Utilisation du cloud dans le secteur hospitalier et de la santé : ce qu'il faut savoir et prendre en compte

Un aperçu pratique de l'utilisation du cloud par les établissements de santé

Version 1.1, août 2026

Auteurs (en ordre alphabétique) : Erik Dinkel, Stefan Hunziker, Stefan Juon, Philipp Stoll, Werner Ulmer

Contenu

Introduction

Le présent document fournit aux établissements de santé une base objective et indépendante pour la gestion des solutions cloud. Il ne traite volontairement ni de prestataires ou de produits spécifiques et ne prend pas position sur l'utilisation du cloud.

L'objectif est de fournir aux établissements de santé une base leur permettant d'aborder de manière autonome et responsable la question de l'utilisation du cloud. À cet effet, le document donne un aperçu des principaux aspects et des considérations à prendre en compte. La première partie s'adresse à toutes les personnes qui s'intéressent à l'utilisation du cloud. La deuxième partie aborde des cas d'usage concrets ainsi que des aspects techniques et s'adresse principalement aux spécialistes.

Management summary

Les établissements de santé ont un mandat de prestation pour la prise en charge des patient·e·s. Celui-ci doit être assuré de manière efficace, appropriée, économique et compétitive. En outre, les établissements de santé font partie des infrastructures critiques de la Suisse et doivent, à ce titre, garantir la sécurité de l'approvisionnement. Des systèmes ICT résilients constituent une condition indispensable à cet effet. L'utilisation des services cloud joue ici un rôle central et est tout simplement nécessaire. Dans une société de plus en plus numérique et interconnectée, où de nombreuses applications et services ne peuvent être utilisés qu'en ligne, l'usage du cloud est une réalité. Une médecine moderne et des systèmes résilients sans recours au cloud ne sont plus possibles.

Les hyperscalers (grandes entreprises opérant à l'échelle mondiale qui fournissent des services cloud) sont des acteurs centraux et non substituables. Eux seuls disposent de la capacité d'échelle, de la force d'innovation, du personnel spécialisé et des produits interopérables en nombre et en taille nécessaires. La question n'est donc pas de savoir s'il faut utiliser ou non les services des hyperscalers, mais quels services peuvent être utilisés et comment. Il convient, selon les différents cas d'usage, de respecter les exigences légales et d'identifier, d'évaluer et de réduire à un niveau acceptable les risques liés à leur utilisation. Chaque organisation, et donc chaque établissement de santé, doit décider de manière autonome si certains services doivent être exploités localement ou via des solutions cloud.

Outre les risques spécifiques aux applications et aux organisations, il existe deux risques centraux dont il faut être pleinement conscient : le verrouillage fournisseur (vendor lock-in) et la défaillance du système. Si l'infrastructure ICT d'une organisation repose entièrement ou en grande partie sur les services cloud d'un seul fournisseur et que celui-ci n'est pas réellement substituable, un changement de fournisseur, s'il est possible, implique des coûts considérables en termes financiers, humains et temporels. Une défaillance d'un tel fournisseur, par exemple à la suite d'une cyberattaque ou d'un autre événement, aurait des conséquences graves pour toutes les organisations utilisant ses services.

Si, par exemple, les services de vidéoconférence, de téléphonie et de messagerie électronique de tous les établissements de santé reposaient sur l'infrastructure d'un seul fournisseur et que celui-ci venait à tomber en panne, tous les établissements de santé en Suisse ne seraient plus joignables par ces canaux. L'utilisation des services cloud augmente donc non seulement la résilience des systèmes ICT, mais peut aussi la compromettre dans les cas décrits. Il est dès lors indispensable de prévoir des redondances et des plans de contingence.

Renoncer aux services cloud, de manière générale et dans le domaine médical en particulier, n'est ni pertinent ni possible si les établissements de santé, en tant que partie des infrastructures critiques, doivent continuer à remplir leur mandat de prestation au bénéfice des patient·e·s et à garantir la sécurité de l'approvisionnement en soins en Suisse. Le présent document constitue une aide d'orientation pour les établissements de santé dans leur réflexion et dans une utilisation des services cloud adaptée aux risques.

Partie générale – État des lieux et cadre général

1 Introduction à l'utilisation du cloud

L'utilisation des services cloud est depuis longtemps une réalité dans un monde de plus en plus numérique. La numérisation s'impose progressivement dans le secteur de la santé, qui est déjà — ou sera dans un avenir proche — inconcevable sans solutions numériques. Il en résulte de nouveaux potentiels et de nouvelles opportunités dont bénéficieront à la fois la société dans son ensemble et les individus. Les solutions cloud constituent un élément central de cet univers numérique, avec les opportunités et les risques qui y sont associés.

Entre mandat de prestations et transformation numérique

Dans le cadre de leur mandat et des conventions de prestations correspondantes, les établissements de santé assurent la prise en charge des patient·e·s, laquelle doit être efficace, appropriée, économique et compétitive dans la région qui leur est attribuée. Une interconnexion croissante avec les prestataires en amont et en aval, visant une prise en charge aussi intégrée que possible, est au cœur de cette évolution. Selon le Conseil fédéral, les établissements de santé font partie des infrastructures critiques. Afin de pouvoir remplir leur mission en situation de crise, des systèmes ICT résilients sont nécessaires — les services cloud y sont particulièrement adaptés. À cela s'ajoute l'évolution du marché : de nombreuses applications et services ne sont désormais plus proposés sur la propre infrastructure locale « on premise ».

L'analyse de la thématique de l'utilisation du cloud est donc incontournable pour les établissements de santé. Le présent document vise à servir de guide d'orientation et à permettre une réflexion structurée et différenciée sur le sujet.

Structure du document

La première partie du présent document s'adresse aux décideur·euse·s des établissements de santé ainsi qu'à toute personne s'intéressant à l'utilisation de solutions cloud. Elle couvre les thèmes suivants :

- Les différentes formes de solutions cloud
- Le rôle des hyperscalers et le mythe du « Swiss Cloud »
- L'évolution des solutions cloud
- Les considérations juridiques liées au cloud
- Le cas particulier du US Cloud Act
- Les considérations économiques liées au cloud

La deuxième partie du document s'adresse aux personnes qui s'occupent de la mise en œuvre concrète des solutions cloud. Elle couvre les thèmes suivants :

- L'importance du cloud pour le backup et le recovery
- Cloud only vs. utilisation hybride
- Cas d'usage
- Mesures techniques et organisationnelles
- Chiffrement et gestion des clés

2 Différentes formes de solutions cloud

Les services cloud ou le cloud computing désignent la mise à disposition de ressources informatiques — telles que la puissance de calcul, le stockage, les logiciels applicatifs et les bases de données — via Internet. Contrairement aux modèles informatiques traditionnels, dans lesquels les entreprises doivent exploiter leurs propres serveurs et infrastructures, les services cloud permettent de recourir à des prestataires tiers pour assumer ces tâches.

Le cloud offre de nombreux avantages, notamment en matière de scalabilité, de flexibilité, de fiabilité et de réduction des coûts. Les entreprises peuvent adapter rapidement et facilement les ressources dont elles ont besoin, sans devoir investir dans des infrastructures ou du personnel. En outre, le cloud computing permet d'accéder à un éventail plus large d'applications et de les déployer plus rapidement. Dans l'ensemble, il constitue une solution innovante pour les organisations souhaitant moderniser et optimiser l'utilisation de leur infrastructure ICT.

Le cloud computing est une approche permettant de fournir et d'utiliser des services informatiques de manière dynamique et adaptée aux besoins via un réseau. Les ressources mises à disposition sont regroupées dans un pool et peuvent être rapidement sollicitées et gérées avec un effort minimal, voire une interaction réduite avec le fournisseur. La facturation s'effectue sur la base de l'utilisation mesurée.

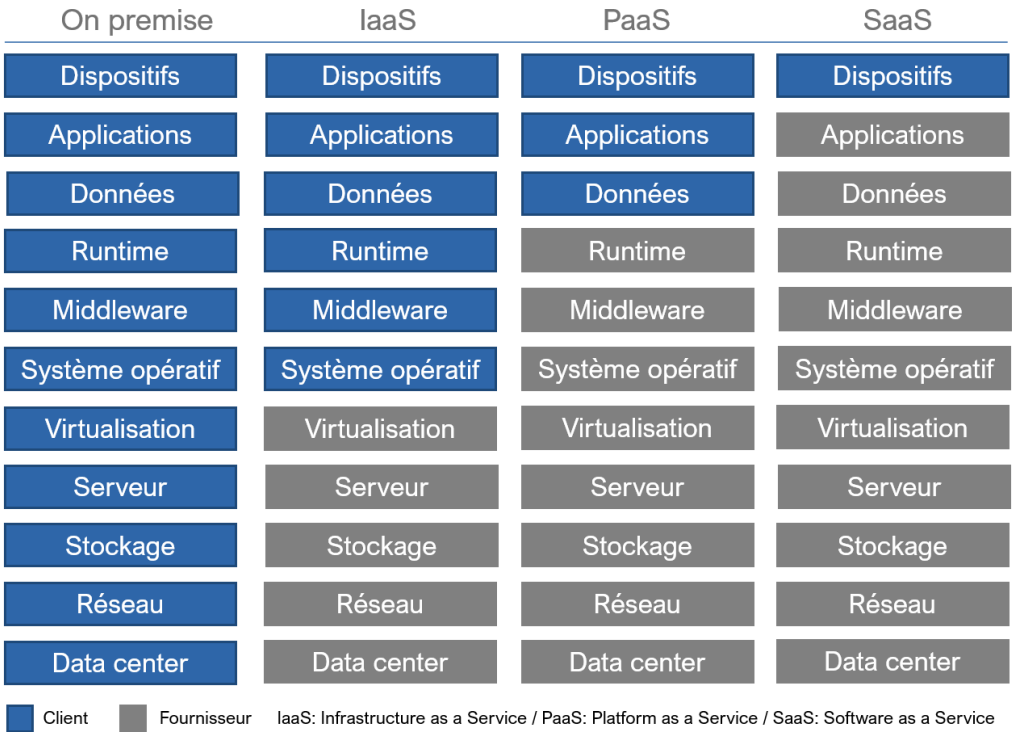
Modèles cloud : IaaS, PaaS, SaaS

Selon les services fournis et les responsabilités assumées, les services cloud peuvent être distingués en trois modèles :

- Infrastructure-as-a-Service (IaaS): ce modèle fournit des composants d'infrastructure informatique de base tels que la puissance de calcul, le stockage et les ressources réseau via Internet. Les client·e·s peuvent exécuter leurs propres applications et systèmes d'exploitation sur ces infrastructures.
- Platform as a Service (PaaS) : ce modèle offre aux développeur·euse·s une plateforme pour créer, exécuter et gérer des applications sans avoir à se soucier de l'infrastructure sous-jacente.
- Software as a Service (SaaS) : ces services permettent aux utilisateur·trice·s d'accéder à des applications logicielles via Internet. Les applications sont hébergées et maintenues par des prestataires tiers, tandis que les client·e·s les utilisent en ligne.

Ces modèles se caractérisent notamment par une répartition différente des responsabilités entre le fournisseur cloud et le client.

Aperçu des différents types de services cloud en comparaison avec les systèmes locaux (« on-prem ») :



3 Le rôle des hyperscalers et le mythe du « Swiss Cloud »

Les hyperscalers sont de grandes entreprises opérant à l'échelle mondiale, qui fournissent des services de cloud computing à très grande échelle. Parmi les hyperscalers les plus connus figurent Amazon Web

Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud et Alibaba Cloud. Ces entreprises exploitent d'immenses centres de données à travers le monde afin de fournir des infrastructures IT et des services cloud.

Les hyperscalers : le moteur du marché du cloud computing

Le rôle des hyperscalers sur le marché du cloud computing est devenu de plus en plus important ces dernières années. Les organisations qui dépendent de services cloud recherchent souvent des solutions rapides, évolutives et fiables. Les hyperscalers sont en mesure de répondre à ces exigences grâce à l'exploitation de centres de données à très grande échelle, leur permettant de proposer une vaste gamme de services d'infrastructure IT et de cloud.

En recourant aux services cloud des hyperscalers, les organisations peuvent également réaliser des économies, car elles n'ont pas à investir massivement dans leur propre infrastructure IT. Les hyperscalers offrent en outre un large éventail de services, notamment l'Infrastructure as a Service (IaaS), la Platform as a Service (PaaS) et le Software as a Service (SaaS), que les organisations peuvent utiliser selon leurs besoins.

Par ailleurs, les hyperscalers disposent d'un haut niveau d'expertise et de technologies pour accompagner les client·e·s dans le développement, la mise en œuvre et la gestion des services de cloud computing. Cela en fait une option clé pour les organisations souhaitant rester compétitives dans l'environnement économique actuel.

Dans l'ensemble, les hyperscalers sont devenus indispensables dans le monde actuel du cloud computing. Sans eux, il serait plus difficile pour les organisations de réagir rapidement et de manière flexible aux exigences du marché.

« Swissness » dans le contexte cloud

Les termes « Swiss Cloud » et « Swissness » se réfèrent à des services cloud proposés par des entreprises suisses et hébergés en Suisse. Il existe une perception selon laquelle ces services offrent des standards plus élevés en matière de protection des données, de sécurité et de confidentialité que ceux proposés par d'autres fournisseurs.

Il est important de noter que la « Swissness » ne constitue pas un label ou une certification officiellement reconnue. Il existe néanmoins plusieurs raisons pour lesquelles les services cloud suisses sont souvent considérés comme particulièrement sûrs et fiables. La Suisse dispose de lois strictes en matière de protection des données et de normes élevées en matière de vie privée et de sécurité des données. Elle bénéficie également d'une stabilité politique, bd'un haut degré de sécurité juridique et d'une neutralité reconnue, ce qui renforce la confiance.

En outre, les entreprises suisses jouissent souvent d'une solide réputation en matière de qualité et de fiabilité, ce qui peut contribuer à renforcer la confiance dans leurs services cloud.

Cela ne signifie toutefois pas que tous les services cloud suisses sont automatiquement plus sûrs ou plus fiables que ceux d'autres fournisseurs. Il est essentiel d'examiner attentivement les caractéristiques propres à chaque service cloud afin d'identifier la solution la mieux adaptée aux besoins spécifiques d'une organisation.

4 Évolution future des solutions cloud

De nombreuses prévisions existent quant à l'évolution des services cloud. Parmi les principales tendances et évolutions figurent :

Stratégies multi-cloud : les organisations adoptent de plus en plus une combinaison de services cloud de différents fournisseurs afin d'accroître la flexibilité et la fiabilité de leur infrastructure IT.

Edge computing : le traitement des données et des applications ne se fait plus uniquement dans des centres de données centralisés, mais aussi à la périphérie (edge), c'est-à-dire à proximité des utilisateur·trice·s finaux ou des sources de données. Cela permet des temps de réponse plus rapides et de meilleures performances.

Intelligence artificielle et apprentissage automatique : les services cloud offrent une plateforme idéale pour traiter de grands volumes de données et exécuter des algorithmes de machine learning. Cela permet aux organisations d'extraire des informations précieuses et de développer des applications innovantes.

Technologies de conteneurs : les conteneurs informatiques emballent et transportent des logiciels de manière standardisée (de la même façon que les conteneurs maritimes transportent des marchandises) et permettent aux organisations de gérer et de faire évoluer leurs applications de manière plus efficace et flexible, contribuant ainsi à rendre le cloud encore plus accessible.

Cloud only / hybrid cloud : les organisations adoptent de plus en plus des modèles hybrides combinant cloud public et cloud privé. Cela leur permet de bénéficier des avantages du cloud sans devoir migrer entièrement leur infrastructure IT.

Hybrid cloud / on-premise : une partie des applications et de l'infrastructure est exploitée dans le cloud, tandis qu'une autre reste opérée localement. Une variante typique consiste, par exemple, à exploiter les applications de communication et de collaboration dans le cloud, tout en maintenant localement les applications critiques liées au cœur de métier, notamment celles contenant des données structurées et sensibles. Le choix d'exploiter une application dans le cloud ou localement se fait au cas par cas, sur la base d'une analyse des opportunités, des risques, des coûts et des exigences légales.

Dans l'ensemble, l'avenir des services cloud sera marqué par l'innovation et de nouvelles technologies, permettant aux organisations d'utiliser leur infrastructure IT de manière plus efficace et efficiente. Les organisations qui recourent au cloud seront en mesure de réagir plus rapidement et avec davantage de flexibilité aux évolutions de leur environnement, renforçant ainsi leur compétitivité.

5 Considérations juridiques relatives au cloud

Le cloud computing implique toujours une externalisation et donc un traitement des données par des tiers. Celui-ci est confié contractuellement à un prestataire chargé de traiter les données pour l'établissement de santé mandant. Il ne s'agit pas d'une publication des données. Cette distinction est importante, car le traitement de données pour le compte d'autrui est soumis à des exigences différentes de celles applicables à la publication. La responsabilité des données demeure toutefois toujours auprès de l'établissement de santé mandant.

Types de données et exigences de protection

Pour une utilisation du cloud conforme au droit, la première question porte sur les données à traiter dans le cloud : de quelles données s'agit-il et quel est leur niveau de sensibilité ? Selon le type de données, les exigences juridiques et de sécurité de l'information diffèrent. Il est utile de distinguer les catégories suivantes :

- Données publiques
- Données internes à l'organisation
- Données commerciales confidentielles
- Données personnelles (pouvant être publiques, internes ou confidentielles)
- Données personnelles sensibles, telles que les données des patient·e·s

Statut des données

Lorsque les données sont soumises au secret professionnel ou au secret de fonction — comme c'est le cas des données des patient·e·s — ces obligations doivent être respectées en plus des exigences en matière de protection des données.

Une fois le type de données déterminé, il convient d'examiner leur état : sont-elles identifiables, pseudonymisées ou anonymisées ? Selon ce statut, elles continuent ou non à être considérées comme des données personnelles.

Des données sont considérées comme pseudonymisées (ou suffisamment pseudonymisées) lorsqu'elles ne peuvent être attribuées à une personne déterminée par des tiers qu'au prix d'efforts disproportionnés.

Une réidentification reste possible via une clé d'identification. Si cette clé est exclusivement détenue par le mandant, les données peuvent être considérées comme anonymisées du point de vue du prestataire.

Contrairement à la pseudonymisation, l'anonymisation est irréversible : toute identification d'une personne devient impossible. Une fois anonymisées, les données ne sont plus considérées comme des données personnelles.

Pays de stockage et de traitement

La question du lieu de stockage et de traitement des données est également déterminante : celles-ci sont-elles traitées en Suisse ou à l'étranger ?

Si les données sont traitées en Suisse, le droit suisse s'applique, y compris le secret professionnel et le secret de fonction. Selon la pratique courante, le prestataire peut être contractuellement lié à un niveau de protection équivalent, et les violations peuvent être poursuivies. Selon une interprétation juridique plus stricte, également défendue par certaines autorités de surveillance, le secret professionnel pourrait en principe s'opposer à une externalisation vers le cloud. Une telle interprétation restrictive rendrait pratiquement impossible l'utilisation du cloud par les établissements de santé pour le traitement des données des patient·e·s. Dans une société de plus en plus numérique, la question se pose alors de savoir si les établissements de santé peuvent encore remplir leur mission sans recourir au cloud.

Si les données sont traitées à l'étranger, ce n'est plus le droit suisse mais le droit du pays concerné qui s'applique, ce qui limite les possibilités de contrôle et d'exécution.

Exigences légales pour le traitement des données sensibles

Lorsque des données personnelles sensibles (par ex. données des patient·e·s) sont traitées dans le cloud, une base contractuelle est impérative du point de vue du droit de la protection des données. Le principe de finalité ainsi que celui de proportionnalité doivent être respectés : les données ne peuvent être traitées que dans le but pour lequel elles ont été confiées, et seules les données strictement nécessaires peuvent être utilisées.

Toute nouvelle opération de traitement ou toute modification substantielle concernant des données personnelles sensibles nécessite la réalisation d'une analyse d'impact relative à la protection des données. Selon la base juridique applicable (droit fédéral ou cantonal), un contrôle préalable ou une consultation de l'autorité de surveillance peut être requis.

Si les données sont traitées à l'étranger, cela n'est admissible que si le niveau de protection des données dans le pays destinataire est au moins équivalent à celui de la Suisse. Même si des garanties contractuelles peuvent être mises en place, leur mise en œuvre est plus difficile et le droit local s'applique. En raison de ce risque accru, une transparence totale ainsi qu'un consentement explicite et vérifiable des personnes concernées sont nécessaires. Les exigences légales et le devoir de diligence restent pleinement applicables.

Enfin, les données doivent toujours être protégées conformément à l'état actuel de la sécurité de l'information, notamment par des mesures telles que le chiffrement et des contrôles d'accès basés sur les rôles, tant lors de la transmission que du stockage.

6 Cas particulier du US Cloud Act

L'utilisation du cloud computing dans le cadre d'un traitement de données pour le compte d'autrui impliquant des données personnelles sensibles, notamment des données des patient·e·s, est en principe possible selon la pratique juridique courante, pour autant qu'une base contractuelle adéquate existe et que les mesures nécessaires en matière de sécurité de l'information soient mises en place. Cela vaut en particulier lorsque l'infrastructure cloud se situe en Suisse. Un cas particulier concerne toutefois l'application extraterritoriale du US Cloud Act.

Selon cette législation, les autorités américaines peuvent, dans le cadre d'une procédure pénale en cours contre une personne, exiger l'accès aux données de cette personne auprès d'entreprises ayant un lien avec les États-Unis. Ainsi, lorsqu'une organisation — y compris un établissement de santé — traite des données dans le cloud auprès d'un fournisseur ayant un lien avec les États-Unis, les autorités américaines

peuvent potentiellement accéder à ces données, même si l'infrastructure cloud utilisée est située en Suisse.

Le traitement de données des patient·e·s par un fournisseur cloud ayant un lien avec les États-Unis est donc problématique du point de vue de la protection des données et doit faire l'objet d'une analyse individuelle approfondie. De manière générale, et en particulier dans le cas de fournisseurs cloud ayant un lien avec les États-Unis, il est essentiel de définir et de spécifier au préalable les cas d'usage concrets. Sur cette base, il convient d'évaluer les risques, les opportunités et les coûts, ainsi que de vérifier les exigences juridiques.

Outre la confidentialité, l'intégrité et la disponibilité des données doivent également être prises en compte. Ce dernier aspect est déterminant pour garantir le fonctionnement d'un établissement de santé et, par conséquent, la sécurité de l'approvisionnement d'une infrastructure critique. Sur la base de cette analyse, des mesures doivent être définies et mises en œuvre sans délai afin d'éliminer les risques ou de les réduire à un niveau acceptable.

6.1 Remarque concernant le Privacy Shield 2.0 et le Swiss-U.S. Data Privacy Framework

Le 10 juillet 2023, la Commission européenne a adopté la décision d'adéquation relative au EU-U.S. Data Privacy Framework, également désigné parfois sous le nom de « Privacy Shield 2.0 ». Cette décision établit que les États-Unis assurent un niveau de protection adéquat pour les données à caractère personnel transférées depuis l'UE à des entreprises américaines certifiées conformément au EU-U.S. Data Privacy Framework et figurant sur la liste correspondante du U.S. Department of Commerce. En principe, des données à caractère personnel peuvent être transférées à ces entreprises sans garanties supplémentaires en matière de protection des données.

Pour les transferts de données depuis la Suisse, une réglementation suisse correspondante existe depuis le 15 septembre 2024 sous la forme du Swiss-U.S. Data Privacy Framework. Le Conseil fédéral a inscrit les États-Unis, pour les données personnelles transférées à des entreprises américaines certifiées dans le cadre de ce dispositif, sur la liste des États ou secteurs spécifiques assurant un niveau de protection des données adéquat. En vertu de l'article 16, alinéa 1, LPD, de tels transferts de données peuvent en principe être effectués sans garanties supplémentaires. En revanche, les transferts vers des entreprises américaines non certifiées continuent de nécessiter des garanties appropriées conformément à l'article 16, alinéa 2, LPD.

La stabilité juridique et institutionnelle de ces cadres de protection des données doit toutefois être réévaluée à la lumière de la décision rendue par la Cour suprême des États-Unis le 29 juin 2026 dans l'affaire Trump v. Slaughter. La Cour suprême a jugé incompatible avec le principe constitutionnel de la séparation des pouvoirs la réglementation légale selon laquelle les membres de la Federal Trade Commission ne pouvaient être révoqués que pour certains motifs importants, notamment en cas de manquement à leurs obligations, d'incapacité ou d'abus de fonction. Les Commissioners de la FTC peuvent ainsi, en principe, être révoqués par le Président sans qu'un tel motif de révocation doive être démontré.

Cette décision revêt une importance particulière pour le Swiss-U.S. Data Privacy Framework, car la FTC est chargée de faire respecter les principes de protection des données auprès de la plupart des entreprises américaines participantes. L'évaluation suisse de l'adéquation réalisée en 2024 partait expressément du principe que les Commissioners de la FTC ne pouvaient être révoqués pendant leur mandat de sept ans que pour un motif important et, sur cette base, qualifiait la FTC, conjointement avec le U.S. Department of Transportation, d'autorité de surveillance indépendante. La suppression de cette protection contre la révocation constitue dès lors une modification ultérieure substantielle d'un élément sur lequel reposait l'évaluation suisse de l'adéquation. Elle peut susciter des doutes quant à l'indépendance institutionnelle de la FTC ainsi qu'à l'absence d'influence politique sur la mise en œuvre du Swiss-U.S. Data Privacy Framework.

La décision de la Cour suprême n'abroge toutefois pas directement le Swiss-U.S. Data Privacy Framework. La reconnaissance suisse de l'adéquation demeure formellement applicable tant que le Conseil fédéral ne modifie pas la réglementation correspondante dans l'ordonnance sur la protection des données ou qu'une autorité compétente ou un tribunal ne parvient pas à une conclusion différente. Compte

tenu de l'évolution des conditions institutionnelles, il faut toutefois s'attendre à un nouvel examen du Framework. Les entreprises qui s'appuient exclusivement sur le Swiss-U.S. Data Privacy Framework pour leurs transferts de données devraient suivre l'évolution de la situation et, en particulier lorsqu'il s'agit de données personnelles sensibles ou de volumes importants de données personnelles, préparer des garanties complémentaires ou alternatives.

La question de savoir si l'introduction du EU-U.S. Data Privacy Framework et du Swiss-U.S. Data Privacy Framework a une incidence sur le cas particulier du U.S. CLOUD Act demeure controversée. Les deux cadres de protection des données ne suppriment pas les pouvoirs légaux dont disposent les autorités américaines pour exiger, dans les conditions prévues par le CLOUD Act, la remise de données par des fournisseurs américains.

Dans l'état actuel des choses, le présent document part donc du principe que le cas particulier du U.S. CLOUD Act doit continuer à être pris en compte séparément. La décision de la Cour suprême renforce au contraire la nécessité d'évaluer régulièrement, outre la certification formelle d'un destinataire américain, les risques effectifs liés à l'accès aux données, à la surveillance et aux voies de recours.

7 Considérations économiques relatives au cloud

Avec l'essor des offres cloud et le passage de modèles « on-premise » vers des licences en mode locatif, une nouvelle approche financière de l'utilisation des logiciels s'est imposée dans les organisations. Alors qu'auparavant le matériel et les logiciels étaient acquis en propre, les logiciels sont aujourd'hui de plus en plus achetés « as a Service » sur une base d'abonnement. Il ne s'agit donc plus d'investissements, mais de coûts d'exploitation directement imputés aux charges courantes (passage de CapEx à OpEx). Cela permet de réduire les risques financiers, puisqu'il n'est plus nécessaire de planifier et de réaliser des investissements avec immobilisation du capital et amortissement (généralement sur quatre ans).

Ce modèle (OpEx) offre ainsi une flexibilité nettement accrue. Les solutions peuvent être adaptées plus rapidement aux besoins réels, et la pression liée au financement de la maintenance diminue. Selon le modèle d'abonnement choisi, on peut également s'attendre à ce que les évolutions techniques soient mises en œuvre plus rapidement que dans un modèle d'acquisition (CapEx). De plus, l'accès à de nouvelles technologies est considérablement facilité et accéléré.

Le principal avantage économique du cloud computing réside dans la flexibilité qu'il procure. Il permet aux organisations d'adapter rapidement leur environnement IT aux exigences et aux besoins en constante évolution. Compte tenu de la numérisation croissante et accélérée de la société, cette capacité devient de plus en plus déterminante. Cela vaut en particulier pour le secteur de la santé, lui aussi engagé dans une transformation numérique rapide.

Il serait toutefois erroné d'affirmer qu'une solution basée sur le cloud est toujours moins coûteuse qu'une solution locale (« on-premise »). Les impacts financiers doivent être évalués au cas par cas, en fonction des applications concrètes et des efforts nécessaires pour garantir une utilisation conforme au droit et sécurisée. Il convient également de tenir compte du fait que les fournisseurs cloud peuvent ajuster leurs prix au fil du temps — généralement à la hausse — et qu'un changement de fournisseur peut entraîner des coûts importants.

8 Aspects géopolitiques

Compte tenu des évolutions géopolitiques récentes, il convient, en plus des éléments mentionnés ci-dessus, de prendre en considération la situation géopolitique ainsi que le comportement parfois imprévisible de certains acteurs.

En raison de ces évolutions et de la nouvelle réalité à laquelle nous sommes confronté·e·s, il ne peut être totalement exclu que, par exemple, des hausses arbitraires de droits de douane ou des restrictions réglementaires aient des répercussions sur les exploitant·e·s ou les utilisateur·trice·s de services cloud, que des connexions ou des services soient limités ou interrompus afin d'exercer une pression, ou encore qu'un centre de données d'un fournisseur soit physiquement détruit dans le cadre d'un conflit armé —

comme cela s'est produit début mars 2026 lors d'une attaque de missiles contre un centre de données de Amazon Web Services aux Émirats arabes unis.

Ces risques sont renforcés par la forte dépendance à un nombre limité de fournisseurs mondiaux. Il en résulte un profil de risque complexe, comprenant non seulement des dimensions techniques, mais aussi stratégiques et de politique de sécurité, susceptibles d'influencer directement la sécurité de l'approvisionnement dans le secteur de la santé. Ces éléments doivent être pris en compte dans les réflexions et les décisions, en pesant les risques, les opportunités et les alternatives, et en définissant des mesures appropriées.

Partie spécifique – Détails pour la mise en œuvre concrète

9 L'importance du cloud pour le backup et le recovery

Les analyses d'impact sur l'activité (Business Impact Analysis), associées à des exigences élevées en matière de Recovery Time Objective (RTO) et de Recovery Point Objective (RPO) dans les établissements de santé, mettent en évidence l'importance d'une haute disponibilité des systèmes ICT. Les incidents montrent qu'un établissement de santé peut, dans le pire des cas, fonctionner temporairement sans un soutien informatique essentiel — mais au prix d'une forte baisse de productivité et d'un effort considérable pour maintenir et reconstituer les flux d'information pertinents. Dans un cadre de gestion de la continuité des activités (Business Continuity Management) à plusieurs niveaux, les solutions cloud offrent des approches efficaces et évolutives pour garantir ou rétablir la continuité.

Un autre avantage des solutions cloud réside dans le fait que l'expertise, les services et le support sont généralement fournis par le prestataire, et que la mise à jour des systèmes et logiciels est assurée. En règle générale, les systèmes sont donc rapidement mis à jour et les failles de sécurité corrigées. Les niveaux de service doivent être définis contractuellement et, selon le type de service cloud, la responsabilité du client varie.

L'intégration des données issues de systèmes médicotechniques constitue un défi supplémentaire. De nombreux fournisseurs d'appareils, tels que les stimulateurs cardiaques ou les dispositifs de mesure de la glycémie, collectent ces données dans des solutions cloud propriétaires. Pour un traitement optimal, ces données devraient pouvoir être agrégées et mises à disposition dans les systèmes de l'équipe de soins interprofessionnelle.

Remarque : lors de l'utilisation de dispositifs médicaux, les directives de la Fédération des médecins suisses doivent être respectées.

10 Cloud only vs. utilisation hybride

La transition du modèle actuellement dominant « on-premise » vers le cloud est un processus de longue durée, dépendant de plusieurs facteurs :

- Disponibilité des offres et retrait progressif des applications ou services locaux
- Réduction des systèmes legacy non compatibles avec le cloud
- Exigences légales et réglementations en matière de protection des données
- Coexistence de services cloud privés et publics
- Nouveaux services disponibles exclusivement via le cloud (p. ex. télémédecine, monitoring à distance des patient·e·s, utilisation de wearables)

Défis de gestion : besoins du business et technologies

La compétence clé (Unique Selling Proposition, USP) d'un service ICT au sein d'un établissement de santé réside dans sa capacité à faire le lien entre la technologie et les processus principaux de diagnostic et de traitement des patient·e·s. Sans une compréhension approfondie de ces deux domaines, il n'est pas possible de fournir un conseil et un accompagnement proactifs créateurs de valeur. Les technologies de base et les infrastructures tendent à devenir des commodités ; le défi pour les services ICT internes

consiste dès lors à orchestrer les différents éléments et prestataires, ainsi qu'à gérer de manière optimale la complexité.

Défis ICT : pénurie de personnel qualifié et transformation numérique

La transformation numérique dans le secteur de la santé accuse un retard d'environ dix ans par rapport à d'autres secteurs (banques, assurances, télécommunications). Ce retard s'observe également, dans une mesure comparable, par rapport à certains pays étrangers (Estonie, Singapour, États-Unis).

Par conséquent, de nombreuses applications locales, souvent basées sur des architectures client/serveur, sont encore en usage, sans séparation claire des différentes couches (données, logique métier, présentation). Les fournisseurs sont souvent de petites et moyennes entreprises (PME), dont la capacité d'exécution à long terme — notamment en matière de support opérationnel et d'évolution — est parfois limitée.

La pénurie de spécialistes ICT se manifeste particulièrement dans deux domaines : d'une part, les formations ICT sont peu attractives pour les personnes entrant dans le secteur de la santé ; d'autre part, les établissements de santé ne sont pas compétitifs en termes de rémunération pour attirer des profils spécialisés (p. ex. ingénieur·e·s M365, architectes en sécurité des systèmes d'information, etc.). En outre, indépendamment de leur utilisation du cloud, les établissements de santé doivent gérer un grand nombre de dispositifs médicotechniques connectés au réseau, ce qui constitue un domaine spécifique nécessitant du personnel IT hautement spécialisé.

11 Cas d'usage

11.1 Videotéléphonie

La vidéotéléphonie transmet des données audio et vidéo en temps réel. En règle générale, il s'agit uniquement d'une transmission sans stockage des données. Une exception existe lorsque les échanges sont enregistrés à des fins de traçabilité ou d'assurance qualité.

Principales questions à examiner :

- La vidéotéléphonie peut-elle être techniquement limitée à la seule transmission de données audio et vidéo ?
- Est-il connu quelles données secondaires (métadonnées) sont stockées par le fournisseur à des fins de signalisation, et si ce stockage ainsi que leur traitement ultérieur sont conformes aux exigences légales ? Le fournisseur applique-t-il le principe de minimisation des données, selon lequel seules les données strictement nécessaires sont collectées et traitées ?
- La vidéotéléphonie ou les données audio et vidéo transmises dans ce contexte ont-elles un lien avec des données personnelles ? Il ne s'agit pas uniquement des données utilisateur·trice·s transmises, mais aussi des images des participant·e·s, qui peuvent présenter un besoin de protection de la vie privée.
- Il est recommandé d'utiliser un arrière-plan virtuel, comme le permettent généralement les applications courantes. Cette fonctionnalité est toutefois souvent disponible uniquement via une application installée et non via un navigateur. Dans ce cas, il est conseillé d'informer les participant·e·s qu'il est autorisé de désactiver la caméra pour protéger la vie privée. Cette information devrait idéalement être communiquée dès l'invitation ou au plus tard au début de la séance.
- Les données utilisateur·trice·s peuvent-elles au minimum être chiffrées ? Ce chiffrement est-il end-to-end ou seulement pendant la transmission (data-in-transit) ou le stockage (data-at-rest) ?

En cas d'enregistrement, les données audio et vidéo sont stockées. Les questions supplémentaires suivantes se posent :

- Quel est l'objectif de l'enregistrement ? Combien de temps les données sont-elles conservées ? Cette durée peut-elle être réduite ? Est-il garanti que les données ne seront pas utilisées à d'autres fins et qu'elles seront supprimées dans un délai approprié après réalisation de l'objectif ?

- Existe-t-il une base légale, un intérêt légitime ou le consentement des participant·e·s pour ce traitement ? Cela vaut-il également pour les données utilisateur·trice·s transmises pendant la communication ?

Risques de la communication basée sur le cloud

Une utilisation large, voire généralisée, de services de communication basés sur le cloud crée une forte dépendance en termes de disponibilité. Une panne du fournisseur ou une perturbation de l'accès (connectivité) peut avoir un impact majeur sur le fonctionnement de l'établissement de santé, en particulier pour les communications critiques internes et externes. Il est donc recommandé de prévoir des solutions de secours (redondances) et de les tester régulièrement à l'aide de scénarios réalistes.

L'intégration croissante d'algorithmes de détection de contenus inappropriés (notamment via l'intelligence artificielle) comporte le risque que des images médicales transmises soient classées à tort comme contenus inappropriés et bloquées. Cela peut avoir un impact important sur certains cas d'usage, notamment la télémédecine. Ces fonctionnalités sont souvent introduites par les fournisseurs sans préavis ou avec un préavis très court, ce qui complique l'adaptation des établissements de santé. Il est donc essentiel de clarifier en amont les possibilités de configuration et de désactivation de ces mécanismes avec le fournisseur.

En résumé, l'utilisation de la vidéotéléphonie dans les établissements de santé présente des avantages significatifs et peut générer une forte valeur ajoutée dans de nombreux cas d'usage. Toutefois, il est essentiel de ne pas se laisser guider uniquement par ces avantages et d'évaluer de manière rigoureuse une utilisation large ou généralisée. Les modèles d'exploitation hybrides et échelonnés ont fait leurs preuves, notamment lorsque les communications critiques sont assurées via des solutions locales traditionnelles.

11.2 Collaboration

La collaboration comprend, au sens général, l'interaction via la vidéotéléphonie ainsi que, en complément, la modification simultanée de données stockées de manière centralisée par des participant·e·s internes et externes. Le cas d'usage décrit au point 11.1 est ainsi étendu par le stockage et le traitement de données, généralement dans l'environnement cloud d'un fournisseur de services.

Principales questions à examiner :

- Peut-on garantir que les données stockées de manière centralisée sont suffisamment protégées contre les accès non autorisés (objectif de protection : confidentialité) et les modifications non autorisées (objectif de protection : intégrité) ?
- Les données peuvent-elles être restaurées en cas de perte dans l'environnement cloud du fournisseur (objectif de protection : disponibilité) ?
- Les accès et les modifications des données peuvent-ils être tracés ?
- L'attribution des droits d'accès relève-t-elle exclusivement du propriétaire de l'espace de travail commun ou de personnes explicitement autorisées par celui-ci (administration déléguée) ? Ou chaque participant·e peut-il/elle partager des données avec des tiers ?

11.3 Messagerie instantanée

La messagerie instantanée (chat) désigne généralement l'envoi de messages courts à une personne ou à un groupe. Le contenu peut inclure, outre du texte, des images ou des documents en pièce jointe. Les messages sont stockés afin de pouvoir être consultés ultérieurement. La communication s'effectue généralement au sein d'un espace d'adressage protégé, de sorte que seuls les membres de cet espace peuvent recevoir les messages.

Principales questions à examiner :

- L'expéditeur·rice d'un message peut-il/elle toujours identifier qui a accès au contenu ?
- Peut-on garantir que les données transmises ne sont pas utilisées à d'autres fins par le fournisseur (cf. WhatsApp) ?

- Sait-on quelles métadonnées sont collectées et stockées dans le cadre de la transmission, à quelles fins et par qui elles sont traitées ? Le fournisseur applique-t-il le principe de minimisation des données ?

11.4 E-mail

Le courrier électronique désigne la transmission de textes et de données via une application dédiée, souvent un client de messagerie. Cette application n'est pas seulement utilisée pour transmettre des informations, mais aussi pour les stocker, par exemple dans une structure de dossiers au sein du client.

Principales questions à examiner :

- Le chiffrement des données est-il assuré de manière continue lors de la transmission ?
- Une signature peut-elle être utilisée afin de vérifier l'authenticité de l'expéditeu·rice au moyen de procédés cryptographiques ?
- Existe-t-il une possibilité distincte de transmission chiffrée des e-mails, allant au-delà du simple chiffrement du transport ?

11.5 Systèmes cliniques et administratifs

Dans le contexte des systèmes cliniques et administratifs, on entend les systèmes utilisés pour le traitement des données des patient·e·s — donc des données personnelles particulièrement sensibles — ainsi que des données des collaborateur·trice·s, qui peuvent également inclure des données sensibles. Cela englobe en principe l'ensemble des systèmes d'information et des applications métiers, ainsi que les systèmes périphériques et services auxiliaires associés.

Principales questions à examiner :

- Est-il possible de déterminer de manière transparente dans quel pays (juridiction) et, idéalement, dans quel centre de données du fournisseur les données sont stockées ?
- Peut-on exclure que des services annexes (p. ex. à des fins d'analyse) entraînent un transfert des données vers un pays ne disposant pas d'un niveau de protection adéquat ?
- Peut-on vérifier que les données sont chiffrées au minimum pendant la transmission (data-in-transit) et le stockage (data-at-rest), et idéalement aussi pendant le traitement (data-in-processing) ?
- Est-il garanti que la gestion des clés est assurée par le client ou un tiers mandaté, et non par le fournisseur ?
- Peut-on idéalement garantir que les données sont déjà chiffrées avant leur transmission vers l'environnement cloud du fournisseur, via un service tiers ?
- Le client connaît-il les points d'accès potentiels du fournisseur aux données en clair (p. ex. via des memory dumps à des fins de support) ?
- Le client sait-il depuis quel pays le fournisseur fournit ses services de support ? Peut-il s'assurer qu'aucune donnée sensible n'est transférée vers un pays sans niveau de protection adéquat dans ce cadre ?
- Le fournisseur est-il disposé et capable de divulguer ses relations de sous-traitance ? Existe-t-il une obligation d'information et un droit de veto du client en cas de nouveaux sous-traitants ?
- Le client peut-il garantir une sortie complète de l'environnement cloud dans un délai raisonnable (en général trois à six mois), sans interruption majeure de service ? Cela reste-t-il garanti en cas de changement de propriété du fournisseur ?
- Le client peut-il restaurer intégralement les données en cas de perte, tout en respectant les exigences de sécurité ?
- Le client peut-il maintenir un niveau de service suffisant en cas de perturbation du cloud du fournisseur (continuité de service) ?
- Le fournisseur accorde-t-il un droit d'audit suffisant (tests d'intrusion, audits) ? Met-il à disposition des rapports d'audit externes ?

- Le client peut-il compter sur une connectivité suffisante vers l'environnement cloud ?
- Le client a-t-il réalisé une analyse des risques conforme aux exigences réglementaires et assure-t-il leur gestion sur toute la durée du service ?

12 Mesures techniques et organisationnelles

12.1 Détermination des risques par cas d'usage

Dans la section précédente, les différents cas d'usage ont été décrits et les principales questions d'analyse présentées. Les réponses à ces questions permettent d'identifier les risques existants. L'utilisation d'un catalogue de risques constitue également un outil utile dans ce processus.

Sur la base des réponses, le catalogue de risques peut être analysé afin de déterminer si un risque s'applique ou non. Un tel catalogue peut par exemple inclure les risques suivants (basés sur l'ENISA Cloud Computing Risk Assessment) :

Risques organisationnels

R.1 Verrouillage fournisseur (lock-in)

R.2 Perte de contrôle des processus

R.3 Défis en matière de conformité

R.4 Atteinte à la réputation

R.5 Défaillance ou perturbation du service cloud

R.6 Acquisition du fournisseur cloud

R.7 Défaillance de la chaîne d'approvisionnement

Risques techniques

R.8 Sur- ou sous-allocation des ressources

R.9 Isolation insuffisante par rapport aux autres client·e·s du cloud

R.10 Risques internes chez le fournisseur

R.11 Compromission des interfaces applicatives avec le cloud

R.12 Interception ou écoute des données lors de la transmission

R.13 Vol de données lors de l'upload ou du download

R.14 Suppression insuffisante des données

R.15 Attaques par déni de service distribué (DDoS)

R.16 Economic Denial of Service (EDoS)

R.17 Perte des clés de chiffrement

R.18 Scans Internet malveillants

R.19 Compromission de l'infrastructure cloud

R.20 Conflits entre sauvegardes locales et cloud

Risques juridiques

R.21 Accès aux données imposé par la loi

R.22 Évolution du cadre juridique

R.23 Risques liés à la protection des données

R.24 Risques de licence / violations de licence

Une fois les risques identifiés, il convient d'en évaluer les impacts. Cela implique d'estimer la probabilité de survenance ainsi que l'ampleur des dommages. Alternativement, une estimation des impacts minimaux et maximaux peut être réalisée.

Evaluation des dommages potentiels

L'évaluation des impacts peut être structurée selon les dimensions suivantes : confidentialité, disponibilité, intégrité et traçabilité. Il s'agit d'analyser les conséquences pour l'établissement de santé, par exemple en cas d'indisponibilité d'un service critique.

Concrètement, il s'agit d'évaluer les dommages potentiels si la vidéotéléphonie, les plateformes de collaboration, la messagerie, l'e-mail ou des systèmes cliniques et administratifs ne sont plus disponibles, si des données sont volées, manipulées, supprimées ou détruites, ou si l'intégrité ou la traçabilité des informations n'est plus assurée.

Il est essentiel de prendre en compte le type et le volume des données traitées, ainsi que la criticité des processus concernés. Il faut également considérer la perte de contrôle sur les données, la dépendance vis-à-vis du fournisseur (vendor lock-in) et le risque d'attaques cyber via les systèmes exposés dans le cloud.

Mesures pour minimer les risques

Une fois les risques et leurs impacts identifiés, il convient d'évaluer les mesures existantes et le niveau de risque résiduel. Si ce dernier est jugé trop élevé, des mesures supplémentaires doivent être mises en œuvre jusqu'à atteindre un niveau acceptable.

Les objectifs de protection — confidentialité, disponibilité, intégrité et traçabilité — doivent être garantis de manière adéquate. Pour cela, il est nécessaire de définir les mesures mises en place et les risques résiduels associés.

Des solutions doivent exister et des responsabilités doivent être définies pour les domaines suivants :

- Authentification
- Autorisation
- Logging et audit
- Sauvegarde des données
- Mises à jour logicielles / patching
- Protection périmétrique (phishing, sécurité des e-mails, pièces jointes)
- Protection des informations (selon la classification des données)
- Prévention des fuites de données (DLP)
- Security Information & Event Management (SIEM), threat intelligence
- Sécurité des terminaux connectés au cloud (endpoint protection)

Enfin, il convient de déterminer si ces exigences peuvent être couvertes par les solutions proposées par le fournisseur cloud ou s'il est préférable d'adopter une stratégie multi-fournisseurs. La décision dépend notamment des solutions déjà en place, du niveau de satisfaction à leur égard, ainsi que des avantages potentiels en termes d'efficacité et de coûts. L'intégration des solutions existantes doit également être prise en compte.

12.2 Chiffrement et gestion des clés

Afin de protéger adéquatement les données, le chiffrement constitue une mesure essentielle. Il convient de distinguer trois types de chiffrement : 1) le chiffrement lors de la transmission (in transit), 2) le chiffrement lors du stockage (at rest) et 3) le chiffrement lors du traitement (in process). Le chiffrement des données lors de leur transmission vers le cloud est impératif et non contesté — il doit toujours être garanti.

Gestion du chiffrement lors du stockage

En ce qui concerne le chiffrement des données stockées dans le cloud (at rest), les fournisseurs proposent différentes solutions de gestion des clés qu'il convient d'évaluer. Cette gestion est une condition préalable à l'utilisation du cloud : sans gestion adéquate des clés, les services cloud ne peuvent pas être utilisés. Il est donc crucial de clarifier les modalités d'accès aux clés.

Une distinction essentielle réside dans le fait que la gestion des clés est soit assurée par le fournisseur dans le cloud (chaque client disposant de sa propre clé), soit gérée localement par l'établissement de santé. Dans ce dernier cas, la responsabilité incombe entièrement à l'établissement. Si la gestion des clés est assurée par le fournisseur, celui-ci garantit la fonctionnalité, mais il existe un risque que des collaborateur·trice·s disposant de droits d'accès puissent accéder aux clés et donc aux données. Ce risque n'existe pas en cas de gestion locale.

Des solutions renforcées permettent d'exiger une autorisation supplémentaire pour tout accès aux clés par des employé·e·s du fournisseur. Cette autorisation peut être accordée soit par des personnes désignées du fournisseur, soit par des représentant·e·s de l'établissement de santé.

Il convient toutefois de veiller à ce que les personnes autorisant ces accès soient disponibles conformément aux niveaux de service requis. Si une assistance en dehors des heures de bureau est nécessaire, les personnes chargées de l'autorisation doivent également être disponibles, faute de quoi les interventions ne pourront pas être réalisées à temps.

Gestion du chiffrement lors du traitement

Le chiffrement des données en cours de traitement (in process) constitue un défi particulier, spécialement lorsque l'exécution des solutions SaaS se fait directement dans le cloud et non localement ou dans le navigateur. Les solutions disponibles varient selon les fournisseurs, mais elles impliquent généralement une complexité accrue, une sensibilité aux erreurs et des limitations fonctionnelles.

Ce type de chiffrement suppose que les personnes traitant les données utilisent une clé qui n'est pas détenue par le fournisseur. La gestion cryptographique doit donc être assurée par l'établissement de santé. Par exemple, dans le cadre d'un traitement collaboratif avec des partenaires externes, ceux-ci doivent d'abord accéder à l'infrastructure de l'établissement afin d'obtenir un certificat (clé), leur permettant ensuite de déchiffrer et de traiter les données dans le cloud.

Cette configuration est complexe et comporte des risques pour la disponibilité. De plus, la solution de chiffrement doit être compatible avec les applications cloud utilisées ; dans le cas contraire, celles-ci ne peuvent pas être exploitées. Il est donc nécessaire de vérifier, au cas par cas, si une solution de chiffrement des données en cours de traitement est disponible et quelles sont ses limitations. À ce jour, aucune solution ne permet un chiffrement fiable « in process » tout en conservant l'ensemble des fonctionnalités. En l'absence de ce chiffrement, la fonctionnalité est totale, mais les données peuvent être accessibles aux collaborateur·trice·s du fournisseur disposant de droits appropriés pendant leur traitement.

Note linguistique : Ce document existe en plusieurs versions linguistiques. En cas de divergence ou d'interprétation la version allemande fait foi.

À propos des auteurs

Erik Dinkel

Erik Dinkel est depuis 2018 RSSI et, depuis 2024, également Chief Security Officer de l'Universitätsspital Zürich (USZ). Avant son arrivée à l'USZ, il a travaillé dans le Business Risk Management ainsi qu'en tant que Head Access Governance chez Credit Suisse Suisse. Il est titulaire d'un master de l'Université de Zurich (M.A. UZH) en science politique et possède des formations complémentaires en management, gestion des risques et sécurité de l'information (CAS UZH, CAS FHNW, BSI). Depuis 2021, il est chargé de cours en cybersécurité et sécurité de l'information à la Hochschule Luzern et, depuis fin août 2025, président du Healthcare Cyber Security Center.

Stefan Hunziker

Médecin promu et spécialiste en informatique de gestion, Stefan Hunziker a dirigé dès 2002 l'informatique médicale et, de 2012 à 2025, l'informatique du LUKS Gruppe. Parallèlement, il a représenté en tant que CIO le domaine informatique au sein de la direction du groupe de 2021 à 2025. Durant cette période, il a notamment été responsable de l'intégration informatique de l'hôpital de Nidwald au sein du LUKS Gruppe. Depuis 2026, il soutient l'Universitätsspital Zürich en tant que chef de projet dans la transformation numérique.

Stefan Juon

Stefan Juon a travaillé de 2009 à 2022 au Kantonsspital Graubünden dans différentes fonctions, notamment comme RSSI et co-responsable ICT de 2016 à 2022. Il possède des formations en ingénierie et en gestion d'entreprise au niveau tertiaire ainsi que des qualifications complémentaires en sécurité de l'information, gestion des risques et architecture IT. Il est en outre certifié ITIL, TOGAF et CISA.

Philipp Stoll

Philipp Stoll est ingénieur en mécanique de formation. Pendant les 20 dernières années précédant sa retraite, il a été membre de la direction de l'Universitäts-Kinderspital beider Basel (UKBB). Depuis lors, il exerce en tant que consultant pour des entreprises du secteur de la santé. Ses domaines de compétence comprennent la construction, la logistique, les achats, la maintenance, la technologie médicale ainsi que la sécurité, avec une spécialisation particulière à l'interface entre les utilisateurs et les planificateurs. Depuis 2011, il est également délégué de H+ auprès de l'Office fédéral de la protection de la population (OFPP) et de l'Office fédéral pour l'approvisionnement économique du pays (OFAE).

Werner Ulmer

Werner Ulmer est depuis 2024 RSSI de la Direction de l'économie publique du canton de Zurich. Auparavant, il était RSSI du Kantonsspital St. Gallen (aujourd'hui HOCH Health Ostschweiz) et des réseaux hospitaliers associés, où il a été responsable de la mise en place stratégique et opérationnelle de la sécurité de l'information jusqu'à l'obtention de la certification ISO 27001. Grâce à des formations approfondies — notamment à la Hochschule Luzern — et à une longue expérience, il dispose d'une expertise reconnue en cybersécurité, sécurité de l'information, gestion des risques et gouvernance de la sécurité.