les cabinets médicaux, les solutions sur le cloud sont utilisées pour classer des données de patients, composées de données démographiques et médicales, ou pour recourir à des applications telles que Microsoft Office 365.

Les caractéristiques suivantes d'un service sur le cloud ont été définies dans le Standard SP 800-145 du National Institute of Standards and Technology (NIST)[1] qui est internationalement reconnu.

Caractéristique	Explication
Self-service disponible	Au besoin, l'utilisateur de services sur le cloud peut se procurer lui-même des ressources informatiques, par exemple un serveur de temps ou du stockage en réseau, sans devoir interagir pour cela avec le prestataire de services sur le cloud.
Accès au réseau	Les ressources informatiques sont disponibles sur le réseau, l'accès étant possible depuis un téléphone mobile, une tablette, un ordinateur portable ou un poste de travail, ou par virtualisation des appareils cités.
Regroupement des ressources	Les ressources informatiques sont regroupées et peuvent donc être sollicitées par plusieurs utilisateurs ayant une infrastructure différente.
Élasticité rapide	Les ressources informatiques peuvent être rapidement adaptées par les utilisateurs de services sur le cloud.
Service administré	Contrôler les systèmes sur le cloud et optimiser automatiquement les ressources informatiques. L'utilisation des ressources est surveillée, contrôlée et communiquée pour assurer la transparence tant du prestataire de services sur le cloud que de l'utilisateur.

Tableau 1
Caractéristiques des services sur le cloud

Modèle de services sur le cloud

Un modèle de services définit l'étendue des prestations du prestataire de services sur le cloud. Plus l'étendue des services sur le cloud mis à disposition est grande, plus le domaine de responsabilité et l'influence de l'utilisateur sur l'infrastructure de la technologie d'information et de communication sont grands.

On distingue entre Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) et Infrastructure-as-a-Service (IaaS). Les solutions SaaS comprennent la mise à disposition d'une application complète qui est exploitée et gérée par le prestataire de services sur le cloud. Les utilisateurs d'une solution SaaS peuvent accéder aux applications de tiers par le navigateur internet ou une application sur le terminal. Les solutions PaaS incluent une plate-forme complète pour développer, exploiter ou gérer des applications qui sont administrées par le prestataire de services sur le cloud. Les solutions IaaS intègrent des ressources pour une infrastructure informatique complète, par exemple capacités de calcul, réseaux ou mémoires.

Le graphique ci-après illustre les trois modèles de services et les domaines de responsabilité correspondants.

1 The NIST Definition of Cloud Computing: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Acteurs de services sur le cloud

Prestataire de services sur le cloud Le prestataire de services sur le cloud est responsable de la mise à disposition, de la maintenance et de l'entretien des services sur le cloud, c'est-à-dire qu'il est responsable du matériel et des logiciels en fonction du modèle de services sur le cloud.

Modèle de services sur le cloud Un modèle de services sur le cloud représente un ensemble prédéfini de ressources informatiques qui sont mises à disposition par le prestataire de services sur le cloud. Les plus connues sont Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS).

Modèle d'implémentation de services sur le cloud Un modèle d'implémentation de services sur le cloud se réfère au type de l'implémentation du modèle de services sur le cloud. Il s'agit de Public Cloud, Private Cloud, Community Cloud et Hybrid Cloud.

Service sur le cloud Un service sur le cloud comprend l'ensemble de toutes les ressources et prestations mises à disposition ou proposées par internet par un prestataire de services sur le cloud. La mise à disposition et l'utilisation de ces prestations sont assurées exclusivement par les interfaces et protocoles techniques.

Utilisateurs de services sur le cloud Les utilisateurs de services sur le cloud sont toutes les parties qui utilisent un service sur le cloud. Dans ce document, ce terme se réfère aux médecins et à leurs prestataires TIC mandatés.

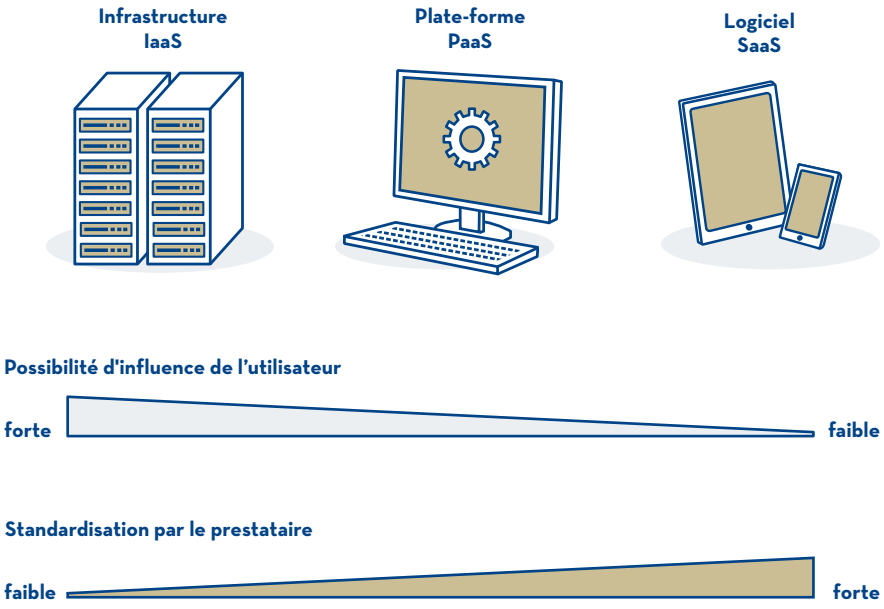


Illustration 1
Aperçu des modèles de services sur le cloud en référence à la CSA

Responsabilités	SaaS	PaaS	IaaS
Données	○	○	○
Application	●	○	○
Environnement d'exécution/container	●	●	○
Système d'exploitation	●	●	○
Couche de virtualisation	●	●	●
Mise à disposition et exploitation du matériel	●	●	●
Sécurité physique	●	●	●

○ Utilisateur cloud ● Prestataire cloud

Illustration 2
Responsabilités des utilisateurs de services sur le cloud et des prestataires de services sur le cloud en référence à la CSA

Modèles d'implémentation de services sur le cloud

On distingue quatre modèles différents pour l'implémentation de services sur le cloud:

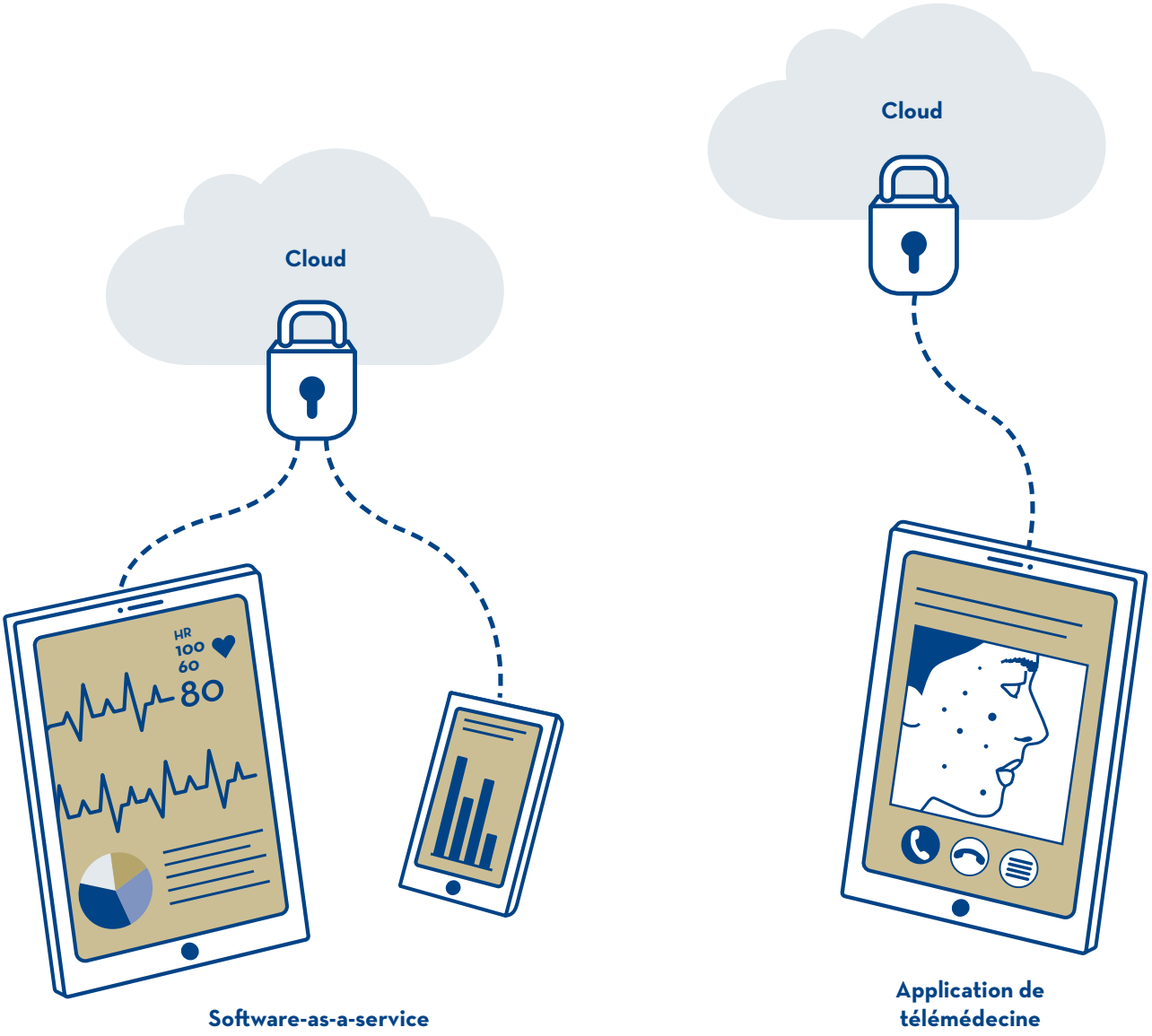
Public Cloud L'infrastructure sur le cloud est accessible à un grand nombre d'utilisateurs ou à un groupe industriel de grande taille. Elle est la propriété d'une organisation qui propose des services sur le cloud. On citera comme exemples Dropbox, Google Drive ou Microsoft Office 365.

Private Cloud L'infrastructure sur le cloud est exploitée pour une entreprise donnée. Elle est administrée soit par l'entreprise soit par un tiers mandaté. L'infrastructure peut se trouver à l'intérieur ou à l'extérieur de l'entreprise.

Community Cloud L'infrastructure sur le cloud est exploitée pour un ensemble d'entreprises qui ont des intérêts communs (p. ex. la même branche ou les mêmes exigences en matière de sécurité). Elle est administrée soit par une des entreprises affiliées soit par un tiers mandaté. L'infrastructure peut se trouver à l'intérieur ou à l'extérieur des entreprises.

Hybrid Cloud L'infrastructure sur le cloud est une forme mixte des modèles d'implémentation décrits ci-dessus. Le terme Hybrid Cloud est aussi employé pour des solutions qui incluent des composants tant sur site que sur le cloud.

E1 Applications et interfaces

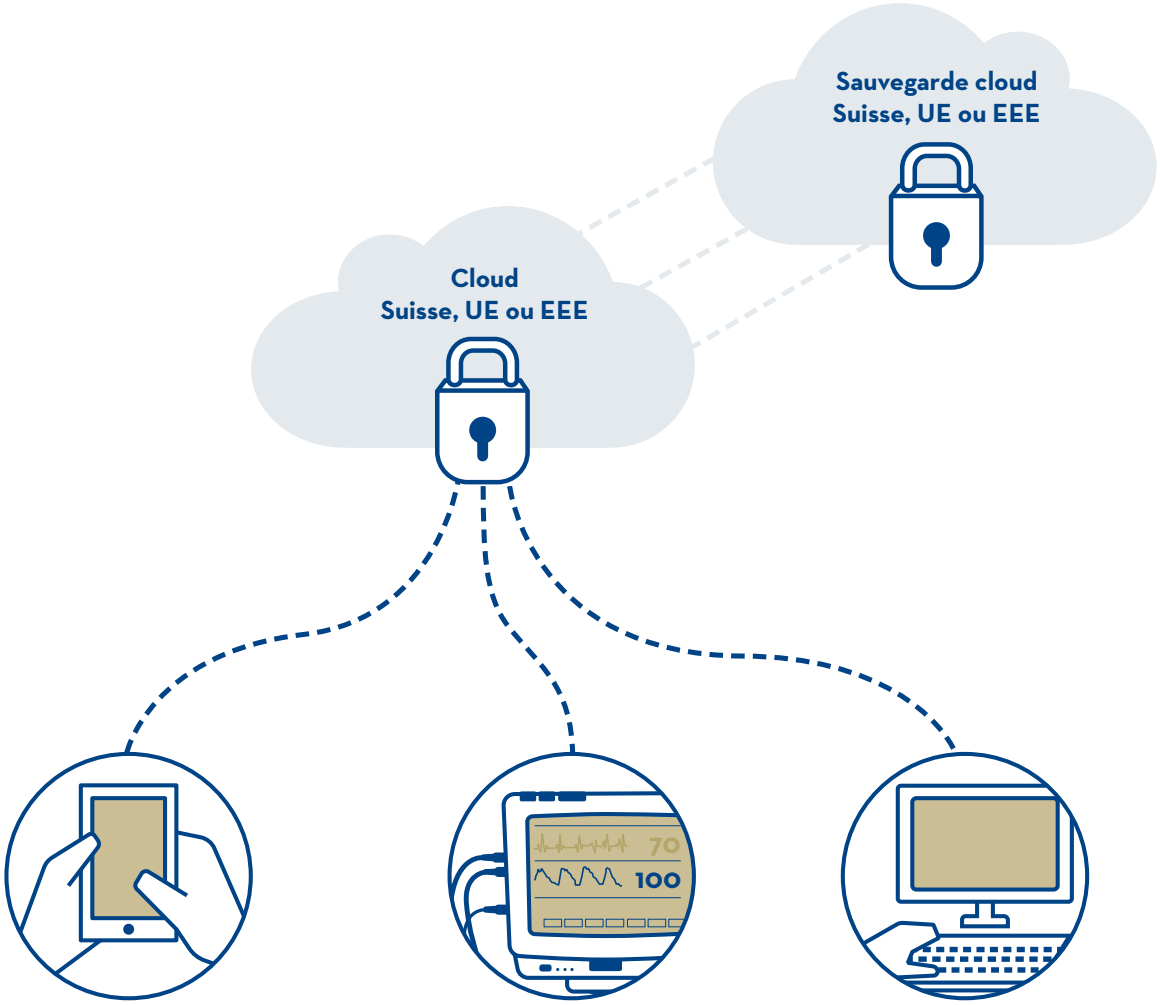


Le Secure Development Life Cycle (SDLC) a gagné en importance pour la migration et la mise à disposition d'applications sur le cloud. Les prestataires de services sur le cloud doivent s'assurer que les meilleures pratiques de la sécurité informatique soient intégrées tant pour les applications que pour les interfaces pendant tout le cycle de vie des applications.

Exigences

A-1.01	M	**Exigences pour les interfaces** Les applications et les interfaces de programmation applicative (API) doivent être conçues, développées, mises à disposition et testées selon les standards de sécurité (p. ex. OWASP pour les applications internet).
A-1.02	S	**Appel de service en ligne** L'appel d'un service en ligne à partir d'un client doit s'effectuer par une passerelle intégrant un pare-feu d'applications et une API de gestion.

E2 Garantie de l'audit et de la conformité



Le domaine de la garantie de l'audit et de la conformité traite du respect de la législation en vigueur, du respect des prescriptions internes, des standards reconnus, p. ex. ISO 27001, ainsi que de la garantie de la conformité pendant un audit.

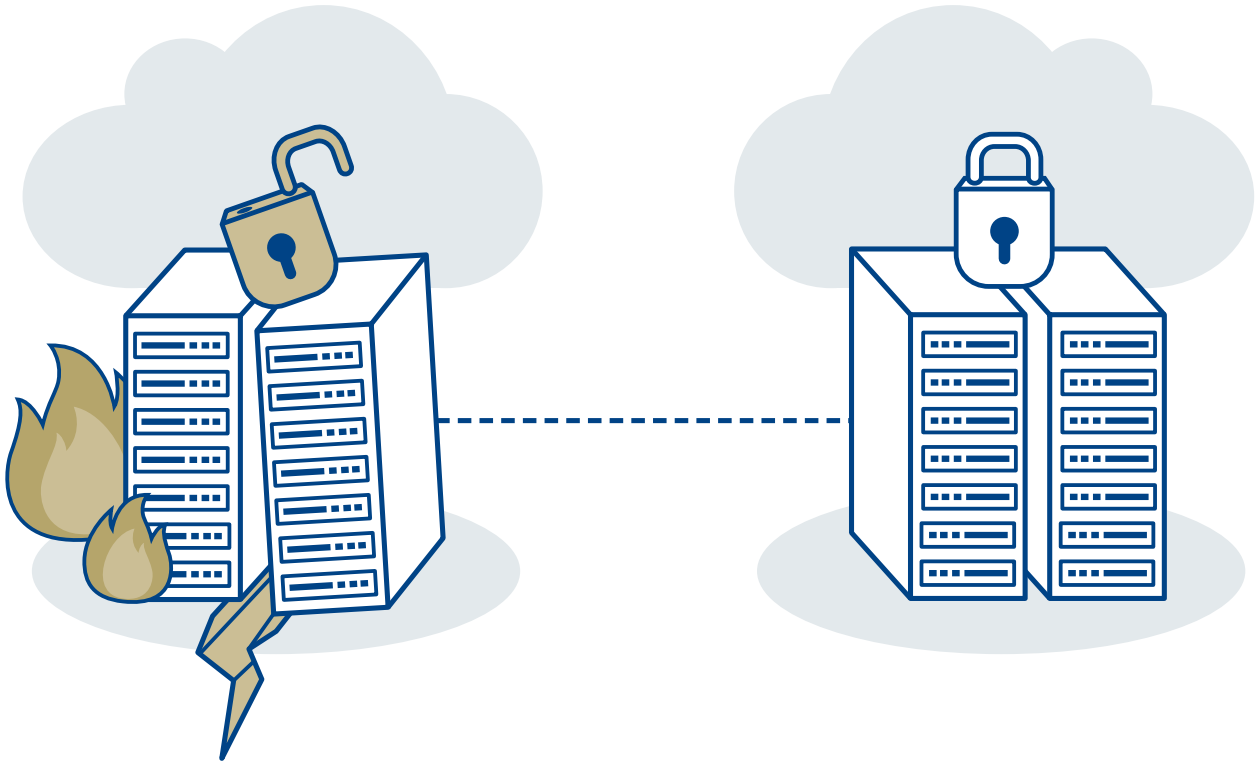
Les dispositions légales qui doivent être prises en compte en rapport avec l'utilisation de services sur le cloud sont la loi fédérale sur la protection des données (LPD) et notamment l'article 10a LPD Traitement de données par un tiers. D'après cet article, le traitement de données personnelles peut être confié à un tiers pour autant que les critères suivants soient remplis:

- Aucune obligation légale ou contractuelle de garder le secret ne l'interdit.
- Le prestataire de services sur le cloud ne traite les données que dans la mesure où l'utilisateur (le médecin) pourrait lui-même le faire.
- L'utilisateur de services sur le cloud doit s'assurer que la sécurité des données est garantie par le prestataire.
- Le respect du contrat doit être régulièrement vérifié.

Exigences

A-2.01	M	**Lieu de conservation des données, sauvegarde incluse** La conservation des données du système doit correspondre aux exigences légales selon l'art. 6 LPD (Communication transfrontière de données). La conservation et le traitement des données doivent s'effectuer en Suisse, dans l'Union européenne ou dans l'Espace économique européen.
A-2.02	S	**Juridiction des prestataires de services sur le cloud** Le prestataire de services sur le cloud doit avoir son for en Suisse ou dans l'Union européenne.
A-2.03	M	**Pouvoirs d'information et d'investigation (consultation des données par les acteurs étatiques)** Le prestataire de services sur le cloud doit fournir des informations transparentes sur les pouvoirs d'information et d'investigation accordés aux acteurs étatiques.

A3 Gestion de la continuité des affaires



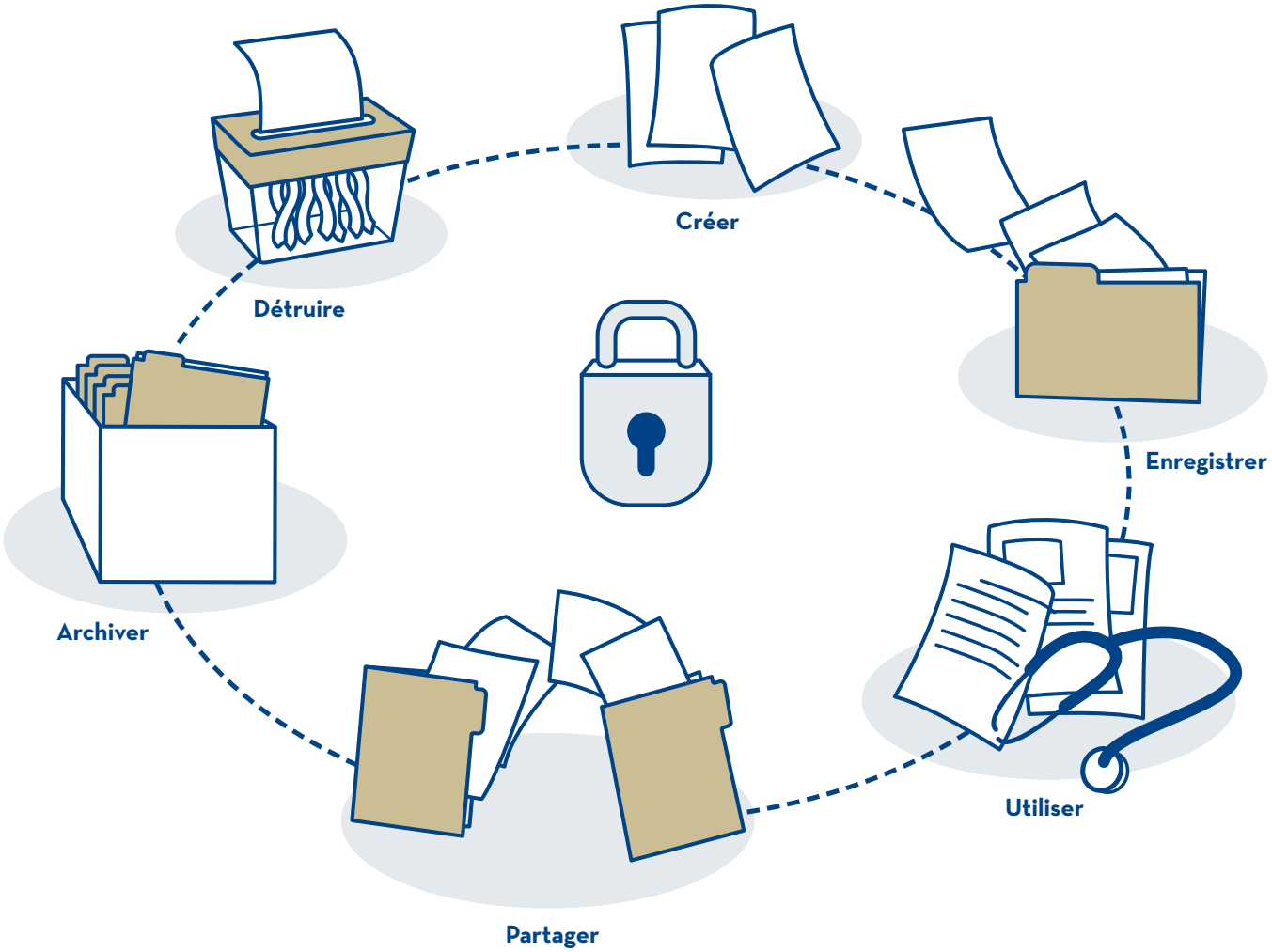
La gestion de la continuité des affaires (Business Continuity Management, BCM) se focalise sur le maintien et le rétablissement de processus de gestion critiques en cas de panne des systèmes informatiques ou de catastrophe afin de pouvoir rapidement reprendre l'activité économique. La gestion de la continuité des affaires, dont l'efficacité et l'exhaustivité doivent être attestées, relève de la responsabilité du prestataire de services sur le cloud. Un indicateur fort pour cela est l'obtention de la certification ISO 22301.

La récupération de données et applications (Disaster Recovery Planning) est aussi d'une importance capitale en cas de perte de données ou de panne des systèmes informatiques. Pour cela, le prestataire de services sur le cloud doit disposer d'une stratégie de sauvegarde des données, étant donné qu'il est responsable de la sauvegarde et de la récupération des données et systèmes. Les détails concernant la sauvegarde doivent être réglés dans le cadre du SLA[2] entre le prestataire de services sur le cloud et le médecin.

2 Voir aussi «Contrat-cadre de services en nuage (services cloud)» de la FMH: www.fmh.ch/fr/themes/ehealth/informatique-cabinet-medical.cfm#i137122

Exigences		
A-3.01	M	**Sauvegarde et récupération de données–processus** Les processus pour la sauvegarde (backup) et la récupération (restore) de données doivent être définis, documentés et adaptés aux exigences du client final. Les processus de récupération doivent être vérifiés à intervalles réguliers. Un protocole de test doit être mis à la disposition de l'utilisateur final à la demande de celui-ci. La sauvegarde de données doit s'effectuer sous forme cryptée et correspondre à l'état actuel de la technique.
A-3.02	M/S	**Gestion de la continuité des affaires** Le prestataire de services sur le cloud doit prouver vis-à-vis de l'utilisateur que le service dispose d'une gestion de la continuité des affaires efficace. Il peut par exemple le faire par le biais d'une certification selon ISO 22301.

E4 Sécurité des données et gestion du cycle de vie de l'information

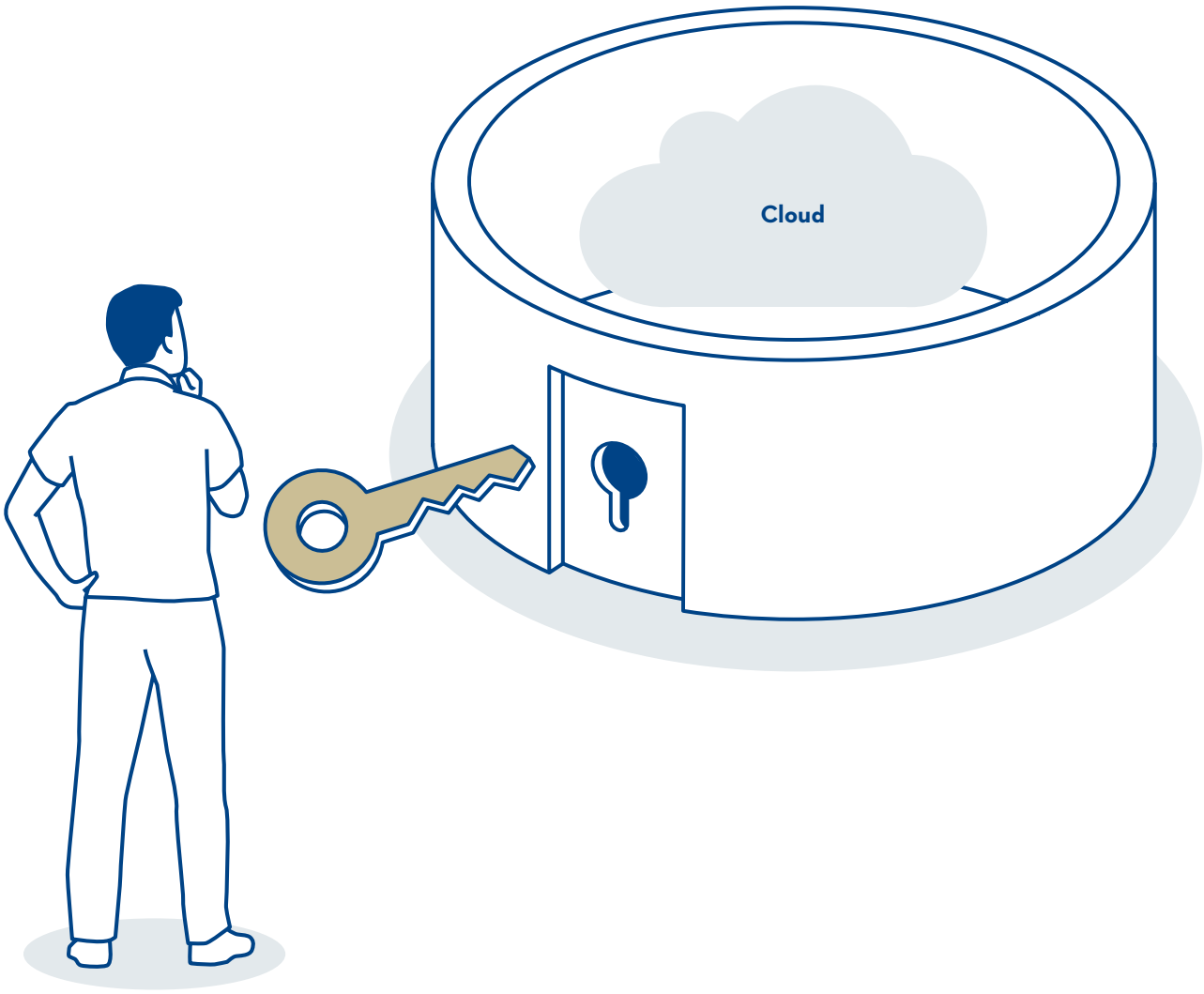


La gestion du cycle de vie de l'information (Information Lifecycle Management, ILM) désigne un ensemble de stratégies mises en place pour gérer les données, y compris leurs métadonnées. Elle permet de s'assurer que les dispositions légales sont respectées tout au long du cycle de vie des données, de leur saisie à leur suppression ou à leur archivage. Ces dispositions comprennent par exemple les délais légaux (cantonaux) de conservation et de prescription pour les dossiers médicaux ou les droits à la portabilité des données ou à l'oubli inscrits dans le règlement général de l'UE sur la protection des données.

Exigences

A-4.01	M	**Portabilité et exportation de données** L'exportation de données dans des formats électroniques standard permettant leur traitement ultérieur doit être possible à intervalles réguliers ou à l'expiration du contrat. Idéalement, le service sur le cloud dispose d'une fonctionnalité qui permet d'exporter les données sans le concours du prestataire de services sur le cloud.
A-4.02	M	**Suppression de données** Le prestataire de services sur le cloud doit, en tenant compte de l'obligation de conserver, procéder à la suppression complète des données de contenu et secondaires, y compris les copies de sauvegarde de l'utilisateur, dans les cas suivants: – en cas de changement des dispositifs de stockage à des fins d'entretien – sur demande de l'utilisateur de services sur le cloud – en cas de résiliation du contrat Les méthodes employées à cet effet, par exemple l'écrasement répété de données ou la suppression de la clé, empêchent la récupération des données avec des moyens forensiques.
A-4.03	M	**Demande de renseignements** L'utilisateur de services sur le cloud doit s'assurer que le prestataire puisse garantir les demandes de renseignements selon l'art. 8 LPD et de retrait du consentement pour le traitement de données, de telle manière que le prestataire de services sur le cloud puisse fournir des renseignements sur l'ensemble des données personnelles disponibles ou, en cas de retrait du consentement, intégralement supprimer les données personnelles.

E5 Sécurité physique

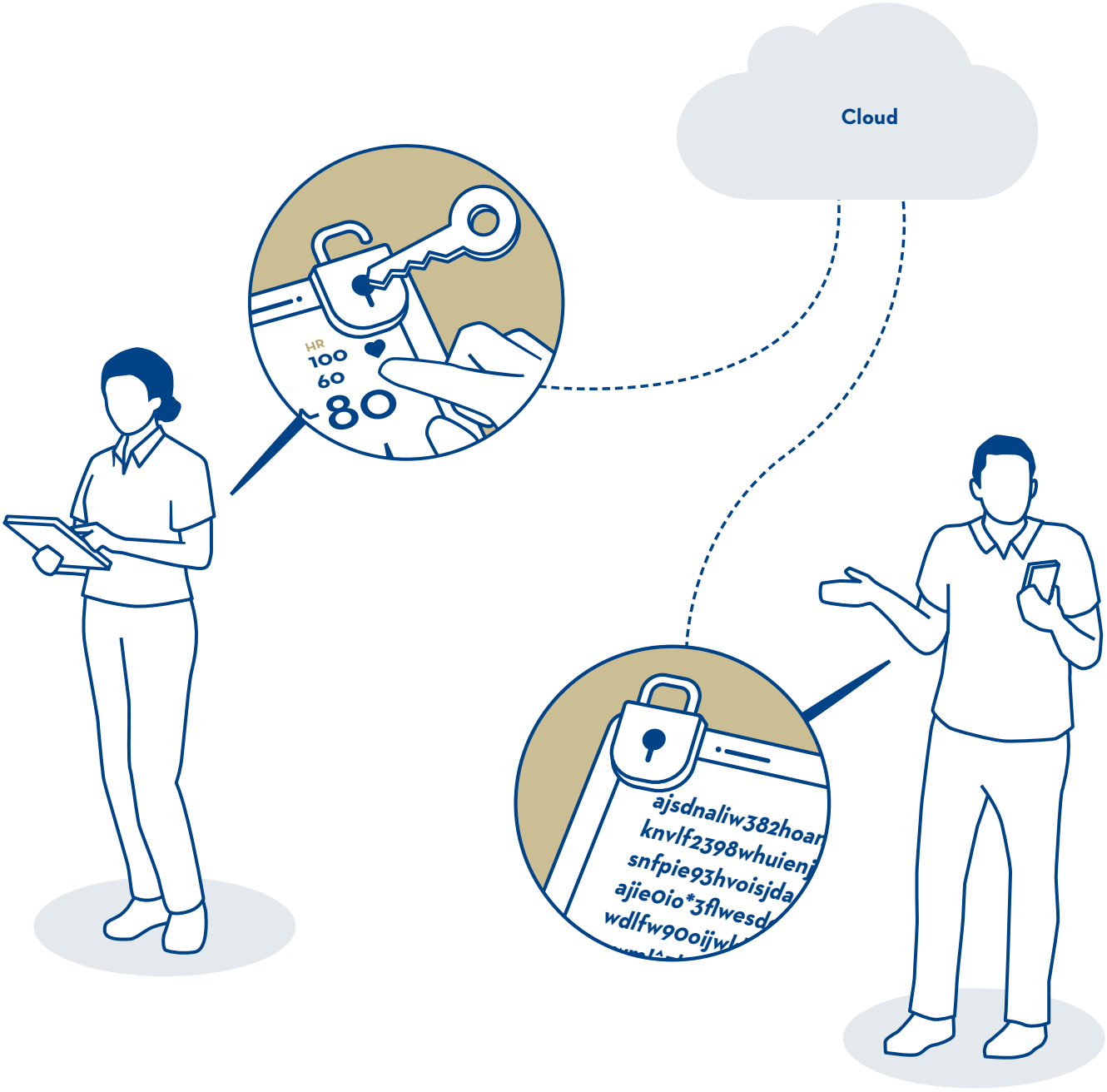


Pour garantir une sécurité physique suffisante, il est essentiel que les responsabilités des collaborateurs du prestataire de services sur le cloud soient clairement définies et que des mesures pour assurer la protection physique du centre de calcul soient implémentées.

Exigences

A-5.01	M	**Accès physique au centre de données** L'accès physique aux ressources d'information par les utilisateurs et collaborateurs du prestataire de services sur le cloud doit être limité. Des mesures de sécurité physiques doivent être implémentées, par exemple des mécanismes d'identification physique et des systèmes électroniques de surveillance et d'alarme.

E6 Cryptage et gestion des clés



Les données non cryptées sur le cloud ou des droits d'accès trop larges peuvent mettre en péril la confidentialité, l'intégrité et la disponibilité des données. Pour réduire le risque d'une violation de la confidentialité et de l'intégrité des données, les données stockées (données au repos) et les données transmises (données en transit) doivent être protégées par un procédé cryptographique correspondant.

Exigences

A-6.01	M	**Cryptage de mémoire des données de contenu (données au repos)** Les données du prestataire de services sur le cloud doivent être enregistrées sous forme cryptée dans chaque phase du cycle de vie des données. Les clés privées utilisées pour le cryptage doivent être communiquées exclusivement à l'utilisateur de services sur le cloud. Le prestataire de services sur le cloud ne doit en aucun cas avoir accès aux données.
A-6.02	M	**Gestion des clés** Un procédé de restauration efficace doit exister pour pouvoir récupérer les données cryptées en cas de besoin. S'il est nécessaire de récupérer la clé, il existe un procédé de restauration efficace. Une possibilité est de distribuer des clés partielles à différents acteurs. Celles-ci sont alors conservées dans un coffre-fort et utilisées en cas de besoin selon un processus de consensus.
A-6.03	M	**Cryptage de transport (données en transit)** La communication doit s'effectuer par un protocole internet standard actuel. La communication sur toutes les connexions entrantes et sortantes vers et à partir de l'infrastructure sur le cloud, y compris les interfaces à l'intérieur de l'infrastructure sur le cloud, doit être authentifiée et cryptée. La communication doit au minimum être cryptée avec TLS 1.2.
A-6.04	M	**Procédé de cryptage** Des procédés de cryptage conformes à la meilleure pratique actuelle doivent être utilisés. Les procédés ci-après ou des procédés équivalents sont autorisés. – Procédés de hachage: SHA2-256, SHA2-384, SHA2-512 ou SHA3-256, SHA3-384, SHA3-512 – Procédés symétriques: AES-256 – Procédés asymétriques: RSA-2048, ECDSA-224 ou Ed25519 Les procédés adaptés ou développements propres au prestataire ne sont pas autorisés. Il faut utiliser des protocoles actuels. Des protocoles comportant des failles de sécurité critiques connues ne doivent pas être utilisés.

E7 Gouvernance et gestion des risques

La gouvernance (le pilotage) de la sécurité des données et de la protection des données comprend les domaines exigences, processus et contrôle interne pour valider si les conditions concernant la protection des données et la sécurité des données sont respectées par le prestataire de services sur le cloud. Le prestataire de services sur le cloud déclare s'il dispose d'un système de gestion de la sécurité de l'information (SGSI). L'attribution des responsabilités tant pour la protection et la sécurité des données que pour la gestion des risques entre l'utilisateur de services sur le cloud et le prestataire dépendent du modèle de services choisi.

Exigences

A-7.01	S	**Certifications transparentes** Le prestataire de services sur le cloud doit mettre à disposition les certificats et rapports d'audit disponibles: – certification selon ISO/IEC 27001, – rapports d'audit selon ISAE340, SSAE16 ou rapports SOC2, – preuve relative au respect de la protection des données acceptée par les autorités de protection des données compétentes.
A-7.02	M	**Droit d'audit** Si le prestataire de services sur le cloud n'est pas en mesure de présenter des rapports d'audit de tiers, il doit garantir contractuellement à l'utilisateur que celui-ci ou un tiers mandaté peut procéder aux audits ou vérifications techniques (p. ex. tests d'intrusion).
A-7.03	M	**Accord de niveau de service (SLA)** Le SLA entre le prestataire de services sur le cloud et l'utilisateur doit couvrir le niveau de service pour le client final (le cabinet médical).
A-7.04	S	**Reporting SLA** Sur demande, le prestataire de services sur le cloud doit mettre à disposition un rapport comportant au moins les données suivantes: – chiffres clés sur la disponibilité, la performance ou la capacité de données du service – temps de réponse et de réaction de l'organisation de service du prestataire – définition de fenêtres de maintenance et d'autres temps d'arrêt planifiés – définition de la fréquence et de la qualité des processus de maintenance – définition des objets livrés tels que rapports de test ou médias de sauvegarde – mesures et conséquences en cas de non-respect des accords – évènements et incidents durant la période sous revue
A-7.05	M	**Sous-traitants** Le prestataire de services sur le cloud doit communiquer la liste de tous les sous-traitants à l'utilisateur et apporter une preuve du respect de l'obligation de confidentialité[3].
A-7.06	M	**Notification en cas d'arrêts planifiés** Le prestataire de services sur le cloud doit informer par courriel l'utilisateur des temps d'arrêt prévus au moins dix jours ouvrables à l'avance.

3 Voir aussi: «Contrat-cadre de services en nuage (services cloud)» www.fmh.ch/files/doc3/contrat-cadre-de-services-en-nuage-services-cloud-word.docx et annexes incluses

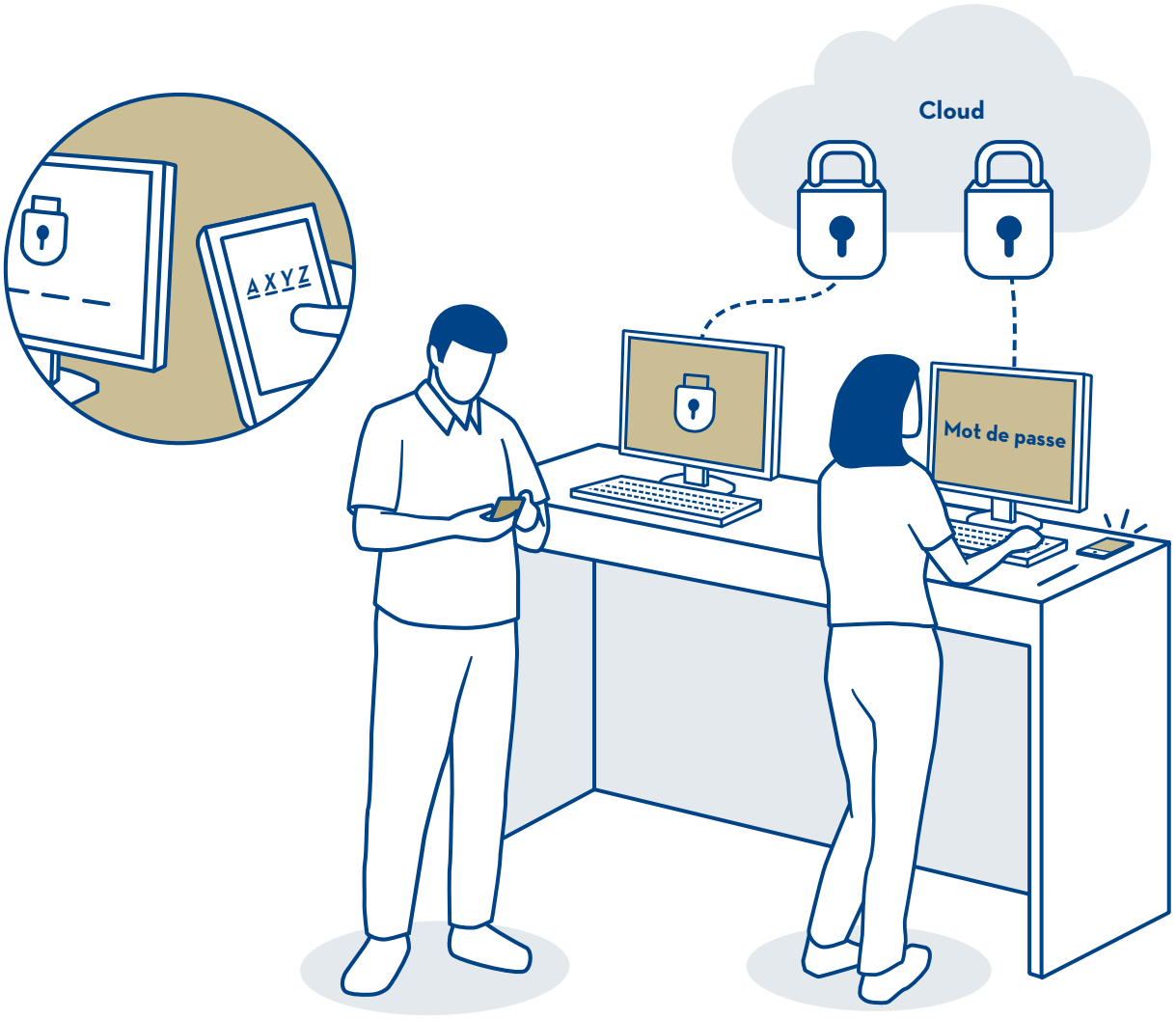
E8 Personnel

Le personnel joue un rôle important dans le domaine de la sécurité de l'information. Le but de cette exigence est de réduire le risque d'une mise en péril de la confidentialité, de la disponibilité ou de l'intégrité des données par le personnel du prestataire de services sur le cloud.

Exigences

A-8.01	**M**	**Contrats de travail** Les contrats de travail du prestataire de services sur le cloud doivent inclure des dispositions relatives au respect des directives en matière de protection des données et de sécurité de l'information.
A-8.02	**M**	**Formation et sensibilisation** Les collaborateurs du prestataire de services sur le cloud doivent régulièrement bénéficier d'une formation et sensibilisation concernant la protection des données et la sécurité de l'information.

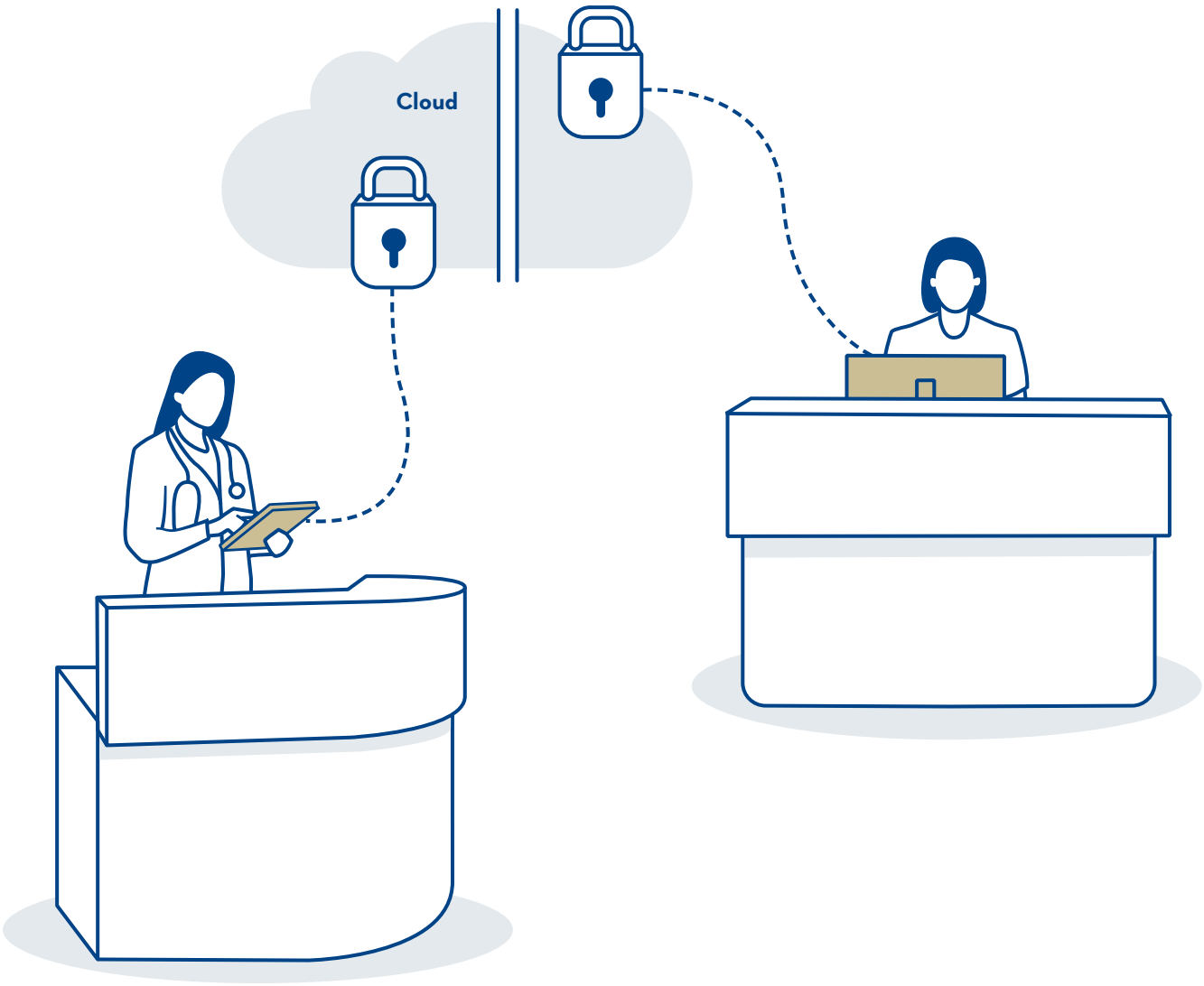
E9 Gestion de l'identité et de l'accès



Le contrôle de l'accès aux données est une mesure efficace pour prévenir tout accès non autorisé à des informations sensibles et protéger l'intégrité des données. Pour ce faire, il faut tenir compte du principe «Need to know» ou «Least Privilege». La mise en œuvre de l'authentification peut s'effectuer par un procédé à facteur simple ou à facteurs multiples.

Exigences		
A-9.01	M	**Authentification des utilisateurs (utilisateurs de services sur le cloud)** L'authentification des utilisateurs de services sur le cloud doit s'effectuer par une authentification à facteurs multiples.
A-9.02	M	**Authentification des administrateurs (utilisateurs de services sur le cloud)** L'authentification des administrateurs de services sur le cloud doit s'effectuer par une authentification à facteurs multiples.
A-9.03	M	**Récupération des données d'accès** Un processus efficace pour récupérer les données d'accès doit être à disposition comme solution de secours.
A-9.04	S	**Identity Provider** Il faut s'assurer que l'intégration d'un fournisseur d'identité externe dans la solution sur le cloud soit possible.
A-9.05	S	**Accès avec authentification unique** Un protocole d'accès avec authentification unique tel que OAuth 2.0 doit être supporté pour améliorer la sécurité et la convivialité.
A-9.06	M	**Connexion de l'Identity-Store à l'Active Directory (AD) du cabinet médical** Une connexion avec l'Identity Store du cabinet médical doit être possible, si existant. La connexion doit être aménagée de manière à ce que seules les données nécessaires (principe «Need to know») soient mises à la disposition du prestataire de services sur le cloud. Les mots de passe AD ne doivent cependant pas être sauvegardés chez le prestataire de services sur le cloud.
A-9.07	S	**Authentification machine à machine** Un procédé basé sur un certificat doit être utilisé pour l'authentification de machine à machine.
A-9.08	M	**Accès par les administrateurs du prestataire de services sur le cloud** Il faut s'assurer que les administrateurs du prestataire de services sur le cloud n'aient pas accès aux données non cryptées de l'utilisateur.
A-9.09	M/S	**Accès à l'administration** Les accès administratifs par le prestataire de services sur le cloud doivent s'effectuer à partir d'un réseau dédié ou être sécurisés par un procédé d'authentification à facteurs multiples. Tous les accès administratifs doivent être consignés et, si nécessaire, pouvoir être consultés par l'utilisateur de services sur le cloud.

E10 Sécurité de l'infrastructure sur le cloud et de l'environnement de virtualisation



La sécurité de l'infrastructure sur le cloud et de l'environnement de virtualisation comprend les thèmes sécurité du réseau, protection de l'utilisation, sécurité de l'hyperviseur, du conteneur et des réseaux logiciels.

Exigences

A-10.01	M	**Conservation des données séparée** Suivant l'architecture choisie et les documents mis à disposition, le prestataire de services sur le cloud doit prouver que le service sur le cloud proposé garantit une séparation logique et appropriée des données par rapport aux données d'autres utilisateurs (séparation des entités). Le prestataire de services sur le cloud doit préalablement mettre à disposition un interlocuteur compétent pour les questions techniques. Les documents suivants doivent être mis à disposition par le prestataire de services sur le cloud: – architecture du système – documentation du système – manuel d'utilisation – concept de sécurité – concept d'urgence/BCM
A-10.02	M	**Sécurité du réseau** Pour protéger le réseau, le prestataire de services sur le cloud doit prévoir: – un pare-feu, – des systèmes de détection et de prévention d'intrusions, – un pare-feu d'applications (XML/WAF) et – une protection contre les attaques par déni de service distribué.
A-10.03	M	**Protection contre les maliciels** Afin d'assurer la protection contre les maliciels, le prestataire de services sur le cloud doit prévoir des logiciels antivirus et/ou des systèmes de détection d'intrusions au niveau du modèle de services et du périmètre du réseau.

E11 Interopérabilité et portabilité des composants d'application

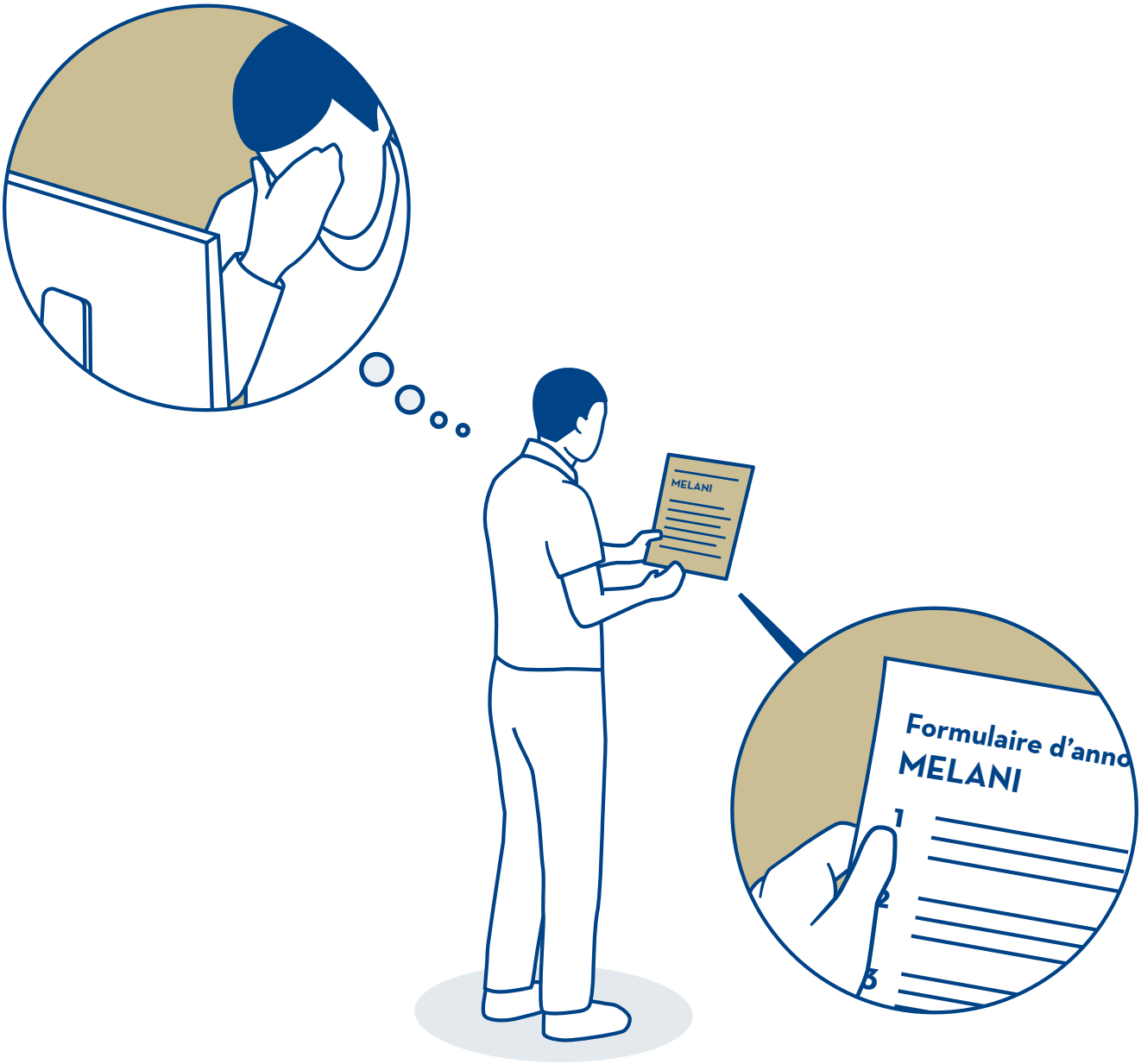
L'interopérabilité est la condition pour que les composants d'un écosystème sur le cloud puissent interagir. Les composants d'un tel écosystème peuvent provenir de différentes sources, tant du cloud que de composants traditionnels sur site. L'interopérabilité exige que ces composants puissent être remplacés par d'autres ou de nouveaux composants de différents prestataires tout en continuant de fonctionner.

La portabilité définit la simple possibilité de déplacer des composants d'application à un autre endroit et de les réutiliser, indépendamment du prestataire, de la plate-forme, du système d'exploitation, de l'infrastructure, du site, de la mémoire, du format de données ou des interfaces de programmation applicative (API).

Exigences

A-11.01	M	**Virtualisation** Le prestataire de services sur le cloud doit utiliser une plate-forme de virtualisation et des formats de virtualisation normalisés (p. ex. OVF) pour assurer l'interopérabilité.
A-11.02	S	**Interfaces de programmation applicative (API)** Le prestataire de services sur le cloud doit utiliser des API ouvertes publiques pour appuyer l'interopérabilité entre les composants et faciliter la migration d'applications.
A-11.03	M	**Protocoles réseau standardisés** Le prestataire de services sur le cloud doit utiliser des protocoles réseau standardisés pour l'importation et l'exportation de données et la gestion du service. Le prestataire de services sur le cloud doit mettre à disposition un aperçu des standards d'interopérabilité et de portabilité utilisés.

E12 Gestion des incidents, recherche électronique et forensique sur le cloud



Le terme de la gestion des incidents de sécurité englobe la détection, le traitement, la notification et la suppression des incidents de sécurité.

Exigences

A-12.01	M/S	**Gestion des incidents de sécurité du prestataire de services sur le cloud** Le prestataire de services sur le cloud doit présenter une gestion des incidents de sécurité. Pour cela, le prestataire de services sur le cloud devra par exemple présenter une certification selon ISO/IE 27035.
A-12.02	M	**Notification d'incidents de sécurité** Le prestataire de services sur le cloud doit informer l'utilisateur en l'espace de 72 heures des incidents de sécurité détectés qui pourraient le concerner.
A-12.03	M/S	**Point de contact pour les incidents de sécurité** Le prestataire de services sur le cloud doit communiquer à l'utilisateur un point de contact pour les incidents de sécurité.

E13 Gestion des menaces et vulnérabilités

Des prescriptions relatives à la protection et des processus de surveillance sont nécessaires pour éviter que l'infrastructure informatique, les composants du système ou les terminaux soient touchés par des maliciels.

Exigences

A-13.01	M/S	**Attestation relative à la vérification technique (p. ex. analyse des vulnérabilités ou test d'intrusion)** Le prestataire de services sur le cloud doit régulièrement procéder à une vérification technique par un service indépendant et mettre les résultats à la disposition de l'utilisateur. Cette vérification technique doit être réalisée au moins une fois par année.
A-13.02	S	**Enregistrement des évènements liés à la sécurité** Le service sur le cloud doit au minimum permettre d'enregistrer les informations suivantes sur les évènements liés à la sécurité: – décisions d'accès – comportement de charge – modifications des données d'utilisation
A-13.03	S	**Conservation des données de protocole** Le prestataire de services sur le cloud doit conserver tous les protocoles pendant au moins six mois[4] et les mettre à la disposition de l'utilisateur. Les six mois s'appliquent pour autant qu'aucune autre disposition légale n'existe. Par ailleurs, la réglementation selon A-4.02 concernant la suppression de données doit aussi être respectée pour les données de protocole.

4 Ces six mois ont valeur de recommandation. Les délais plus longs sont souvent problématiques pour les prestataires de services sur le cloud. Des délais plus courts peuvent entraîner une perte d'informations importantes dont on peut avoir besoin en cas d'incident constaté après coup (perte de données, accès non autorisé).

Annexe

Glossaire

Active Directory Technologie de Microsoft qui regroupe différents services pour gérer les autorisations et l'accès aux ressources réseau.

Application Firewall (pare-feu d'applications) Pare-feu qui pilote l'entrée et la sortie ainsi que l'accès à une application ou à un service.

Application Programming Interface (API) (interface de programmation applicative) Interface technique d'un programme par laquelle il communique avec d'autres logiciels.

Authentification à facteurs multiples Authentification signifie vérification qu'une personne est bien celle qu'elle prétend être. À facteurs multiples signifie que cela se fait au moyen de plusieurs caractéristiques indépendantes.

Backup (sauvegarde) Copie de données sur un support à partir duquel elles peuvent être récupérées en cas de panne ou d'autres évènements.

Client Ordinateur fixe ou poste de travail pouvant recevoir des informations et applications d'un serveur.

Container (conteneur) Unité de logiciels qui rassemble les codes et toutes leurs dépendances pour que l'application puisse facilement être déplacée d'un environnement informatique vers un autre et exécutée. Contrairement à une machine virtuelle (MV), un conteneur ne possède pas de système d'exploitation ou noyau propre.

Gateway (passerelle) Une passerelle est un nœud dans un réseau qui sert d'accès vers un autre réseau.

Hypervisor (hyperviseur) Composante qui crée et exécute une machine virtuelle. Les hyperviseurs permettent d'exploiter plusieurs systèmes invités sur un seul système hôte.

On-Premise (sur site) Modèle d'utilisation et de licence pour des programmes informatiques basés sur serveur (logiciels). Le logiciel est acheté par l'utilisateur et normalement exploité par celui-ci. Contrairement au système sur demande (On-Demand-Service) où l'utilisateur ne se charge pas lui-même de l'exploitation, mais confie cette tâche par exemple au prestataire de services sur le cloud.

RSA Procédé cryptographique asymétrique qui peut être utilisé pour le cryptage et la signature numérique.

Single Sign-on (SSO, accès avec authentification unique) Single Sign-on signifie qu'un utilisateur peut, après s'être identifié à son poste de travail, accéder à tous les ordinateurs et services pour lesquels il dispose d'une autorisation locale, à partir du même poste de travail, sans devoir s'enregistrer individuellement pour chaque service.

Test d'intrusion Cyberattaque autorisée et simulée lancée contre un système pour évaluer la sécurité du système.

Transport Layer Security (TLS) / Secure Sockets Layer (SSL) Secure Sockets Layer est un protocole hybride pour la transmission cryptée et sécurisée de données sur internet. TLS est le successeur du Secure Sockets Layer.

Web Service Permet la communication de machine à machine sur la base de réseaux de calcul HTTP ou HTTPS.

Abréviations

AD	Active Directory
API	Application Programming Interface
BCM	Gestion de la continuité des affaires (angl. Business Continuity Management)
CSA	Security Guidance – For Critical Areas of Focus in Cloud Computing V4.0 der Cloud Security Alliance.
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ISO	International Standards Organisation – l'organisme international de normalisation
LPD	Loi fédérale sur la protection des données
OVF	Open Virtualization Format
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SSO	Single Sign-on
TIC	Technique de l'information et de la communication (angl. Information and Communication Technology)
TLS	Transport Layer Security
WAF	Web Application Firewall

Impressum
Éditrice: FMH – Fédération des médecins suisses, Berne
Texte: Redguard AG, Berne; ti&m AG, Zurich
Graphisme/illustration: Hahn+Zimmermann, Berne
Publication: mai 2020
www.fmh.ch


ajsdnaliw382hoan
knvlf2398whuienj
snfpie93hvoisjda
ajie0io*3flwesd
wdlfw90oijwl