AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Mise en place d'une application web ou mobile d’accès au SIS pour des tiers

Guide pratique technique
PGSSI-S

Publication : août 2022 | *Classification : Publique* | *Version : v1.1*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. PREAMBULE

1.1. Objet du guide

Le présent guide propose un ensemble de règles et de recommandations de sécurité relatives à la mise en place, au sein d'un Système d'Information de Santé (SIS), d'une application accessible depuis Internet par des tiers. Cette application est typiquement une application « web » utilisable via un navigateur web.

L'objet de ces règles est de garantir la protection des données et des traitements mis à dispositions de tiers via ce type d'application, ainsi que la protection des autres données et traitement du vis-à-vis de ces accès web. Les règles sont issues des bonnes pratiques en matière de SSI dont les sources sont présentées en Annexe 1 « Fondements du guide ».

Ce document fait partie des guides pratiques techniques de la Politique Générale de Sécurité des Systèmes d'Information de Santé [PGSSI-S].

Ce document s'adresse :

- Aux responsables de structure qui, en tant que responsables de traitement, décident de la mise en œuvre des accès tiers à leur SIS dans le respect des finalités de l'application ;
- Aux personnes agissant sous leur responsabilité, et en particulier celles impliquées dans :
  - La conception et la réalisation de l'application,
  - L'hébergement et l'exploitation de l'application,
  - La mise en œuvre de la sécurité des SIS.

Pour des raisons de facilité de lecture, dans la suite du document, le terme « Responsable du SIS » ou « Responsable » est utilisé pour désigner toute personne en charge de la mise en œuvre de tout ou partie des règles, qu'elle soit la personne responsable de la structure ou une personne agissant sous sa responsabilité.

1.2. Définitions et concepts

Les documents cités en référence sous la forme [REF], ainsi que ceux sur lesquels s'appuie le présent guide sont présentés sont détaillés en Annexe 1. La consultation de ces documents permettra au lecteur d'approfondir les thèmes traités.

Le glossaire en Annexe 2 donne la signification des acronymes et de certains termes techniques utilisés.

1.2.1. Service en ligne

Dans le cadre de ce guide, le terme « service en ligne » désigne un service d'accès, via Internet, à des données et traitements mis à disposition par le SIS.

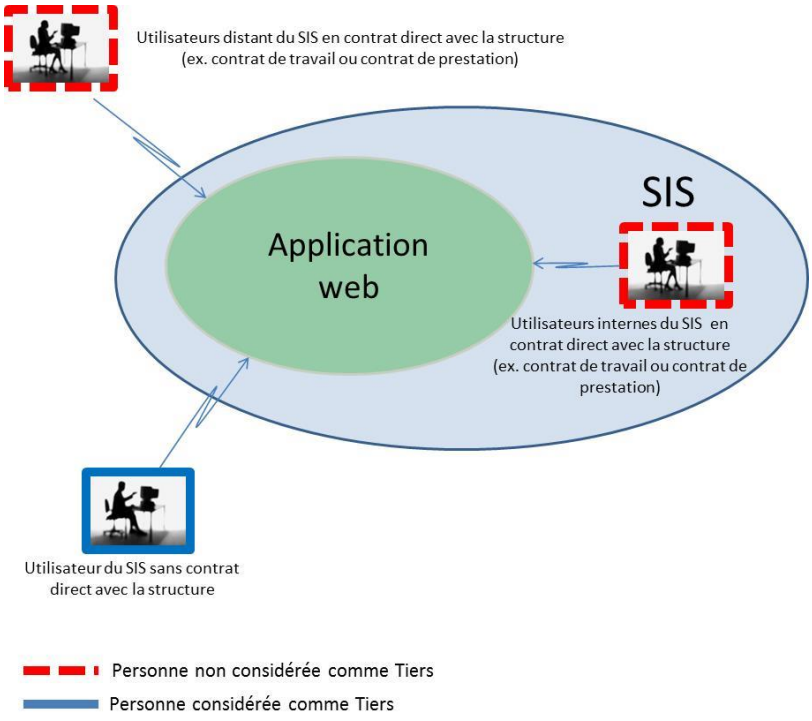
Les services en lignes considérés dans ce guide sont généralement, mais pas nécessairement, des services numériques en santé au sens de l'article L1470-1 du code de la santé publique [CSP-L1470].

1.2.2. Application web

Dans le cadre de ce guide, un ou plusieurs services en ligne offerts par le SIS à des tiers via une même interface web constituent une application web.

1.2.3. Tiers

Le terme « tiers » désigne, de manière générale, toute personne que le Responsable autorise à accéder à des services en ligne fournis par le SIS, sans que ce Responsable n'ait de maîtrise sur l'environnement, le contexte d'utilisation ou les moyens mis en œuvre du côté de l'utilisateur.



1.2.4. Accès web tiers

Dans ce guide, on désigne par « accès web tier » au SIS toute application web donnant accès à des tiers, par Internet, à des données et traitements mis à disposition par le SIS.

1.3. Périmètre d'application du guide

Le périmètre d'application de ce guide est celui fixé à l'article L1470-1 du code de la santé publique [CSP-L1470] : est concerné l'ensemble des services numériques en santé, les systèmes d'information (SI) ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités.

Au sein de ce périmètre, le présent guide décrit les règles applicables aux systèmes permettant l'accès de tiers aux SIS via une application web.

1.3.1. Périmètre système concerné

Ce guide ne concerne que les accès web à des services offert par le SIS : les applications web considérées sont celles qui permettent à des tiers d'accéder, et de manière plus générale de réaliser des traitements[1] de données de santé à caractère personnel (*par exemple relatives au parcours de soins : prise de rendez-vous dans un cabinet ou un établissement de santé, consultation de résultats d'examens de biologie médicale…*), médico-économiques (*par exemple relatives à de la facturation de soins ou de services complémentaires*), à des données à caractère personnel ou à des données sensibles, quelle que soit la finalité de ces applications.

Dans la mesure où ces applications web traitent de telles données, elles sont considérées comme faisant partie d'un SIS.

1.3.2. Périmètre utilisateur concerné

Ce guide concerne uniquement les accès à des applications web par des tiers tels que défini plus haut au chapitre 1.2.3.

Dans la pratique, et selon les cas, ces tiers peuvent être :

- Des usagers des services proposés par l'établissement de santé (ex. : patients, proches de patient, fournisseurs…) ;
- Des professionnels de santé (PS) extérieurs à l'établissement de santé, qui n'ont pas de lien juridique direct (contrat ou autre) avec la structure et qui concourent à la prise en charge de patients.

Les accès en mobilité par des personnes disposant d'un lien juridique direct avec la structure sont, de fait, exclus du périmètre du guide.

1.4. Limites du périmètre d'application du guide

1.4.1. Autres modalités d'accès à des services ou données du SIS

Les modalités d'accès à des services ou données du SIS autres que par une application web n'entrent pas dans le périmètre du guide (ex. : demande de dossier médical émanant de patient, de représentant légal, d'ayant-droit, réquisition et plus généralement toute demande faite par écrit faisant l'objet d'une extraction réalisée par le Responsable et transmise au demandeur quel que soit le média utilisé pour cette transmission).

1.4.2. Services de télémédecine, de téléconseil ou de commerce en ligne

Les applications web proposant des services de télémédecine, de téléconseil ou de commerce en ligne sont également exclues du présent guide. Ils présentent en effet certains enjeux et risques spécifiques du fait de leurs fonctions et des technologies mises en œuvre, et requièrent des mesures de sécurité complémentaires qui ne sont

[1] Au sens du 2) de l'article 4 du [RGPD] : « traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. »

pas présentées ici. Les règles proposées dans le présent guide restent néanmoins applicables et peuvent servir de base de travail pour la sécurisation de ce type de sites.

1.4.3. Accès à des services sans interaction avec le SIS

Les applications web proposant des services qui n'échangent aucune donnée avec le SIS, et qui n'interagissent pas avec lui, sont également exclues du présent guide.

1.4.4. Interventions à distance sur le SIS

Le cas des interventions réalisées à distance sur le SIS n'entre pas dans le champ de ce guide. Il est traité dans le guide pratique technique « Règles pour les interventions à distance sur les Systèmes d'Information de Santé » [GRIAD].

2. ENJEUX PRINCIPAUX RELATIFS AUX ACCES AU SIS PAR DES TIERS VIA UNE APPLICATION WEB

2.1. Cadre de l'accès au SIS par des tiers

L'article L1111-7 du code de la santé publique dispose que « *Toute personne a accès à l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit, par des professionnels de santé, par des établissements de santé par des centres de santé, par des maisons de naissance, par le service de santé des armées ou par l'Institution nationale des invalides qui sont formalisées ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment des résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé […]* ». L'accès des titulaires de l'autorité parentale et des ayants droit est réglementé.

Il appartient au Responsable de mettre en place des procédures et des moyens de contrôle d'accès respectant la réglementation en vigueur dans le cas où l'accès à son dossier médical par le patient ou les personnes autorisées de son entourage se fait au moyen d'un accès tiers au SIS.

2.2. Multiplication des applications web liées aux données de santé à caractère personnel

Les services en ligne se développent fortement dans le secteur de la santé.

L'ouverture d'un accès tiers à un SIS peut avoir plusieurs finalités :

- La communication d'informations à l'usager du système de santé, et en particulier de données de santé lorsque l'usager est patient de la structure ou personne autorisée (*par exemple tuteur légal*). Ce type d'accès ouvre la possibilité d'échanges dématérialisés qui permettent une transmission rapide et évitent l'envoi de courrier postal ou le déplacement de l'usager. Cette catégorie inclut notamment les serveurs de résultats pour les examens de biologie médicale ;
- L'ouverture de services à destination des patients ou de personnes autorisées. Ce type d'accès permet par exemple d'améliorer l'efficacité de certains processus de prise en charge. Cette catégorie regroupe des services tels que la prise de rendez-vous en ligne, le rappel de certaines actions que le patient doit effectuer, les conseils personnalisés, la saisie d'informations en vue d'une hospitalisation…
- L'ouverture de services à destination de PS extérieurs à l'établissement de santé concourant à la prise en charge du patient. Ce type d'accès permet par exemple au PS d'accéder à un espace collaboratif de prise en charge du patient ou de visualiser des informations de soin concernant son patient. Cette catégorie inclut des services tels que l'imagerie médicale utile à la production de soins et n'ayant pas vocation à être intégré dans un outil de coordination des soins tel que le DMP.

2.3. Cadre juridique relatif au traitement des données de santé à caractère personnel

Le cadre législatif et réglementaire impose le respect de règles précises dès lors que sont traitées des données à caractère personnel, et en particulier quand elles sont traitées informatiquement. Ces règles sont d'autant plus contraignantes que ces données ont trait à la santé d'un patient et sont ainsi soumises au secret professionnel.

Le présent guide est notamment établi pour aider les acteurs concernés à respecter les obligations légales et règlementaires applicables au traitement informatisé des données à caractère personnel, dont les données de santé à caractère personnel, et en particulier certaines exigences de la loi « informatique et libertés » [L78-17], du « règlement général sur la protection des données » [RGPD] et du code de la santé publique en matière de protection des données des patients.

Il est rappelé que les structures publiques qui mettent en œuvre des services en ligne tels que des accès web doivent également se conformer au Référentiel Général de Sécurité [RGS].

☞ Il est toutefois rappelé que le présent guide ne constitue qu'une aide et que son application n'exonère pas des obligations en vigueur.

☞ Il appartient à chaque responsable d'un traitement qui met en œuvre un accès tiers au SIS d'identifier les lois et règlements applicables et de s'y conformer. Les exigences applicables dépendent en particulier de la nature des données, de la finalité et de la nature du traitement, de l'organisation de mise en œuvre de l'application web…

- Il est rappelé que la communication au patient de certaines informations doit parfois respecter un processus spécifique. En particulier, quand l'information communiquée entre dans le cadre du dispositif d'annonce, une consultation d'annonce doit impérativement précéder la mise à disposition des données de santé et du diagnostic.

2.4. Risques liés à la mise en œuvre d'accès de tiers aux données de santé du SIS

Les accès web tiers constituent, par nature, des points d'entrée très exposés du système d'information. Leur sécurisation revêt une grande importance au regard des différents types d'atteintes au SIS potentiellement induites par l'exploitation des vulnérabilités des services en ligne par des personnes malintentionnées :

- Atteinte à l'intégrité des informations (modifications illégitimes des données de santé à caractère personnel, des données de rendez-vous médical…), en particulier lorsqu'elle a pour effet d'impacter les processus de prise en charge des patients ;
- Atteinte à la confidentialité des données à caractère personnel du patient (divulgation au-delà de l'équipe de soins, voire divulgation publique) ;
- Atteinte à la disponibilité des services proposés aux patients, en particulier lorsqu'elle est susceptible d'impacter les processus internes de la structure offrant le service (blocage du système de prise de rendez-vous du patient en ligne par exemple) ou de dégrader la prise en charge des patients ;
- Atteinte à l'auditabilité des opérations réalisées sur les données de santé (absence de traces d'accès ou de modification des données, modification intempestive de ces traces...).

L'exploitation de vulnérabilités par des personnes malveillantes peut en outre conduire à l'intrusion dans le SIS ou dans les terminaux des tiers qui y accèdent, et à la propagation d'incidents de sécurité à ces systèmes, avec des impacts potentiellement graves pouvant aller jusqu'à la perte de chance de patients.

Dès lors, il est clair qu'une séparation aussi forte que possible entre l'application web et le reste du SIS est nécessaire afin de redire ces risques.

3. PRINCIPES ESSENTIELS A APPLIQUER

3.1. Principes de sécurité

3.1.1. Identifier les enjeux et les risques liés à l'accès de tiers envisagé

La conception de l'application, de son intégration avec le SIS et des modalités de son hébergement et de son exploitation doivent être réalisés en regard d'une analyse de risque concernant les services qu'elle propose, et en prenant explicitement en compte la protection des données de santé à caractère personnel qui y sont traitées.

Ce dernier aspect comprend en particulier la garantie de confidentialité des données (que ce soit un vol massif de données par un attaquant externe, ou la consultation plus ou moins étendue de données par un professionnel, un usager ou un autre type d'intervenant) ainsi que d'intégrité des données (modification non autorisée ou accidentelle des données).

L'analyse de risque doit couvrir l'ensemble des accès potentiels aux données, qu'ils soient fonctionnels (utilisateurs du service) ou techniques (personnels en charge de la construction, de la maintenance ou de l'exploitation du système hébergeant l'application et des systèmes de gestion des SI associés). Il est fortement recommandé de mener cette analyse de risque selon une méthodologie formalisée et éprouvée, telle que la méthode EBIOS Risk Manager [EBIOS RM] proposée par l'ANSSI.

3.1.2. S'appuyer autant que possible sur des solutions existantes

La conception, la réalisation et l'exploitation de services d'accès web au SIS ouvert aux tiers qui respectent les exigences de sécurité liées aux données de santé personnel nécessitent la mobilisation de moyens notables.

Aussi, dès lors qu'un tel projet est étudié, il est fortement recommandé de vérifier s'il existe déjà un service mutualisé en mesure de remplir les fonctions attendues tout en répondant aux exigences de sécurité formulées pour l'application.

Par exemple, s'il s'agit de conservation d'informations utiles à la coordination des soins, l'alimentation du Dossier Médical Partagé (DMP) du patient ou la transmission directe via une messagerie sécurisée de santé devraient être privilégiées. Ces services bénéficient des moyens de protection appropriés pour ce type d'informations et ne nécessitent pas la mise en place d'application web au niveau des SIS.

3.1.3. Intégrer l'application web dans le processus standard de gestion continue de la sécurité

Comme tout composant du SIS, l'application web doit être intégrée au processus standard de gouvernance et de gestion continue de la sécurité des SI de la structure, sur l'ensemble des étapes de son cycle de vie :

- Sélection ou conception ;
- Réalisation le cas échéant ;
- Intégration au SIS ;
- Hébergement et exploitation ;
- Correction et évolution ;
- Fin d'exploitation (migration vers une autre application ou arrêt définitif).

Pour rappel, les autorités administratives doivent appliquer le Référentiel Général de Sécurité [RGS] pour la sécurisation de leurs échanges avec d'autres autorités administratives ou avec des usagers, ainsi que la Politique de Sécurité des Systèmes d'Information pour les Ministère Chargés des Affaires Sociales [PSSI-MCAS]. L'analyse de risque et l'homologation[2] de l'application préalablement à sa mise en production font partie des démarches imposées par ces textes.

Bien entendu, les exigences déclouant des textes mentionnés au chapitre 2.3 doivent également être prises en compte dans la gestion continue de la sécurité de l'application web.

3.2. Utilisation du guide

Comme rappelé au chapitre précédent, la sécurité d'une application web doit être :

- Prévue dès la phase de conception de l'application ;
- Mise en place dans la phase de réalisation (développement, intégration et tests) ;
- Maintenue pendant toute la phase de fonctionnement des services en ligne que l'application propose.

Les règles de sécurité du guide intéressent l'ensemble des acteurs de ces différentes phases.

Le guide invite tout **Responsable** :

- À mettre en œuvre les règles générales ;
- À faire respecter toutes les règles par les services chargés de la mise en œuvre en interne et/ou par les prestataires externes et à en contrôler la bonne application.

Le guide invite les **acteurs en charge de la conception, de la réalisation ou de la maintenance** d'une application web :

- À mettre en œuvre les règles liées à la conception et à la réalisation de l'application ;
- À justifier de leur bonne application auprès du Responsable.

Le guide invite les **acteurs en charge de l'hébergement ou de l'exploitation** d'une application web :

- À mettre en œuvre les règles liées à l'hébergement et à l'exploitation de l'application ;
- À justifier de leur bonne application auprès du Responsable.

Les règles sont présentées au chapitre **Erreur ! Source du renvoi introuvable.**.

[2] Voir [HOMOLOGATION]

4. REGLES POUR LA MISE EN PLACE D'UN ACCES WEB AU SIS POUR DES TIERS

La totalité des règles ci-après est applicable à toute mise en place d'un accès web au SIS pour des tiers, sauf mention spécifique. Il n'est donc pas distingué des paliers de mise en œuvre.

4.1. Règles générales

4.1.1. Bonnes pratiques concernant une application accessible via le web

N°	Règle
[GP1]	Le Responsable doit veiller au respect des obligations légales et qui relèvent de son périmètre de responsabilité pour l'application : finalité de l'application web, consentement du patient, certification ou agrément de l'hébergeur des données de santé, obligations relatives à la mise en ligne d'un site Internet telles que mentions légales, conditions générales d'utilisation, conservation des données de connexion, information des utilisateurs sur la collecte d'informations à caractère personnel…
[GP2]	Le Responsable doit veiller à ce que les données échangées entre l'application et le reste du SIS soient protégées en confidentialité et en intégrité et que leur origine soit garantie (authenticité des données).
[GP3]	Le Responsable doit veiller à ce que des dispositions de protection et de cloisonnement physique ou logique entre l'application (ou sa plateforme d'hébergement) et le reste du SIS empêchent la propagation d'incidents de sécurité ou de code malveillant entre ces deux sous-ensembles.
[GP4]	Le Responsable doit veiller à ce que des dispositions de protection et de cloisonnement physique ou logique entre l'application (ou sa plateforme d'hébergement) et les applications accessibles depuis Internet mais destinées au personnel interne à la structure empêchent la propagation d'incidents de sécurité ou de code malveillant entre ces deux sous-ensembles.
[GP5]	Le Responsable doit veiller à ce que des dispositions de protection et de cloisonnement physique ou logique entre l'application (ou sa plateforme d'hébergement) et des applications relevant d'autres Responsables empêchent la propagation d'incidents de sécurité ou de code malveillant entre ces applications.
[GP6]	Le Responsable doit veiller à interdire toute utilisation des données réelles de l'application à d'autres fins que celles prévues, notamment à l'exclure des activités de développement, de test ou de maintenance. Pour cela, des outils de génération de jeux de données de test, ou à défaut des outils validés d'anonymisation des données doivent être disponibles, et les procédures d'utilisation associées documentées.
[GP7]	Le Responsable doit veiller à ce que chaque personne intervenant dans le maintien en condition opérationnelle de l'application (administrateur, exploitant, agent de maintenance, etc.) ait signé un engagement individuel de confidentialité.
[GP8]	L'exploitant et le Responsable doivent convenir de leurs engagements respectifs pour assurer le bon fonctionnement de l'application. A ce titre, ils doivent mettre en œuvre des procédures de surveillance de la sécurité, de gestion des incidents de sécurité et de gestion des vulnérabilités relatives à l'application web.
[GP9]	Le Responsable doit suivre et faire contrôler au moins une fois tous les trois ans : ► La sécurité de l'hébergement et de l'exploitation de l'application ; ► La prise en compte du traitement des vulnérabilités dans l'application et dans sa plateforme d'hébergement. Il doit notamment s'assurer de la réalisation régulière de tests de vulnérabilités et de tests d'intrusion sur l'application et sur la plateforme. Dans le cas d'un recours à une prestation d'hébergement externe par un hébergeur de données de santé certifié ou agréé, le Responsable peut se baser sur le certificat ou l'agrément de l'hébergeur pour les aspects qui relèvent du périmètre de responsabilité de l'hébergeur en question et qui sont pris en compte dans la

N°	Règle
	certification ou l'agrément (*par exemple, le traitement des vulnérabilités applicatives peut relever de l'hébergeur ou de son client en fonction du contrat passé*).

4.1.2. Règles générales relatives à l'accès authentifié de tiers

N°	Règle
[GA1]	Tout utilisateur de l'accès web tiers doit faire l'objet d'une identification électronique avant de pouvoir utiliser l'application (s'il est autorisé à le faire) dès lors qu'au moins un des services en ligne proposés par l'application permet le traitement[3] de données à caractère personnel, qu'il s'agisse ou non de données de santé.
[GA2]	L'identification électronique des utilisateurs de l'accès web tiers doit être conforme aux référentiels d'identification électroniques de la PGSSI-S correspondant à la nature de ces utilisateurs dès lors qu'au moins un des services en ligne proposés par l'application est un service numérique de santé au sens de l'article L1470-1 du code de la santé publique [CSP-L1470]. Les référentiels qui doivent être respectés en application des articles L1470-1 à L1470-5 du code de la santé publique sont, en fonction de la nature des utilisateurs de l'application : ► Le « référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes morales] » [IE-ASPM] pour les utilisateurs qui sont des acteurs des secteurs sanitaire, médico-social et social et qui sont personnes morales ; ► Le « référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes physiques] » [IE-ASPP] pour les utilisateurs qui sont des acteurs des secteurs sanitaire, médico-social et social et qui sont personnes physiques ; ► Le référentiel d'identification électronique des usagers [IE-Usagers] pour les utilisateurs qui sont des usagers des secteurs sanitaire, médico-social et social et qui sont des personnes physiques (*patient, citoyen, aidant...*).
[GA3]	Il est recommandé que les exigences fixées par les référentiels mentionnés dans la règle GA2 et relatives à l'identification électronique des seuls acteurs des secteurs sanitaire, médico-social et social soient également appliquées pour les applications web qui, bien que ne donnant pas accès à des traitements de données de santé à caractère personnel, donnent accès à des traitements d'autres types de données à caractère personnel ou de données sensibles réalisés au sein du SIS. Note : En ce qui concerne l'identification électronique des usagers, la règle GA2 ne peut pas être étendue à d'autres périmètres que ceux permettant leur prise en charge à des fins sanitaires et médico-sociales (voir article L1111-8-1 du code de la santé publique [CSP-L1111-8-1]).
[GA4]	Le Responsable doit s'appuyer sur un ensemble de procédures qui définissent les règles de gestion des comptes utilisateurs et qui couvrent notamment : ► La phase d'enrôlement comprenant la création des comptes d'accès individuel des tiers et dans laquelle l'identité de chaque tiers est : • Soit vérifiée lors de la remise des moyens d'identification électronique à ce dernier (*par exemple, l'utilisation de CPS pour l'authentification de tiers professionnels de santé*), • Soit intégrée sur la base des informations d'identités fournies par le moyen d'identification électronique accepté pour l'identification de l'utilisateur en conformité avec la règle GA2 ; ► Les situations dans lesquelles un compte doit être suspendu (*par exemple : absence prolongée du titulaire du compte ou non usage prolongé du service, suspicion d'usurpation du compte…*) ou bloqué (*par exemple : départ ou décès du titulaire du compte, résiliation par le titulaire…*). ► La vérification régulière (au moins annuelle) de la légitimité du maintien de chaque compte ;

[3] Au sens du 2) de l'article 4 du [RGPD]

N°	Règle
	Ces différents aspects, comme ceux traités par les autres règles GA, doivent être modulés en fonction des enjeux spécifiques aux services offerts par l'application web considérée et de leurs modalités d'utilisation.
[GA5]	Le Responsable doit vérifier qu'il dispose des informations lui permettant d'informer chaque tiers, qu'il soit utilisateur ou bien qu'il soit la personne à laquelle se rapporte la donnée (*par exemple le patient*), en cas d'incident ou de suspicion d'incident pouvant affecter l'utilisation de l'application ou les données à caractère personnel le concernant.
[GA6]	Le Responsable doit sensibiliser les tiers à la sécurité des terminaux utilisés pour accéder à l'application.[4]
[GA7]	Le Responsable doit sensibiliser les tiers à la sécurité de leurs moyens d'identification et d'authentification.
[GA8]	Le Responsable doit donner aux tiers les coordonnées du support, leur permettant notamment de signaler des tentatives d'hameçonnage[5] ou d'autres courriels malveillants relatifs aux services offerts par l'application.
[GA9]	Il est recommandé aux fournisseurs de services numériques en santé de produire un engagement de conformité aux référentiels d'identification électronique [IE-ASPM], [IE-ASPM] et/ou [IE-Usagers] concernés, comme détaillé dans ces mêmes référentiels. Des modèles d'engagement de conformité [ENGAGEMENT] sont proposés conjointement à ces référentiels d'identification électronique.

4.1.3. Règles générales relatives à l'utilisation de mécanismes cryptographiques

N°	Règle
[GC1]	La mise en œuvre de chiffrement, de contrôle d'intégrité, de signature ou de cachet électronique, de vérification de mot de passe, de génération de valeur aléatoire, et plus généralement de tout mécanisme cryptographique à fin d'authentification d'utilisateur ou de système, ou de protection de données, doit Ces mécanismes doivent être conformes : ► Aux règles techniques du RGS [RGS-A1] ; ► Au guide de sélection d'algorithmes cryptographiques [CRYPTOSEL] publié par l'ANSSI ; ► Au guide des mécanismes cryptographiques [CRYPTO] publié par l'ANSSI.
[GC2]	Les détails de mise en œuvre des mécanismes cryptographiques étant propices à des erreurs qui en dégradent fortement l'efficacité, il est hautement recommandé de n'utiliser que des librairies logicielles de haut niveau (c'est-à-dire ne pas recourir directement aux primitives cryptographiques élémentaires), éprouvées et validées par des experts du domaine, en respectant scrupuleusement les modalités précises de mises en œuvre prescrites par ces solutions.
[GC3]	Un soin particulier doit être apporté à la gestion des clés utilisées pour les mécanismes cryptographiques. On pourra se reporter au document du RGS qui traite de ce sujet [RGS-B2].

[4] Pour cette règle comme pour les deux suivantes, il s'agit de mettre en place une sensibilisation adaptée à des tiers ne disposant pas d'expertise spécifique.

[5] Également appelé « filoutage » ou « phishing » : technique d'obtention illicite d'identifiants et de mots de passe de victimes en usurpant l'identité d'une entreprise ou d'un organisme connu, généralement à l'aide de courriels imitant ceux de cet organisme.

4.2. Conception et réalisation de l'application

4.2.1. Processus de conception et de réalisation

N°	Règle
[CR1]	L'application web doit être de conception simple et son codage doit respecter des standards pérennes (issus du W3C[6] par exemple) afin de faciliter son contrôle, sa maintenance et sa réversibilité.
[CR2]	Le maître d'œuvre du développement de l'application doit garantir au Responsable que : ► Des mesures ont été prises afin d'éviter les différents types de vulnérabilités identifiées et publiées par l'OWASP (voir [OWASP]) ; ► L'absence de telles vulnérabilités a été vérifiée avant mise en production ; ► Les différentes problématiques et les recommandations associées décrites dans le guide « Recommandations pour la mise en œuvre d'un site web : Maîtriser les standards de sécurité côté navigateur » [RECOWEB] publié par l'ANSSI ont bien été prises en compte. ► Les exigences de protection des données à caractère personnel découlant du [RGPD] ont été prises en compte dès la conception de l'application et tout au long de sa réalisation, ainsi que le Guide RGPD de l'équipe de développement [GDEVCNIL] élaboré par le CNIL.
[CR3]	Le code de l'application doit au minimum être vérifié par un outil de détection automatique de vulnérabilités courantes dans les applications web (comme par exemple l'utilisation de fonctions « dangereuses », l'absence de contrôle des entrées, l'absence de nettoyage des sorties…). Ces vérifications peuvent également être réalisées par une équipe interne si la structure dispose de ces compétences particulières, ou par un prestataire d'audit de code disposant si possible de la qualification PASSI[7] délivrée par l'ANSSI.
[CR4]	La phase de recette de l'application et de ses mises à jour majeures doit intégrer des tests de vulnérabilités et des tests d'intrusion faisant l'objet d'un rapport formel.
[CR5]	Les environnements de développement, de recette et de préproduction doivent être distincts de l'environnement de production. Ils doivent disposer de protections similaires à celles mises en œuvre pour la production (voir règles DT12 et HE2) Il est recommandé que les environnements de développement, de recette et de préproduction soient distincts et cloisonnés les uns vis-à-vis des autres.
[CR6]	Pendant toute la durée de vie de l'application web, le maître d'œuvre de la réalisation de l'application doit : ► Signaler au Responsable les vulnérabilités publiées ou détectées relatives à l'application livrée ; ► Fournir les correctifs ou les consignes qui permettent d'empêcher l'exploitation des vulnérabilités dans l'attente de la fourniture du correctif.

4.2.2. Accès authentifié de tiers

N°	Règle
[AA1]	L'application doit permettre aux tiers de réaliser uniquement des actions qui relèvent de leur rôle (*par exemple, pas de modification de documents médicaux par des non PS*).

[6] https://www.w3.org/

[7] Prestataire d'audit de la sécurité des systèmes d'information

N°	Règle
[AA2]	Les mécanismes assurant le lien entre le tiers et les données et traitements auxquels il accède doivent être robustes. En particulier, aucun tiers connecté ne doit pouvoir accéder à des données de santé à caractère personnel auxquelles il n'a pas droit (*par exemple, la modification de paramètres de connexion, comme une modification de l'URL une fois la session ouverte, ne doit pas permettre d'accéder à des données d'autres personnes*).
[AA3]	L'application doit vérifier la validité (chaîne de certification, non expiration et non-révocation) des certificats cryptographiques utilisés dans le cadre de ses échanges avec des équipements distants.
[AA4]	Outre la conformité aux référentiels d'identification électronique rappelée aux règles GA2 et GA3, les guides « Recommandations relatives à l'authentification multifacteur et aux mots de passe » [ANSSI-MDP] de l'ANSSI ou la fiche « Authentification par mot de passe : les mesures de sécurité élémentaires » [CNIL-MDP] de la CNIL doivent être respectés, selon le type de moyens d'identification électronique utilisés dans l'application.
[AA5]	Quand l'application web accède au SIS pour le compte d'un utilisateur authentifié, cet accès doit être réalisé selon les modalités exposées au chapitre « Identification électronique indirecte » du référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes morales] [IE-ASPM].
[AA6]	Les mots de passe ou les liens Internet proposés par l'application aux utilisateurs comme moyen d'authentification temporaire (*mot de passe initialement fourni à l'utilisateur pour son premier accès aux services, lien Internet de validation d'adresse courriel à la création du compte, mot de passe temporaire de récupération de compte…*) ne doivent pas être prédictibles. L'algorithme de génération de ces mots de passe et liens doit de préférence suivre les principes énoncés par les documents listés par la règle GC1.
[AA7]	L'application doit comporter des mécanismes de détection et de protection contre les tentatives systématiques de connexion faites en usurpant l'identifiant d'utilisateurs légitimes. En particulier, l'application doit limiter la fréquence de tentatives de connexion infructueuses successives. Typiquement, cette limitation peut être réalisée : ► Par compte utilisateur dont l'identité est utilisée pour les connexion infructueuses : par exemple, le système d'ouverture de session peut interdire toute nouvelle tentative de connexion pour ce compte utilisateur avant un délai de 2 secondes après le premier échec d'authentification, puis doubler ce délai entre les tentatives de connexion à chaque nouvel échec, jusqu'à par exemple un délai maximum de 5 minutes (soit à partir du 9e échec) entre toutes les tentatives suivantes ; ► Par adresse IP d'origine de la tentative de connexion : dans ce cas, le principe de délai imposé entre chaque nouvelle connexion infructueuse est associé à l'adresse IP d'origine plutôt qu'au compte utilisateur concerné, et le maximum pour ce délai croissant peut être positionné à un niveau beaucoup plus élevé que dans l'option précédente, typiquement de l'ordre de l'heure ou de la journée, voire plus. Les mécanismes de limitation mis en œuvre doivent éviter d'entrainer un blocage effectif du compte utilisateur pour l'utilisateur légitime, qui requerrait une intervention manuelle de déblocage et ouvrirait la porte à un déni de service massif à l'encontre des utilisateurs. C'est pourquoi la seconde des deux options présentées ci-dessus est la plus favorable : elle permet de se focaliser sur le ou les sources d'attaque plutôt que sur les cibles, et ne bloquent pas les utilisateurs légitimes. Cette disposition ne remplace en rien la nécessité d'alerte automatique des administrateurs système en cas d'échec d'authentification répété. En ralentissant l'attaque potentielle, elle laisse au contraire le temps au personnel compétent d'intervenir ou permet d'activer des dispositions complémentaires le cas échéant.
[AA8]	Il convient d'interroger la nécessité d'autoriser aux utilisateurs de disposer de plusieurs sessions ouvertes simultanément. Si cette possibilité n'est pas jugée nécessaire, il est recommandé que l'application n'autorise, à tout moment, qu'une seule session ouverte par utilisateur. Dans ce cas, l'application de cette règle peut se faire de deux manières, parmi lesquelles le Responsable doit choisir : ► Soit l'interdiction de nouvelles connexions de l'utilisateur tant qu'une session qui lui est associée est ouverte. Cette option nécessite que l'application vérifie fréquemment (par exemple toutes les minutes) que la partie « cliente » (navigateur web) est toujours active, à défaut de quoi une fermeture intempestive (ex : fermeture

N°	Règle
	du navigateur sans action de déconnexion) du client pourrait laisser la session ouverte pendant une longue durée et interdire toute connexion légitime de l'utilisateur ; ► Soit la fermeture de toute session éventuellement en cours lorsque l'utilisateur associé se connecte. La tentative d'utilisation d'une session fermée automatiquement pour cette raison doit informer l'utilisateur de la raison de la fermeture et lui indiquer le moyen d'alerter la structure s'il soupçonne une usurpation de son compte.
[AA9]	A l'ouverture d'une session authentifiée, l'application web doit indiquer à l'utilisateur la date et l'heure de la dernière connexion effectuée sous son identifiant.
[AA10]	Toute application web utilisant des jetons (cookies ou autres) afin de « matérialiser » l'état authentifié d'une session doit effectuer un suivi des jetons pour chaque session ouverte. Elle doit vérifier l'authenticité de tout jeton qui lui est transmis par le navigateur de l'utilisateur avant de l'utiliser pour identifier la session utilisateur ou utiliser toute information qu'il transporte. La suppression d'un jeton dans a liste des jetons suivis doit permettre l'invalidation de la session authentifiée associée.
[AA11]	Toute application web utilisant des jetons (cookies ou autres) afin de « matérialiser » l'état authentifié d'une session doit limiter la durée de vie de ces jetons à chacune des sessions.
[AA12]	L'application doit permettre à l'utilisateur de se déconnecter à tout instant. Cette déconnexion doit entrainer la suppression des jetons de session.
[AA13]	L'application doit limiter la durée de validité des sessions authentifiées, notamment : ► Par la durée de validité des jetons de sessions ; ► En cas d'inactivité prolongée de l'utilisateurs. Ces paramètres de durée doivent être fixés par le Responsable au vu de l'analyse de risque et des modalités d'utilisation prévues de l'application.

4.2.3. Protections des données et des traitements

N°	Règle
[DT1]	L'application doit intégrer des mécanismes de vérification des données qu'elle reçoit et de celles qu'elle transmet, associés à des mécanismes de traitement des erreurs. Les vérifications doivent porter sur le format et la vraisemblance des données et sur l'absence de code malveillant.
[DT2]	L'application web doit révéler le moins d'information possible à l'utilisateur sur sa réalisation ou son environnement d'exploitation (*éviter par exemple de divulguer la configuration, la version, le langage utilisé, l'organisation des répertoires ; vulgariser les messages d'erreur visibles de l'utilisateur afin de limiter le contenu des messages d'erreur au strict minimum sur la raison de l'échec*…).
[DT3]	L'application ne doit pas permettre à l'utilisateur, par manipulation d'URL ou de paramètres de requête, d'explorer la structure applicative ni d'accéder à des données ou fonctions auxquelles il n'est pas autorisé.
[DT4]	Les données de santé à caractère personnel, conservées par l'application web à titre permanent sur des supports de stockage, doivent l'être sous une forme protégée par chiffrement et par une fonction de contrôle d'intégrité (signature ou cachet électronique par exemple). Ces fonctions et leur mise en œuvre doivent être conformes aux règles GC1, GC2 et GC3. La mise en œuvre du chiffrement doit préserver la capacité de restituer en clair à chaque tiers les données auxquelles il a légitimement accès. Il est fortement préconisé de favoriser une architecture dans laquelle les données ne sont stockées ni sur les frontaux web, ni sur les serveurs d'applications de l'application web.

N°	Règle
	Des mesures relatives au contrôle d'intégrité sont proposées dans le guide pratique technique « Mécanismes de protection de l'intégrité des données stockées » [GMPIDS] du corpus documentaire PGSSI-S.
[DT5]	Les données de santé à caractère personnel, conservées par l'application à titre temporaire sur des supports de stockage dans le cadre de leur traitement, doivent être effacées de ces supports à l'issue de leur traitement. Cet effacement doit être réalisé par écrasement, c'est-à-dire par réécriture des fichiers à l'aide d'un remplissage intégral par une valeur fixe (typiquement zéro) ou aléatoire, ou par une méthode équivalente qui garantisse que les données ne peuvent être consultée ultérieurement par les interfaces d'accès au système de stockage des données[8]. Quand le système de stockage ne peut pas fournir de garantie suffisante d'inaccessibilité effective des données supprimées, les exigences fixées par la règle DT4 doivent également être appliquées aux données conservées à titre temporaire. Pour plus d'information, se reporter au Guide pratique technique « Destruction des données lors du transfert de matériel informatique » [GDD] du corpus documentaire PGSSI-S.
[DT6]	Dès lors que l'utilisateur commence le processus d'authentification, et pour toute la durée de sa session authentifiée, l'application web doit imposer la mise en œuvre de canaux sécurisés HTTPS (à l'aide d'une version du protocole TLS à l'état de l'art et non-vulnérable) pour tout échange entre sa plateforme et le navigateur web de l'utilisateur et mettre en œuvre les fonctions d'authentification, de chiffrement et de contrôle d'intégrité que permet ce protocole. La mise en œuvre de ces technologies doit se conformer aux règles et recommandations du RGS [RGS-A1] et [RGS-B2] et aux recommandations de sécurité relatives à TLS [RECOTLS] publiées par l'ANSSI.
[DT7]	Tout communication par réseau informatique, que ce soit entre l'application web et les autres parties du SIS, ou entre les composants de l'application, doit être réalisée exclusivement par des canaux sécurisés à l'aide de protocoles (TLS quand applicable, à défaut IPSEC si possible, autres sinon) à l'état de l'art et non-vulnérable, et garantir l'authentification des services d'extrémité, ainsi que le chiffrement et le contrôle d'intégrité des flux. La mise en œuvre de ces technologies doit se conformer aux règles et recommandations du RGS [RGS-A1] et [RGS-B2] et aux recommandations de sécurité relatives à TLS [RECOTLS] publiées par l'ANSSI (quand applicables)
[DT8]	Toute session ayant provoqué une erreur interne de l'application web doit être automatiquement fermée.
[DT9]	L'application doit déconnecter automatiquement tout utilisateur dont la session authentifiée est inactive. La durée d'inactivité prise en compte doit être paramétrable par un administrateur de l'application placé sous l'autorité du Responsable.
[DT10]	Lors de la déconnexion d'un utilisateur, l'application web doit, autant que possible (notamment si le côté « client » de l'application, sur le navigateur de l'utilisateur, est toujours actif) provoquer l'effacement des données résiduelles dans le terminal et le navigateur de l'utilisateur. De manière générale, l'application doit être conçue pour que les données liées à la session dans l'environnement utilisateur soient supprimées par le navigateur à la fermeture de la session, de la page web ou du navigateur.
[DT11]	L'application doit intégrer une aide destinée à faciliter son utilisation sûre, c'est-à-dire qui minimise les risques d'erreur ou d'incompréhension dans les actions effectuées par l'utilisateur. L'ergonomie de l'application doit viser le même objectif.
[DT12]	Il est recommandé que l'architecture de la plate-forme applicative prévoie un dispositif de sécurité applicative, de type reverse-proxy ou pare-feu applicatif, en frontal de l'application, afin de ne pas laisser l'application en

[8] Dans le cas du stockage des données dans des fichiers d'un système de fichiers « simple », la seule suppression de fichier laisse généralement les données elles-mêmes inchangées sur le support physique (bien qu'elles n'apparaissent plus directement pour un utilisateur non expert). Ce mécanisme élémentaire n'est donc pas suffisant à l'effacement des données au sens de la règle.

N°	Règle
	communication directe avec Internet au niveau applicatif, et d'être en mesure de bloquer en amont de multiples attaques génériques, et le cas échéant spécifiques, contre l'application.
[DT13]	L'application web doit être conçue pour fonctionner même si l'utilisateur y accède via un ou plusieurs proxy HTTP.

4.2.4. Traces

N°	Règle
[TR1]	En vue du contrôle de la conformité des traitements et du traitement d'incidents de sécurité, l'application doit comporter une fonction d'enregistrement des événements relatifs à la sécurité des services offerts et de leur utilisation. Elle doit au minimum conserver les traces : ► Des ouvertures et des fermetures des services ; ► Des ouvertures et des fermetures des sessions authentifiées d'utilisateurs ; ► Des refus d'accès et des anomalies d'utilisation ou de fonctionnement ; ► Des dépôts et des accès en lecture aux données à caractère personnel, de santé ou non ; ► Des accès en modification ou en suppression à ces données.
[TR2]	Chaque trace doit comporter au minimum : ► La date et l'heure précise de l'événement ; ► Le type de l'événement ; ► Les informations permettant de déterminer l'auteur de l'événement ; ► L'adresse IP du terminal utilisé. Il convient de noter que l'adresse IP du terminal de l'utilisateur doit parfois être obtenue via les entêtes du protocole HTTP plutôt qu'au niveau de la connexion IP à l'application. C'est par exemple le cas quand un « reverse-proxy » est utilisé en frontal de l'application web. Il convient alors d'utiliser la valeur de l'entête HTTP « REMOTE_ADDR » ou « HTTP_X_FORWARDED_FOR » (ou autre selon la configuration du reverse proxy) ajoutée à la requête par le reverse proxy, à la condition toutefois que cet équipement intermédiaire soit « de confiance »[9].
[TR3]	L'application doit permettre au personnel autorisé et à lui seul, placé sous l'autorité du Responsable, de paramétrer les types d'événements à enregistrer, les données constitutives des enregistrements (en respectant les données minimales identifiées dans la règle TR2) et la durée de rétention des enregistrements (et donc le délai d'effacement des traces) conformément à la politique de gestion des traces pour l'application concernée. Afin d'éviter un cumul de rôles préjudiciable à la qualité du système de traces, il est recommandé que ce personnel ne soit pas utilisateur de l'application concernée, ou au moins qu'il ne dispose d'aucun rôle privilégié ou sensible (administrateur de l'application, administrateur système, …). De manière plus générale, des dispositions doivent être prises pour garantir que les traces ne peuvent pas être modifiées de quelque manière que ce soit pendant toute leur durée de conservation, afin qu'elles puissent être utilisées en cas d'investigation, notamment judiciaire. Ces dispositions dépendent des enjeux spécifiques liés aux services en ligne offerts par l'application web considérée. Elles doivent également prendre en compte l'impact potentiel de la génération de traces sur les performances de l'application. Un compromis doit être recherché entre la réponse aux exigences de traces et la réponse aux exigences de performance.

[9] Ces entêtes HTTP, s'ils étaient issus d'une source non fiable, pourraient être utilisés pour faire enregistrer dans les traces une adresse IP falsifiée au lieu de l'adresse réelle.

N°	Règle
	Pour plus d'information sur les traces, se reporter au Guide pratique technique « Imputabilité » [GIMPU] du corpus documentaire de la PGSSI-S.

4.3. Hébergement et à l'exploitation de l'application

N°	Règle
[HE1]	L'hébergement de l'application web doit être réalisé conformément aux dispositions des articles L1111-8 [CSP-L1111-8] et R1111-8-8 [CSP-R1111-8-8] du code de la santé publique. Lorsque le Responsable fait appel, dans le cadre des articles mentionné ci-dessus, à un tiers[10] pour réaliser des activités d'hébergement de données de santé (HDS) telles que définies par l'article R1111-9 [CSP-R1111-9_11] du code de la santé publique, au bénéfice de l'application web, cet hébergeur doit être certifié ou agréé pour ces activités selon les modalités fixées par les articles L1111-8, R1111-10 et R1111-11 [CSP-R1111-9_11] du code de la santé publique.
[HE2]	L'application en production doit bénéficier d'un environnement de sécurité physique, technique et organisationnel conforme aux règles de l'art et capable de la protéger notamment contre : ► Les tentatives d'intrusion ou d'accès physique ou logique par des personnes non autorisées ; ► Les attaques logiques en provenance des réseaux ; ► Les codes malveillants.
[HE3]	L'environnement d'hébergement de l'application web doit intégrer un dispositif de filtrage au niveau réseau (pare-feu) aussi bien vis-à-vis d'Internet que du reste du SIS.
[HE4]	L'environnement d'hébergement de l'application web en production doit être réservé à la production et exclure tout partage logique ou physique avec des applications en préproduction, recette ou développement, ainsi qu'avec toute application ne présentant pas le même niveau d'enjeu de sécurité et le même niveau de sécurisation.
[HE5]	L'environnement d'hébergement de l'application web en production doit être distinct des environnements de production des autres services internes du SIS.
[HE6]	Les dispositions de sécurité de l'application et de sa plateforme d'hébergement doivent encadrer les accès des personnels chargés de son maintien en condition opérationnelle (exploitant, administrateur, agent de maintenance, agent d'entretien, etc…) afin de limiter l'accès aux données de santé de l'application à ce qui est strictement nécessaire pour l'exécution des missions des personnels précités. En outre, ces accès doivent être réalisés sous le contrôle et la responsabilité du Responsable de l'hébergeur lorsque l'application est hébergée par un hébergeur certifié ou agréé à cet effet.
[HE7]	Tous les accès d'exploitation à l'application doivent être répertoriés, contrôlés et limités au strict nécessaire. Les autres possibilités d'accès par le personnel chargé du maintien en condition opérationnelle doivent être neutralisées, et si nécessaire doivent pouvoir être ouvertes en cas de besoin pour une durée limitée dans le cadre d'un processus maîtrisé, sous le contrôle du Responsable.
[HE8]	Il est fortement recommandé que tous les accès logiques donnant aux exploitants ou aux administrateurs la possibilité de lire ou de modifier des données de santé, et plus généralement des données à caractère personnel, même de façon fortuite, soient soumis à une procédure d'identification individuelle et d'authentification forte (à deux facteurs). Les cas où ces principes ne peuvent pas être respectés doivent être identifiés, documentés et justifiés.

[10] Au sens général, hors définition spécifique à ce guide

N°	Règle
	Les accès doivent être tracés et ces traces ne doivent être exploitables que par le personnel en charge du contrôle de la conformité du traitement.
[HE9]	L'application doit faire l'objet d'une surveillance de la sécurité de son fonctionnement selon les règles de l'art, notamment par la mise en place de sondes de détection d'intrusion avec, quand l'analyse de risque permet de conclure que c'est pertinent, des règles de blocage selon les types d'attaques ou de comportements détectés. La mise en œuvre de blocage automatique doit être décidée en tenant compte du fait que cette disposition peut être exploitée par des personnes malveillantes afin de porter atteinte à la disponibilité du système. Elle résulte donc généralement du choix de privilégier la protection des données et traitements contre des accès illégitimes au dépend de la continuité des accès légitimes à ces données et traitement.

Annexe 1 : Documents de référence

Réglementation

Renvoi	Document
[CSP-L1111-8]	Article L1111-8 du code de la santé publique, modifié par l'ordonnance n°2017-27 du 12 janvier 2017 - art. 1. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549/
[CSP-L1111-8-1]	Article L1111-8-1 du code de la santé publique, modifié par la loi n°2020-1525 du 7 décembre 2020 - art. 90. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042661590
[CSP-L1470]	Articles L. 1470-1 à 1470-5 du code de la santé publique (issus de l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043496464
[CSP-R1111-8-8]	Article R1111-8-8 du code de la santé publique, créé par le décret n°2018-137 du 26 février 2018 - art. 2 « Dispositions générales relatives à l'hébergement de données de santé à caractère personnel » https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000036656497/
[CSP-R1111-9_11]	Articles R1111-9 à R1111-11 du code de la santé publique, modifiés par le décret n°2018-137 du 26 février 2018 - art. 2 « Hébergement des données de santé à caractère personnel sur support numérique soumis à certification » https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006196138/
[IE-ASPM]	Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes morales] Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[IE-ASPP]	Référentiel d'identification électronique des acteurs des secteurs sanitaire, médico-social et social [personnes physiques] Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[IE-CA]	Référentiel de contrôle d'accès Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[IE-Usagers]	Référentiel d'identification électronique des usagers Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[GIMPU]	Guide pratique technique « Imputabilité » *(Précédemment nommé « Référentiel d'imputabilité »)* Disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

[L78-17]	Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, dite « loi informatique et libertés »
[PSSI-MCAS]	PSSI – MCAS : Politique de Sécurité des Systèmes d'Information pour les Ministère Chargés des Affaires Sociales https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031386468
[PSSIE]	PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat (ANSSI). https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (« règlement général sur la protection des données »), relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE et Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
[RGS]	Référentiel Général de Sécurité - Version 2.0 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[RGS-A1]	RGS A1 - Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[RGS-B1]	RGS B1 - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[RGS-B2]	RGS B2 - Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

Documents techniques

Renvoi	Document
[ANSSI-MDP]	Recommandations relatives à l'authentification multifacteur et aux mots de passe - V2.0 – octobre 2021 - Guide ANSSI https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
[CNIL-MDP]	Authentification par mot de passe : les mesures de sécurité élémentaires (CNIL) https://www.cnil.fr/fr/mot-de-passe

[CRYPTO]	Guide des mécanismes cryptographiques, version 2.04 du 01/01/2020 ou version ultérieure en vigueur, publié par l'ANSSI https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[CRYPTOSEL]	Guide de sélection d'algorithmes cryptographiques, version 1.0 du 08/03/2021 ou version ultérieure en vigueur, publié par l'ANSSI https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[EBIOS RM]	EBIOS Risk Manager https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/#
[ENGAGEMENT]	Modèles d'engagement de conformité aux référentiels d'identification électronique dans les secteurs sanitaire, médico-social et social de la PGSSI-S, disponibles conjointement à chaque référentiel d'identification électronique [IE-ASPM], [IE-ASPP] et [IE-Usagers]. https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[GDD]	Guide pratique technique « Destruction des données lors du transfert de matériel informatique », disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[GDEVCNIL]	Guide RGPD de l'équipe de développement (CNIL) https://www.cnil.fr/fr/la-cnil-publie-une-nouvelle-version-de-son-guide-rgpd-pour-lequipe-de-developpement https://lincnil.github.io/Guide-RGPD-du-developpeur/
[GMPIDS]	Guide pratique technique « Mécanismes de protection de l'intégrité des données stockées », disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[GRIAD]	Guide Pratique technique « Règles pour les interventions à distance sur les Systèmes d'Information de Santé », disponible dans le corpus documentaire de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[HOMOLOGATION]	Démarche d'homologation de sécurité https://www.ssi.gouv.fr/entreprise/management-du-risque/homologation-de-securite/
[OWASP]	Les dix vulnérabilités de sécurité applicatives web les plus critiques (mise à jour annuelle) – OWASP https://owasp.org/www-project-top-ten/
[PGSSI-S]	Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s Corpus documentaire de la Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[RECOTLS]	Recommandations de sécurité relatives à TLS – V1.2 – mars 2020 - ANSSI https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/

[RECOWEB]	Recommandations pour la mise en œuvre d'un site web : Maîtriser les standards de sécurité côté navigateur - V2.0 - avril 2021 - Guide ANSSI https://www.ssi.gouv.fr/guide/recommandations-pour-la-securisation-des-sites-web/

Annexe 2 : Glossaire

Sigle / Acronyme	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANS	Agence du Numérique en Santé
CPS	Carte de Professionnel de Santé
DMP	Dossier Médical Personnel
ES	Etablissements de santé
HDS	Hébergeur de Données de Santé
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure : protocole de transfert hypertexte sécurisé
OWASP	Open Web Application Security Project
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PS	Professionnel de Santé
RGS	Référentiel Général de Sécurité
SI	Système d'Information
SIS	Système d'Information de Santé
URL	Uniform Resource Locator, (peut être traduit par adresse réticulaire ou adresse universelle, selon le JO du 16/03/1999)
W3C	World Wide Web Consortium