Guide pour la conservation et l'archivage

Version du 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Table des matières

1 Bases légales pour l'effacement

1.1 Généralités

Le présent document explique quand des données personnelles peuvent ou doivent être effacées ou détruites, et ce à quoi il faut alors prêter attention.

Les données personnelles ne peuvent être traitées que pour une finalité précise et dans la mesure où elles sont appropriées et nécessaires à cette fin. Dès que les données personnelles ne sont plus nécessaires au regard de la finalité du traitement, elles doivent être effacées, détruites ou anonymisées.

Les personnes concernées ont en outre le droit d'exiger l'effacement des données personnelles traitées les concernant dès lors qu'il n'existe plus de motif justifiant leur traitement. Les motifs justificatifs sont les délais de prescription et de conservation, qui sont réglés différemment selon les cas.

Remarque : En ce qui concerne les délais de conservation légaux, l'aperçu sur les délais de conservation légaux mis à disposition par la FMH peut servir d'aide [Bases juridiques pour le quotidien du médecin].

1.2 Droit à l'effacement de la personne concernée

En présence d'une demande d'effacement, il convient de tenir compte des éléments suivants :

— La personne requérante doit être identifiée.
— L'existence d'obligations légales de conservation ou d'autres motifs impératifs s'opposant à l'effacement ou à la destruction des données doit être vérifiée. En l'absence de tels motifs, les données personnelles doivent être effacées ou détruites.
— Il y a lieu d'indiquer à la personne requérante si les données ont été effacées suite à sa demande. Si ses données n'ont pas été effacées, il convient de l'en informer et d'en indiquer les motifs.

2 Exigences légales relatives à la conservation et à l'archivage

2.1 Délais de conservation légaux (état au 31.10.2022)

Les établissements de santé produisent quotidiennement des documents qui contiennent notamment des informations (données personnelles) sur la patientèle ainsi que sur le personnel de l'établissement de santé lui-même ou de prestataires. La conservation de ces documents obéit au principe de la proportionnalité. Les données personnelles peuvent donc être conservées aussi longtemps qu'elles sont appropriées et nécessaires à l'exécution des tâches. Les lois fédérales et les législations cantonales fixent en outre des délais de conservation précis. En parallèle, la conservation peut également viser à garantir la traçabilité d'un traitement, d'une évaluation des prestations ou d'un état de fait à titre de preuve.

Les données professionnelles ne contenant aucune donnée personnelle peuvent en principe être conservées de manière illimitée. Elles doivent néanmoins être conservées au moins aussi longtemps que les délais de conservation légaux le prévoient.

Les tableaux suivants présentent, à titre d'information, un aperçu des exigences légales relatives au mode et à la durée de conservation. En l'absence de dispositions légales en matière de conservation, la loi sur la protection des données exige que soient fixés au moins les critères de conservation (art. 12 LPD).

La protection et en particulier la sécurité des données devant être garanties pendant tout le délai de conservation, une liste de contrôle présentant les mesures techniques et organisationnelles pouvant être prises pour maintenir la sécurité des données figure à la dernière section du présent document.

Digression : transfert / abandon de l'activité professionnelle – obligation de conserver les dossiers médicaux

En principe, l'obligation de conserver le dossier médical subsiste en cas de cessation ou de transfert de l'activité professionnelle. La distinction opérée ici porte sur la personne avec laquelle la patiente ou le patient a conclu le contrat de soins. En effet, lorsque le contrat de soins a été conclu avec un cabinet de groupe (SA ou Sàrl), l'obligation de conservation incombe au cabinet lui-même. En revanche, lorsque le contrat de soins a été conclu avec la ou le médecin, celle-ci ou celui-ci doit veiller à ce que les dossiers médicaux soient conservés de manière appropriée.

Si une personne (physique ou morale) reprend le cabinet médical ou la suite du traitement de la patientèle, cela ne signifie pas automatiquement que les dossiers médicaux peuvent lui être transmis ou qu'elle peut les consulter. L'octroi du droit de consulter à la personne repreneuse requiert le consentement préalable de la patiente ou du patient. En l'absence (provisoire) du consentement de la patiente ou du patient, il est possible d'appliquer le principe dit « des deux armoires ». Ainsi, une armoire contient les dossiers médicaux pour lesquels la patientèle a consenti au traitement par la personne repreneuse et une autre contient ceux pour lesquels le consentement de la patientèle fait (encore) défaut. Les dossiers médicaux numériques sont en principe soumis aux mêmes règles.

En cas de cessation d'activité, les médecins restent tenus, dans le délai légal, de fournir à leurs patientes et patients des renseignements sur leur dossier médical. Par conséquent, la ou le médecin doit veiller à ce que les dossiers médicaux soient conservés de manière appropriée et protégés contre tout accès non autorisé, par exemple en les stockant chez soi ou en en déléguant la conservation à un tiers.

Remarque : *Il convient en outre de consulter les éventuelles dispositions cantonales en vigueur (lois cantonales sur la santé ou sur les patients), qui pourraient prévoir des délais de conservation plus longs ou des formes particulières de conservation.*

2.2 Aperçu des délais de conservation légaux

Données sur la santé / documents de la patientèle		
Nature des documents	**Délai et mode de conservation**	**Bases légales**
Dossier médical	En raison du délai de prescription en matière de responsabilité civile, les dossiers médicaux doivent être conservés **20 ans** après la fin du traitement concerné. Par ailleurs, ils ne peuvent être conservés qu'avec le consentement des personnes concernées.	Art. 60, al. 1bis et 2 du code des obligations (CO) / Art. 128a CO Art. 12 du code de déontologie de la FMH
	Remarque : *En ce qui concerne les obligations de conservation quant à sa durée et à sa nature, il convient de consulter les lois cantonales sur la santé applicables au lieu du cabinet médical. Les dispositions cantonales prévoient une obligation de conservation des dossiers médicaux de* **dix ans** *au moins. Certains cantons fixent toutefois une obligation de conservation de* ***20 ans*** *pour des cas spécifiques. En outre, quelques actes législatifs cantonaux prévoient une destruction des documents après 20 ans, à moins qu'un intérêt prépondérant ne s'y oppose.*	Lois cantonales sur la santé (en fonction du lieu du cabinet médical)
Documents relatifs à l'application de rayonnements et à l'exploitation	Les données doivent être conservées conformément aux dispositions applicables au dossier médical.	Art. 20, al. 5, let. a de l'ordonnance sur les rayons X (OrX)
	Toutefois, les données concernant les paramètres d'exposition aux installations de radiothérapie ainsi que les données collectées dans le cadre de systèmes de radiologie à des fins de contrôle de position, de planification et de simulation en radiothérapie sont soumises à un délai de conservation de **20 ans**.	
	Les données recueillies lors d'applications à doses moyennes et élevées et lors de mammographies doivent être conservées pendant **dix ans**.	Art. 20, al. 5, let. b, OrX
Documents relatifs aux opérations en rapport avec le sang ou les produits sanguins	Lorsque la loi sur les produits thérapeutiques impose une obligation d'enregistrer les opérations en rapport avec le sang ou les produits sanguins (p. ex. lors de prélèvements sanguins), les documents doivent être archivés pendant **30 ans**.	Art. 39 et 40 de la loi fédérale sur les médicaments et les dispositifs médicaux (loi sur les produits thérapeutiques, LPTh)
	Remarque : *Des dispositions particulières sont prévues lorsque la cessation de l'activité professionnelle intervient avant l'expiration du délai d'archivage.*	

Documents relatifs à l'utilisation d'organes, de tissus ou de cellules	Lorsque la loi sur la transplantation impose une obligation d'enregistrer l'utilisation d'organes, de tissus ou de cellules, les documents doivent être conservés pendant **20 ans**.	Art. 34 et 35 de la loi fédérale sur la transplantation d'organes, de tissus et de cellules (loi sur la transplantation)
Documents relatifs à la médecine du travail	**40 ans** pour les documents relatifs à la médecine du travail.	Art. 8 de l'annexe 4 au code de déontologie de la FMH
Résultats d'analyses génétiques présymptomatiques	La ou le médecin mandaté ne peut conserver les résultats d'analyses génétiques présymptomatiques que s'ils sont pertinents pour la conclusion du contrat. Les résultats d'analyses ne peuvent être utilisés qu'aux fins pour lesquelles ils ont été recueillis auprès de la personne requérante.	Art. 28 de la loi fédérale sur l'analyse génétique humaine (LAGH)
Documents relatifs à l'information des personnes vivantes donneuses d'organes, de tissus ou de cellules	Les médecins chargés du prélèvement d'organes, de tissus ou de cellules doivent fournir à la personne donneuse potentielle des informations exhaustives et compréhensibles, par oral et par écrit, avant de procéder au prélèvement. Les documents relatifs à l'information de la personne donneuse vivante doivent être conservés pendant **dix ans, séparément** du dossier médical.	Art. 9, al. 4 et 10, al. 2 de l'ordonnance sur la transplantation d'organes, de tissus et de cellules d'origine humaine (ordonnance sur la transplantation)
Obligation de documentation pour les substances soumises à contrôle selon l'ordonnance sur le contrôle des stupéfiants	Les documents, données et supports de données concernant la prescription et le commerce des substances soumises à contrôle au sens de l'ordonnance sur le contrôle des stupéfiants doivent être conservés pendant **dix ans**.	Art. 62 de l'ordonnance sur le contrôle des stupéfiants (ordonnance sur le contrôle des stupéfiants, OCStup)

Documents relatifs au personnel		
Nature des documents	**Délai et mode de conservation**	**Bases légales**
Dossier personnel (contrats de travail, dossiers des collaboratrices et collaborateurs y c. évaluations, certificats de travail, attestations, notes, résiliation, etc.)	**5 ans** à compter du départ de la collaboratrice ou du collaborateur, sur papier (analogique) ou électronique (numérique), de manière à pouvoir prouver des faits et à permettre leur lecture à tout moment.	Art. 330a CO en relation avec art. 128 CO / art. 46 de la loi sur le travail (LTr) et 73 de l'ordonnance 1 relative à la loi sur le travail (OLT 1)
Salaires (certificats de salaire, décomptes, assurances sociales et caisse de pensions)	**5 ans** à compter du départ de la collaboratrice ou du collaborateur, sur papier (analogique) ou électronique (numérique), de manière à pouvoir prouver des faits et à permettre leur lecture à tout moment.	Art. 128, al. 3, CO
Saisie du temps de travail (temps de travail saisi dans un système de saisie du temps de travail)	**5 ans** à compter du départ de la collaboratrice ou du collaborateur, sur papier (analogique) ou électronique (numérique), de manière à pouvoir prouver des faits et à permettre leur lecture à tout moment.	Art. 46 de la loi sur le travail (LTr) et 73 de l'ordonnance 1 relative à la loi sur le travail (OLT 1)

Documents professionnels		
Nature des documents	**Délai et mode de conservation**	**Bases légales**
Factures (débiteurs, créanciers, comptes annuels y c. rapports de révision)	**10 ans** à compter de la fin de l'exercice, sur papier (analogique), électronique (numérique) ou sous toute forme équivalente, de manière à ce que l'état de fait soit garanti et puisse être relu en tout temps.	Art. 958 et 958f CO
Documents fiscaux (tous les documents relatifs à la fiscalité)		
Frais (justificatifs des frais ainsi que tous les documents en rapport avec les frais)		

Autres documents		
Nature des documents	**Délai et mode de conservation**	**Bases légales**
Procès-verbaux de journalisation du traitement automatisé de données sensibles / profilage	Si le cabinet médical traite des données sensibles de manière automatisée ou numérisée et que les mesures mises en œuvre n'offrent pas une protection suffisante des données, il doit consigner le traitement dans un procès-verbal de journalisation. Ces procès-verbaux doivent être conservés pendant **un an** conformément aux exigences en matière de révision.	Art. 4 de l'ordonnance sur la protection des données (OPDo)
Analyse d'impact relative à la protection des données (AIPD) (tous les documents pertinents dans le cadre d'une analyse d'impact relative à la protection des données)	Au moins **2 ans** à compter de la fin du traitement des données. ***Remarque :*** *L'obligation d'établir une AIPD s'applique à tout traitement de données personnelles susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée en cas de violation de la confidentialité ou de l'intégrité, ou en cas d'abus.* *Les responsables du traitement privés sont déliés de leur obligation d'établir une AIPD s'ils sont tenus d'effectuer le traitement en vertu d'une obligation légale. Ainsi, les établissements de santé de droit privé ne sont en principe pas tenus de procéder à des AIPD en raison de leur obligation légale de tenir un dossier médical. Cela ne vaut que pour la tenue du dossier médical conformément à la loi. Si les établissements de santé recourent à des produits cloud, par exemple, une AIPD pourrait s'avérer nécessaire, l'utilisation d'un cloud n'étant pas prescrite par la loi.*	Art. 14 LPD
Documents relatifs à la violation de la sécurité des données (tous les documents pertinents en lien avec l'annonce d'une violation de la sécurité des données)	Au moins **2 ans** à compter de l'annonce d'une violation de la sécurité des données.	Art. 15 LPD

2.3 Liste de contrôle pour la conservation et l'archivage des données personnelles

Lorsque les données doivent être conservées pour une ou plusieurs des raisons susmentionnées ou pour d'autres raisons, il convient également de veiller à la sécurité des données pendant leur conservation. Les listes de contrôle suivantes peuvent servir d'aide pour garantir la sécurité des données lors de la conservation.

Remarque : *La liste de contrôle Effacement constitue une aide quant à la question de savoir si et comment les données personnelles peuvent être effacées.*

D'autres recommandations relatives aux exigences de sécurité dans les cabinets figurent dans le document Exigences minimales pour la sécurité informatique des cabinets médicaux.

Lieu		
Mesure	**Explications/remarques**	**Fait**
Gestion des accès	Les supports de données contenant des données personnelles doivent être conservés en un endroit auquel seul un cercle déterminé de personnes a accès. Par exemple dans des armoires verrouillables, des archives, des locaux avec système de clés ou de badges, etc., pour lesquels seules les personnes autorisées possèdent la clé ou un badge.	☐
Protection contre les événements environnementaux	Les supports de données doivent être conservés de sorte à ne pouvoir être détériorés par l'eau, le feu ou tout autre événement environnemental.	☐

Format		
Mesure	**Explications/remarques**	**Fait**
Protection contre la corrosion / l'altération du papier	Les supports de données doivent être conservés de manière à ne pouvoir être détériorés par la corrosion (supports de données numériques) ou par l'altération du papier (supports de données physiques).	☐
Formats actuels	Les données numériques doivent être conservées dans un format lisible à long terme. À défaut, il faut veiller en temps utiles à l'enregistrement des données dans un format à jour. Les formats suivants peuvent être archivés :	☐

Champ d'application	**Formats compatibles avec l'archivage**
Documents d'Office (Word, Excel, Power-Point, Outlook)	PDF/A
Texte (non formaté)	TXT
Tableaux	CSV
Bases de données	SIARD
Images numériques	TIFF ou PDF/A
Audio	WAVE
Vidéo	MPEG-4

Remarque : *L'enregistrement de données dans un autre format peut les modifier ou causer d'autres dommages.*

Accès		
Mesure	**Explications/remarques**	**Fait**
Droits d'accès	L'accès aux données n'est accordé qu'aux personnes qui en ont réellement besoin (p. ex. à des fins de preuve dans le cadre d'une prétention en responsabilité, pour garantir la lisibilité, etc.). Les droits d'accès aux données doivent être limités au minimum nécessaire (p. ex. à une ou deux personnes). Il faut veiller à ce que les droits puissent être adaptés aux circonstances (p. ex. mutation, suppléance, etc.).	☐
Protection des moyens d'authentification	Il faut veiller à ce que le moyen d'authentification (p. ex. nom d'utilisateur / mot de passe, clé, badge) soit disponible pendant toute la durée de conservation, mais protégé contre l'accès par des personnes non autorisées.	☐
Technologies de chiffrage actuelles	Il faut veiller à recourir à des technologies de chiffrage qui permettent le déchiffrage pendant toute la durée de conservation. En cas de modification de ces technologies au cours de la période de conservation, les données doivent être chiffrées en temps utile à l'aide d'une nouvelle technologie.	☐
Sauvegarde	Lorsque les données sont conservées sous forme de sauvegarde numérique, la restauration de la sauvegarde doit être testée régulièrement (recommandé une fois par an). ***Remarque :*** La recommandation 8 des exigences minimales pour la sécurité informatique élaborées par la FMH fournit d'autres indications sur les mesures à prendre en compte dans le cadre de la création de sauvegardes.	☐

Traçabilité		
Mesure	**Explications/remarques**	**Fait**
Protection contre les modifications non autorisées	Il faut veiller à la visibilité et à la traçabilité des modifications apportées aux données conservées. — Documents papier et supports amovibles : p. ex. liste avec journalisation saisie manuellement — Supports de données numériques : p. ex. journalisation des modifications (logging), y compris pendant la conservation	☐
Protection de la journalisation	Les systèmes de journalisation et les procès-verbaux doivent être protégés contre tout accès non autorisé et toute manipulation.	☐

Collaboration avec des tiers		
Mesure	**Explications/remarques**	**Fait**
Dispositions contractuelles	Lorsque des tiers sont impliqués dans la conservation, des prescriptions contractuelles relatives à la conservation doivent être convenues et leur respect doit être documenté. ***Remarque :*** *Lorsqu'il est fait recours à des prestataires pour la conservation, il convient de veiller à ce qu'ils soient sélectionnés avec soin, instruits quant à leurs obligations et contrôlés régulièrement. Il est recommandé de faire signer une déclaration de confidentialité par les prestataires. Un modèle peut être téléchargé ici.*	☐
Traitement en cas de violation de la sécurité des données	Lorsque des tiers sont impliqués dans la conservation, la procédure en cas de violation de la sécurité des données doit être définie. ***Remarque :*** *La recommandation 10 de la FMH en matière de sécurité informatique (Définir une procédure de gestion des incidents de sécurité) constitue une aide.*	☐
Remise convenue contractuellement	Lorsque des tiers sont impliqués dans la conservation, il faut veiller à la restitution des données à la fin de la collaboration.	☐

Respect des prescriptions		
Mesure	**Explications/remarques**	**Fait**
Contrôle des délais de conservation	Les délais de conservation sont garantis et les données personnelles sont effacées ou détruites immédiatement et de manière irrévocable à l'expiration de ces délais. ***Remarque :*** *En ce qui concerne l'effacement et la destruction de données personnelles, la liste de contrôle Effacement fournit une aide intéressante.*	☐
Documentation	Les délais de conservation et l'effacement ou la destruction subséquente doivent être documentés.	☐

3 Exigences techniques relatives à l'effacement

3.1 Définition de l'effacement et de la destruction

Par destruction de données, on entend généralement la destruction physique des données ou l'effacement irrévocable de données numériques. Alors que par destruction physique on entend la destruction d'un support de données (documents papier, clés USB, CD, etc.), la notion d'effacement englobe le fait de rendre les données enregistrées non identifiables. Contrairement à ce qui se passe lors de la destruction, le support de données est conservé lors de l'effacement.

En principe, le chiffrage de données peut également être considéré comme un moyen d'empêcher l'identification de données lorsque les clés nécessaires au décryptage ont été éliminées.

3.2 Aspects organisationnels

Pour l'effacement dans les délais, il est recommandé d'élaborer une procédure ou un processus définissant ce qui doit être effacé ou détruit, à quel moment et à quelles conditions. Le registre des activités de traitement, qui offre un aperçu des données devant être conservées et de leur durée de conservation, offre une aide à cet égard (cf. modèle de registre des activités de traitement). S'il existe un motif justifiant la poursuite de la conservation, il convient de renoncer à l'effacement. Un tel motif serait, par exemple, le consentement de la patiente ou du patient à la poursuite de la conservation.

3.3 Prise en compte des cas spéciaux

Les données personnelles doivent être irrévocablement effacées ou détruites en tenant compte des délais de conservation légaux et des délais de prescription, puis de l'expiration du délai spécifique. Les données se trouvant dans des archives, sur des copies de sauvegarde ou dans des e-mails ne sont pas exclues de cette règle. Les éléments à prendre en considération ainsi que quelques exemples de procédures sont présentés ci-après à titre d'aide.

3.3.1 Archives

Les données ou les ensembles de données qui doivent être disponibles à long terme, mais qui n'ont plus besoin d'être modifiés, sont souvent placés dans des archives internes. En l'absence de motif justifiant la poursuite de la conservation, les bases de données archivées doivent être détruites dans les délais prescrits par la loi.

Afin de garantir une destruction en temps utile, il est par exemple recommandé de définir un processus de tri annuel. En outre, l'identification claire des données avant le transfert aux archives (p. ex. année du transfert et délai de conservation) facilite le tri.

3.3.2 Sauvegardes

Une protection ou une sauvegarde doit impérativement être installée afin de prévenir toute perte de données. Les sauvegardes à cycles courts (p. ex. quotidiennes, hebdomadaires) sont généralement régulièrement écrasées. Lorsque les données originales sont effacées du système de production, elles disparaissent également des sauvegardes suivantes.

Elles restent en revanche disponibles en présence de sauvegardes à cycles longs (p. ex. mensuelles ou annuelles). En cas de restauration, ces données seraient reconstruites, ce qui annulerait leur effacement.

Afin de s'assurer que les données effacées ne réapparaissent pas après la restauration d'une sauvegarde, il est recommandé de mettre en place un processus de vérification. Il est par exemple possible de tenir une liste dans laquelle sont consignés, à l'aide de données pseudonymisées (p. ex. le numéro de la patiente ou du patient), les jeux de données effacés. En cas de restauration d'une sauvegarde, cette liste permet de vérifier si les données effacées ont également été restaurées. Si tel est le cas, il est possible d'effacer à nouveau immédiatement les données du système de production. En outre, si la date de l'effacement initial est enregistrée dans la liste, la mention peut être supprimée après la dernière sauvegarde à long terme.

En plus d'un tel processus de vérification, des mesures techniques et organisationnelles doivent permettre de contrôler les droits d'accès aux données restaurées.

3.3.3 E-mails

Tout e-mail contenant des données d'une patiente ou d'un patient doit impérativement être archivé dans le dossier médical. Lorsque le dossier médical est effacé conformément aux délais de conservation prescrits par la loi, il convient de veiller à ce que les e-mails associés soient également effacés.

3.4 Exigences en matière de sécurité relatives à l'effacement

Les méthodes d'effacement et de destruction choisies doivent garantir l'effacement définitif. Cela signifie qu'il faut choisir une méthode qui empêche la restauration des données personnelles effacées. Les méthodes permettant de restaurer les données personnelles ne sont pas conformes aux règles en matière de protection des données (p. ex. simple élimination de données personnelles dans des sacs à ordures ou dans des containers à poubelles, ou transfert virtuel dans la poubelle de l'ordinateur ou du cloud).

Le tableau ci-dessous présente les méthodes permettant de garantir un effacement sécurisé. Les explications se basent en particulier sur un aide-mémoire sur la destruction de données électroniques [1], publié par la préposée à la protection des données du canton de Zurich.

[1] https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_vernichten_elektronischer_daten.pdf

Mode de destruction	Description	Évaluation
Destruction physique	Destruction mécanique d'un support de données (broyage, fusion, etc.). Sont considérés comme des supports de données par exemple les CD, clés USB, disques, mais aussi le papier, etc. ***Remarque :*** *S'il est fait recours à des prestataires externes pour l'effacement ou la destruction, il convient de s'assurer que le processus est suffisamment sûr et traçable et que les supports de données ne peuvent pas être réutilisés. Le processus doit être vérifié régulièrement. Le cabinet demeure responsable.*	La conformité de l'effacement aux règles en matière de protection des données est en principe garantie.
Effacement magnétique	Grâce à une magnétisation spécifique, des appareils d'effacement spéciaux permettent d'effacer intégralement les informations contenues dans des disques durs, ce qui rend impossible ou très difficile la reproduction des données. Ce type d'appareil est également efficace pour des disques durs défectueux. Ce procédé est adapté pour les supports de données magnétiques tels que les disques durs et les cartes ou bandes magnétiques (LTO, DLT, DAT, cassettes audio, cassettes vidéo).	L'effacement est irrévocable, mais le procédé rend les supports de données inutilisables.
Effacement par écrasement technique (wiping)	Des fichiers isolés ou des supports de sauvegarde entièrement réinscriptibles peuvent être effacés durablement en les écrasant plusieurs fois avec des chaînes de caractères aléatoires. Cette méthode ne convient pas aux systèmes modernes utilisant des supports de stockage électronique éphémère (Solid State Drive [SSD]).	La destruction est irrévocable.
Effacement de données sur des supports de stockage électronique durable (Solide State Drive)	La plupart du temps, les supports de stockage électronique sont munis d'ordres d'effacement (p. ex. ATA Secure Erase). Si le support de stockage ne dispose d'aucun ordre d'effacement, il est recommandé de chiffrer les données au préalable puis d'effacer la clé.	La destruction est partiellement irrévocable.

Impressum
Edition: FMH – Fédération des médecins suisses, Berne
Publication: mars 2023
www.fmh.ch