8.2 Annexe : Exigences SSI/RGPD de l'ATIH

Exigences de sécurité des systèmes d'information et de protection des données applicables aux activités réalisées par l'ATIH ou pour son compte par un prestataire
Version du 06/10/2026
Contact : security@atih.sante.fr ou donneespersonnelles@atih.sante.fr
Ce document a été élaboré avec l'assistance d'une solution d'intelligence artificielle. Son contenu a été vérifié et validé par l'ATIH.

Table des matières

1 Objet 1
2 Les réflexes essentiels 4
3 Socle général d'exigences 7
4 Exigences spécifiques selon la nature des activités 9
4.1 Traitements de données à caractère personnel 9
4.2 Traitements statistiques de données de santé à caractère personnel 11
4.3 Activités informatiques de développement et de maintenance 11
4.4 Activités informatiques relatives aux infrastructures et réseaux 14
4.5 Assurance qualité, tests et assistance utilisateur 15
4.6 Usage de l'IA 16

1 Objet

Le présent document définit les exigences minimales de sécurité des systèmes d'information et de protection des données applicables aux activités réalisées par l'ATIH ou pour son compte par un **organisme prestataire**, notamment aux activités de développement, de maintenance, d'exploitation, d'assistance, ainsi qu'aux activités impliquant un traitement de données à caractère personnel, notamment des données de santé.

Toute personne ou entité participant à ces activités met en œuvre les mesures techniques et organisationnelles appropriées pour préserver la confidentialité, l'intégrité, la disponibilité et la traçabilité des systèmes, services et données concernés, dans le respect des exigences SSI et RGPD applicables.

Les présentes exigences s'appliquent à toute activité réalisée par l'ATIH ou pour son compte par un **organisme prestataire**, qu'elle soit réalisée par des agents de l'ATIH, des intervenants d'un

organisme prestataire ou toute autre personne autorisée à intervenir sur les systèmes, services ou données concernés.

Dans le présent document, le terme « **chacun** » désigne toute personne physique intervenant dans le cadre des activités concernées, qu'elle soit agent de l'ATIH, intervenant d'un **organisme prestataire** ou toute autre personne autorisée. « **La ligne encadrante de l'ATIH** » désigne la ou les personnes de l'ATIH responsables de l'activité concernée et disposant du pouvoir de décision nécessaire à son organisation et à son pilotage.

Lorsqu'une exigence ne concerne que les **organismes prestataires**, ou lorsqu'elle vise un sous-traitant au sens du RGPD, cela est explicitement indiqué.

Les présentes exigences constituent un socle minimal applicable par défaut. Toute dérogation, adaptation, précision ou exigence complémentaire décidée par l'ATIH est formalisée dans les documents contractuels applicables, dans une instruction documentée ou dans tout autre support validé par l'ATIH. Lorsqu'il s'agit d'une dérogation, cette formalisation intervient préalablement à sa mise en œuvre.

Lorsqu'une dérogation conduit à réduire le niveau de protection prévu par le présent document, ses impacts SSI et RGPD sont préalablement analysés avec l'appui des fonctions compétentes. Lorsque cela est possible, des mesures compensatoires sont définies.

Repères de lecture

Le délégué à la protection des données (DPO) accompagne l'ATIH dans l'application du RGPD. **Le responsable de la sécurité des systèmes d'information (RSSI)** accompagne l'ATIH dans la définition et la mise en œuvre des mesures de sécurité.

La **sécurité des systèmes d'information** (SSI) vise à préserver la **confidentialité**, l'**intégrité**, la **disponibilité** et la **traçabilité** des systèmes, services et données. Ces objectifs consistent notamment à éviter les accès non autorisés, les modifications non maîtrisées, les indisponibilités injustifiées et l'absence de traces permettant de comprendre les actions réalisées.

Une **donnée à caractère personnel** est toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (nom et prénom, adresse électronique, identifiant, photo, combinaison d'informations permettant d'identifier indirectement une personne, etc.).

Un **traitement** désigne toute opération portant sur des données à caractère personnel, notamment la collecte, la consultation, l'utilisation, la conservation, la transmission, l'extraction, l'effacement ou la destruction.
Exemples de traitements : traitement statistique de données PMSI, consultation d'un fichier contenant des dossiers du personnel, gestion d'inscriptions à un événement, enquête de satisfaction, gestion d'une base de données comportant des identifiants ou traces d'activité etc.

Certaines données à caractère personnel relèvent de catégories particulières au sens du RGPD, souvent appelées **données sensibles**. C'est notamment le cas des **données de santé à caractère personnel**. Leur traitement est soumis à **des conditions renforcées** et doit respecter les exigences fixées par la réglementation applicable et par l'ATIH.

Une **violation de données** à caractère personnel correspond à un incident de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données à caractère personnel.

Une **donnée de santé à caractère personnel** est une donnée relative à la santé physique ou mentale d'une personne, ou révélant des informations sur son état de santé.

Le **responsable de traitement** détermine les finalités et les moyens essentiels du traitement.

Le **sous-traitant au sens du RGPD** traite des données à caractère personnel pour le compte du responsable de traitement, sur ses instructions.

Le principe du besoin d'en connaître signifie qu'une personne ne consulte que les informations nécessaires à l'exercice de sa mission, même lorsqu'elle dispose techniquement d'un accès plus large.

Le principe du moindre privilège consiste à attribuer uniquement les droits techniques nécessaires à l'exercice de la mission, pour la durée nécessaire.

2 Les réflexes essentiels

Le présent document constitue le référentiel détaillé des exigences applicables.

Les réflexes suivants en résument les règles essentielles que **chacun** doit respecter dans son périmètre d'intervention :

- **Je protège mes accès** : utiliser exclusivement son compte nominatif et protéger ses moyens d'authentification ;
- **J'accède seulement à ce dont j'ai besoin** : n'accéder qu'aux informations strictement nécessaires à ses missions ;
- **Je ne transmets que le strict nécessaire** : ne transmettre que les informations nécessaires à l'exercice de ses missions, aux seuls destinataires autorisés et par des moyens appropriés ;
- **Au moindre doute, je signale** : signaler sans délai toute difficulté, anomalie, incident ou suspicion d'incident à son responsable (ou référent ATIH pour un prestataire), ainsi qu'aux interlocuteurs compétents selon la nature de la situation : équipe chargée de la sécurité du système d'information (security@atih.sante.fr) ou délégué à la protection des données (donneespersonnelles@atih.sante.fr) ;
- **Avec l'IA, je respecte les règles et je vérifie toujours** : n'utiliser une solution d'intelligence artificielle que dans les conditions autorisées par l'ATIH et vérifier systématiquement ses productions ;
- **Je n'utilise pas d'équipement personnel pour capter ou traiter des informations professionnelles :** ne pas utiliser de lunettes connectées ni tout autre équipement personnel pour capter, enregistrer, analyser, traiter ou transmettre des informations relatives aux activités de l'ATIH ou aux personnes agissant pour son compte ou participant à ses activités, sauf nécessité professionnelle dûment justifiée
- **Je reconnais et protège les informations sensibles** : savoir reconnaître les informations sensibles ou confidentielles et les protéger de manière appropriée.

Des supports pédagogiques et une auto-évaluation permettent d'approfondir ces règles selon les activités et responsabilités exercées.

À retenir sur les informations sensibles ou confidentielles

Une information sensible ou confidentielle est une information dont la divulgation, l'altération, la perte ou l'utilisation par une personne non autorisée pourrait porter atteinte à l'ATIH, à ses partenaires, aux personnes concernées ou à la sécurité du système d'information.

Il s'agit notamment :

- des **données de santé à caractère personnel** et, plus largement, des données à caractère personnel nécessitant une protection particulière ;

- des **informations contractuelles, économiques, financières, stratégiques ou organisationnelles non publiques** ;
- des **informations relatives à la sécurité des systèmes d'information** : vulnérabilités, incidents, mesures de sécurité, configurations, architectures, etc. ;
- des **secrets, mots de passe, clés, certificats, jetons et autres moyens d'authentification** ;
- des **configurations ou informations techniques sensibles** permettant notamment d'accéder aux systèmes ou d'en compromettre la sécurité.

Ces informations doivent être **identifiées, utilisées, stockées et transmises uniquement lorsque cela est nécessaire**, dans le respect des règles de sécurité et des habilitations applicables. En cas de doute sur le caractère sensible ou confidentiel d'une information, il convient de **ne pas la transmettre et de demander conseil** à l'interlocuteur compétent.

Une information peut être considérée comme publique lorsqu'elle a été officiellement publiée ou rendue accessible au public par l'ATIH ou par une source autorisée, sans restriction particulière d'accès ou de réutilisation.

Par défaut, une information non publiée, en cours de préparation, reçue dans le cadre d'une mission, accessible uniquement en interne ou transmise dans un cadre contractuel ou partenarial n'est pas une information publique.

En cas de doute, elle doit être traitée comme une information interne, sensible ou confidentielle selon son contenu.

Le fait qu'une information soit largement connue en interne, accessible dans un outil de travail ou partagée avec plusieurs destinataires ne suffit pas à la rendre publique.

Vigilance particulière concernant les données de santé à caractère personnel

Les activités de l'ATIH impliquent fréquemment l'accès à des données de santé à caractère personnel.

Chacun ne doit **jamais chercher à identifier ou réidentifier les personnes concernées**, **ni exporter, transmettre ou réutiliser des données sans y être autorisé**. Tout accès, toute consultation et tout traitement doivent être strictement limités aux besoins des missions confiées et réalisés dans le respect des habilitations et consignes applicables.

Lorsque l'activité est réalisée dans un environnement homologué permettant le traitement de données de santé à caractère personnel, les engagements individuels, conditions d'utilisation et règles particulières applicables à cet environnement doivent également être respectés.

À retenir sur l'usage de l'intelligence artificielle

- **Une « IA maîtrisée »** est une solution autorisée par l'ATIH ou, pour un organisme prestataire, une solution dont le respect des garanties attendues peut être justifié auprès de l'ATIH, notamment en matière de sécurité, de confidentialité, de non-réutilisation des contenus, de conservation, de localisation et de sous-traitance.
- 🌐 **Dans une IA grand public ou non maîtrisée :** uniquement des contenus publics, strictement fictifs ou anonymisés sans ambiguïté. Un contenu est anonymisé uniquement lorsqu'aucune personne ne peut être identifiée ou réidentifiée, directement ou indirectement, y compris par recoupement avec d'autres informations raisonnablement disponibles.
- 🔐 **Dans une IA maîtrisée, qu'elle soit cloud, locale ou interne :** les contenus nécessaires à l'activité peuvent être transmis, sous réserve de respecter les finalités prévues, le principe de minimisation, les instructions applicables et les deux interdictions rappelées ci-dessous.
- 🚫 **Même dans une IA maîtrisée**, sauf autorisation expresse préalable de l'ATIH dans un cadre documenté : **ne pas transmettre de données de santé à caractère personnel, y compris lorsqu'elles sont pseudonymisées, ni d'informations ou éléments techniques dont la divulgation pourrait permettre l'accès à un système d'information de l'ATIH.**
- ⚠️ **Dans tous les cas :** transmettre uniquement les éléments strictement nécessaires à l'objectif poursuivi, vérifier la réponse produite, respecter les instructions applicables et ne rien transmettre en cas de doute.

3 Socle général d'exigences

Toute activité réalisée par l'ATIH ou pour son compte par un **organisme prestataire** est conçue, organisée et réalisée de manière à intégrer la sécurité des systèmes d'information et la protection des données dès l'origine et pendant toute sa durée de mise en œuvre, selon une approche adaptée à la nature de l'activité, aux risques identifiés et à la sensibilité des données traitées.

La ligne encadrante de l'ATIH veille, pour les activités placées sous sa responsabilité, à ce que les exigences SSI et RGPD applicables soient identifiées, prises en compte dès la définition du besoin, mises en œuvre, suivies et, lorsque nécessaire, réévaluées avec l'appui du RSSI, du DPO et des fonctions compétentes.

La ligne encadrante de l'ATIH, ainsi que l'**organisme prestataire** lorsqu'une activité lui est confiée, veillent notamment à mettre en œuvre et maintenir :

- une limitation des accès aux seules personnes habilitées, selon le principe du besoin d'en connaître et du moindre privilège ;
- des mesures d'authentification et, lorsque cela est justifié, d'authentification renforcée pour les accès sensibles ou d'administration ;
- une gestion des habilitations, des comptes et des accès à privilèges, incluant leur révision et leur retrait lorsqu'ils ne sont plus nécessaires ;
- des mesures de journalisation, de traçabilité et de conservation des événements pertinents de sécurité et d'accès aux données, dans le respect du principe de proportionnalité ;
- des mesures de cloisonnement, de sécurisation des postes, des équipements, des environnements, des flux et des supports ;
- des mesures de sauvegarde, de restauration, de mise à jour, de correction des vulnérabilités et, plus généralement, de maintien en condition de sécurité ;
- la sensibilisation et, lorsque nécessaire, la formation des personnes concernées ;
- une organisation permettant de détecter, signaler, analyser et traiter les incidents de sécurité ou de protection des données ;
- une organisation permettant de s'assurer que les personnes ou entités intervenant sous leur responsabilité ou pour leur compte connaissent et respectent les présentes exigences et, lorsque cela est nécessaire ou demandé par l'ATIH, formalisent l'engagement individuel adapté auprès des intervenants concernés.

Chacun, dans son périmètre d'intervention, respecte les exigences suivantes :

- disposer d'un compte utilisateur unique, individuel, nominatif et incessible ;
- lorsqu'une adresse de courriel est requise, utiliser une adresse de courriel professionnelle valide indiquée dans son compte ;
- disposer uniquement des habilitations strictement nécessaires à l'exercice de ses missions ;
- utiliser les systèmes, services, environnements, données et habilitations auxquels il a accès uniquement pour les besoins des missions qui lui sont confiées et dans le respect des finalités, habilitations, consignes et instructions applicables ;

- signaler sans délai tout départ, changement de fonction, fin de mission ou perte de besoin d'accès afin de permettre le retrait des habilitations, la désactivation des comptes et, le cas échéant, la restitution des moyens d'accès ;
- signaler sans délai toute difficulté, anomalie, incident ou suspicion d'incident à son responsable (ou référent ATIH pour un prestataire), ainsi qu'aux interlocuteurs compétents selon la nature de la situation : équipe chargée de la sécurité du système d'information (security@atih.sante.fr) ou délégué à la protection des données (donneespersonnelles@atih.sante.fr) ;
- respecter les obligations de confidentialité et de discrétion, y compris après la fin de l'activité, de la mission ou de la prestation. La fin de l'intervention ou la suppression des accès n'autorise ni la divulgation ni la réutilisation ultérieure des informations dont une personne a eu connaissance dans le cadre de son activité. Ceci concerne toute information non publique, qu'elle soit technique, opérationnelle ou à caractère personnel.

L'utilisation de lunettes connectées est interdite dans les locaux de l'ATIH et pendant toute activité réalisée pour le compte de l'ATIH, y compris en télétravail. Cette interdiction s'applique à **chacun**. Sauf nécessité professionnelle dûment justifiée, **aucun équipement personnel ne doit être utilisé** pour capter, enregistrer, analyser, traiter ou transmettre des informations (images, sons, vidéos, documents, données, etc.) relatives aux activités de l'ATIH ou aux personnes agissant pour son compte ou participant à ses activités.

Ces exigences générales s'appliquent même lorsque des exigences particulières n'ont pas été définies pour une activité donnée.

Elles constituent un socle minimal auquel s'ajoutent, le cas échéant, les exigences spécifiques fixées par l'ATIH, par la réglementation applicable, par les documents contractuels, par les instructions documentées ou par la prestation concernée.

Lorsqu'un **organisme prestataire** fait appel à un sous-traitant, cotraitant, consultant, collaborateur externe ou tout autre intervenant pour réaliser tout ou partie de l'activité confiée, il s'assure que les présentes exigences, ainsi que les exigences complémentaires applicables, lui sont opposables et effectivement respectées. L'**organisme prestataire** demeure responsable, à l'égard de l'ATIH, du respect de ces exigences par les personnes ou entités intervenant sous sa responsabilité ou pour son compte.

La ligne encadrante de l'ATIH, l'**organisme prestataire** lorsqu'une activité lui est confiée, et **chacun** dans son périmètre d'intervention, veillent au respect de ces exigences complémentaires.

4 Exigences spécifiques selon la nature des activités

Le socle général défini à la section 3 s'applique à toutes les activités. Les sections spécifiques ci-dessous ajoutent ou précisent les exigences applicables selon la nature de l'activité. Lorsqu'une activité relève de plusieurs sections, les exigences correspondantes se cumulent.

4.1 Traitements de données à caractère personnel

Lorsqu'une activité réalisée par l'ATIH ou pour son compte par un **organisme prestataire** implique un traitement de données à caractère personnel, y compris de données de santé à caractère personnel, les personnes ou entités concernées mettent en œuvre des mesures renforcées de protection adaptées à la sensibilité de ces données, aux finalités poursuivies, aux durées de conservation applicables et au risque pour les personnes concernées.

Pour tout nouveau traitement de données à caractère personnel ou toute évolution substantielle d'un traitement existant, **la ligne encadrante de l'ATIH** veille à associer le délégué à la protection des données suffisamment en amont afin de déterminer les actions à conduire avant la mise en œuvre ou l'évolution du traitement.

Chacun, lorsqu'il traite des données à caractère personnel, veille notamment à :

- ne traiter que les données strictement nécessaires aux missions confiées, dans le cadre des finalités autorisées, en respectant les durées de conservation, les règles de sécurité et les instructions applicables ;
- limiter les accès, consultations, extractions, copies et transmissions aux seuls besoins justifiés par l'activité réalisée ;
- ne pas conserver de copies non autorisées de données à caractère personnel au-delà de ce qui est nécessaire aux activités confiées ou aux obligations légales, réglementaires ou contractuelles applicables ;
- respecter les obligations de confidentialité, de discrétion et, lorsque les conditions légales sont réunies, de secret professionnel qui lui sont applicables, notamment dans les conditions prévues à l'article 226-13 du Code pénal ;
- assurer la sécurité, la confidentialité et la traçabilité des données, en prenant toutes les précautions utiles pour prévenir toute perte, altération, divulgation non autorisée ou accès non autorisé ;
- éviter l'utilisation de données réelles lorsqu'elle n'est pas strictement nécessaire, notamment dans les environnements de développement, de test, de démonstration, d'analyse, de support ou d'assistance ;
- ne transférer des données à caractère personnel hors de l'Union européenne que dans un cadre autorisé, conformément au RGPD, aux instructions applicables et, le cas échéant, aux exigences fixées par l'ATIH ;

- transmettre sans délai au DPO ou à l'interlocuteur désigné par l'ATIH toute demande d'exercice de droits reçue d'une personne concernée, sans y répondre directement sauf instruction ou procédure applicable ;
- alerter sans délai le responsable de la sécurité du système d'information (RSSI) ou le délégué à la protection des données (DPO) en cas de problème avéré ou potentiel de sécurité ou de protection des données, avec les informations disponibles permettant d'en apprécier la nature, les données concernées, les conséquences probables et les mesures prises ou proposées.

Les personnes intervenant dans le cadre d'activités réalisées par l'ATIH ou pour son compte sont informées des traitements de données à caractère personnel les concernant dans l'information RGPD mise à disposition par l'ATIH, disponible sur l'intranet et sur demande auprès de donneespersonnelles@atih.sante.fr. Cette information précise notamment les finalités des traitements concernés, les durées de conservation applicables et les modalités d'exercice des droits.

La ligne encadrante de l'ATIH, ainsi que l'**organisme prestataire** lorsqu'une activité lui est confiée, veillent également à :

- s'assurer que les personnes intervenant sous leur responsabilité ou pour leur compte respectent les présentes exigences et disposent des habilitations, consignes et moyens nécessaires à leur application ;
- coopérer avec l'ATIH pour l'analyse des risques, la gestion des incidents, la mise en œuvre de mesures correctives, la réponse aux demandes relatives aux droits des personnes concernées et, le cas échéant, la réalisation ou l'actualisation d'une analyse d'impact relative à la protection des données ;
- mettre à disposition les éléments nécessaires pour démontrer le respect des présentes exigences et coopérer aux contrôles, audits ou vérifications raisonnablement demandés ou réalisés sous l'autorité de l'ATIH ;
- restituer, supprimer ou archiver les données à caractère personnel, les copies et les supports qui en contiennent à la fin de l'activité, dans les conditions et délais définis par les instructions de l'ATIH, les documents contractuels et les obligations légales ou réglementaires applicables.

Lorsqu'un organisme prestataire agit en qualité de sous-traitant au sens du RGPD, les données à caractère personnel qu'il traite pour le compte de l'ATIH ainsi que les copies qui en sont issues sont supprimées au terme de la prestation, sauf instruction documentée de restitution ou d'archivage donnée par l'ATIH ou obligation légale contraire.

Lorsqu'un organisme prestataire traite des données à caractère personnel pour le compte de l'ATIH, il agit en qualité de sous-traitant au sens du RGPD, sauf qualification différente expressément prévue dans les documents applicables. Dans ce cas, les présentes exigences constituent les clauses RGPD applicables par défaut à la prestation, en complément des documents contractuels, du cahier des charges, du marché, du bon de commande, de la convention ou de toute instruction documentée de l'ATIH. En cas de contradiction, les clauses particulières validées par l'ATIH prévalent.

4.2 Traitements statistiques de données de santé à caractère personnel

Les activités de traitement statistique portant sur les données PMSI relèvent d'un cadre de sécurité renforcé, notamment en raison de leur rattachement au système national des données de santé (SNDS). Par choix de protection, l'ATIH applique également des exigences équivalentes à toute activité de traitement statistique portant sur des données de santé à caractère personnel, notamment les données ENC, les données médico-sociales ou toute autre donnée de santé traitée par l'ATIH ou pour son compte par un **organisme prestataire**.

Chacun, pour ces traitements statistiques de données de santé, veille notamment à :

- traiter les données uniquement dans un **environnement homologué** conformément au référentiel de sécurité applicable au Système national des données de santé (SNDS) ;
- n'exporter de l'environnement concerné que des **données anonymes**, sous la forme de statistiques agrégées ne permettant pas d'identifier directement ou indirectement les personnes concernées, ou des données chiffrées selon les modalités validées par l'ATIH et, le cas échéant, prévues par la convention de constitution d'un système fils ;
- **ne pas traiter les données à des fins de réidentification**, notamment par rapprochement, interconnexion, mise en relation ou appariement avec des fichiers ou informations directement ou indirectement nominatives ou susceptibles de révéler l'identité d'une personne ou son état de santé ;
- **ne pas poursuivre les finalités interdites applicables au SNDS** lorsque les données relèvent de ce cadre, notamment la promotion des produits de santé en direction des professionnels de santé ou des établissements de santé, ainsi que l'exclusion de garanties des contrats d'assurance ou la modification de cotisations ou de primes d'assurance pour un individu ou un groupe d'individus ;
- respecter les règles de sécurité, de confidentialité, de traçabilité et de contrôle des accès prévues par **le référentiel de sécurité applicable au SNDS**.

La ligne encadrante de l'ATIH, ainsi que l'**organisme prestataire** lorsqu'une activité lui est confiée, **attestent que les personnes intervenant sous leur responsabilité s'engagent individuellement**, par contrat ou par tout autre acte juridique approprié, à respecter les **conditions générales d'utilisation du SNDS** précisées dans le référentiel de sécurité applicable au SNDS.

Pour les environnements homologués permettant le traitement de données de santé à caractère personnel, l'ATIH peut également conditionner l'accès :

- à la prise de connaissance des conditions générales d'utilisation du SNDS applicables ;
- à l'engagement de l'utilisateur à les respecter, matérialisé par une case à cocher accompagnée du texte applicable, ou par un mécanisme équivalent.

4.3 Activités informatiques de développement et de maintenance

Chacun, lorsqu'il intervient dans des activités informatiques de développement, de maintenance, de test, de diagnostic, de preuve de concept ou d'assistance, applique les exigences de sécurité applicables à son périmètre d'intervention.

4.3.1 Répartition des responsabilités et devoir de conseil

Par principe, l'ATIH définit les exigences de sécurité applicables à l'application, notamment celles relatives à l'architecture, à l'authentification, au chiffrement et à la gestion des accès. Toutefois, lorsqu'une prestation prévoit que tout ou partie de ces exigences sont définies ou précisées par un **organisme prestataire**, celles-ci sont soumises à la validation de l'ATIH. Ces exigences s'appliquent aux activités réalisées en interne ainsi qu'à celles confiées à un **organisme prestataire**.

Chaque personne ou entité concernée est responsable, dans son périmètre, de la mise en œuvre correcte de ces exigences conformément aux bonnes pratiques de sécurité applicative. Lorsqu'une activité est confiée à un **organisme prestataire**, celui-ci est responsable de leur mise en œuvre correcte dans le cadre du développement et de la maintenance.

Au titre de son obligation de conseil, tout **organisme prestataire** intervenant pour le compte de l'ATIH conseille l'ATIH en matière de sécurité, l'alerte sur toute vulnérabilité potentielle, faiblesse de sécurité ou mauvaise pratique susceptible d'affecter la sécurité de l'application et formule les recommandations nécessaires pour améliorer la sécurité de la solution.

4.3.2 Développement sécurisé

Les activités de développement et de maintenance sont réalisées selon des pratiques de développement sécurisé tout au long du cycle de développement logiciel.

Ces pratiques comprennent notamment :

- la prévention des vulnérabilités applicatives décrites dans l'OWASP Top 10 ;
- l'utilisation d'outils d'analyse de sécurité du code et de ses dépendances permettant d'identifier les vulnérabilités.

Les vulnérabilités identifiées sont corrigées avant la livraison de chaque version de l'application, sauf acceptation ou traitement différent formalisé par l'ATIH.

4.3.3 Composants logiciels et SBOM

Les bibliothèques, frameworks et composants logiciels utilisés dans l'application font l'objet d'une gestion sécurisée.

À ce titre, **chacun**, dans son périmètre d'intervention, veille notamment à :

- maintenir un inventaire des composants logiciels utilisés ;
- surveiller les vulnérabilités affectant ces composants ;
- appliquer les mises à jour de sécurité nécessaires.

Lorsqu'une version applicative est livrée par un **organisme prestataire**, celui-ci fournit à l'ATIH un **Software Bill of Materials (SBOM)** pour chaque version livrée. Ce document recense les composants logiciels et bibliothèques utilisés ainsi que leurs versions.

Le SBOM est fourni dans un format standard interopérable, tel que *CycloneDX* ou *SPDX*, afin de permettre son exploitation par des outils de gestion des vulnérabilités.

4.3.4 Environnement de développement

Les mesures nécessaires sont mises en œuvre afin de sécuriser les environnements de développement et de prévenir toute compromission du code source ou de la chaîne de développement.

Ces mesures s'appuient notamment sur les recommandations du Guide d'hygiène informatique de l'ANSSI et comprennent en particulier :

- la gestion des accès aux dépôts de code source ;
- l'authentification forte pour les comptes disposant d'accès aux outils de développement ;
- la protection des environnements d'intégration et de déploiement continus (CI/CD) ;
- la protection des postes de travail des développeurs, des logiciels de développement et plugins utilisés ;
- la gestion sécurisée des secrets et des clés ;
- l'interdiction d'utiliser des données réelles issues des environnements de production, pour toute activité de développement, test, diagnostic, preuve de concept ou assistance par outils automatisés (y compris IA), sauf autorisation écrite préalable de l'ATIH et mise en place de mesures spécifiques définies par l'ATIH.

4.3.5 Vérifications de sécurité

Avant toute livraison de l'application, des analyses de sécurité sont réalisées afin d'identifier les vulnérabilités applicatives et celles affectant les dépendances logicielles.

Ces analyses portent sur l'ensemble du code applicatif, qu'il ait ou non fait l'objet de développements ou de modifications dans le cadre des activités concernées, ainsi que sur l'ensemble des composants logiciels, qu'ils aient ou non fait l'objet de développements ou de modifications dans ce cadre.

Lorsqu'elles sont réalisées par un **organisme prestataire**, celui-ci documente les outils et méthodes utilisés pour la détection des vulnérabilités et transmet à l'ATIH, sur demande ou lors des livraisons majeures, les rapports complets issus de ces analyses (y compris les vulnérabilités acceptées ou exclues par action manuelle).

Sauf accord contraire documenté de l'ATIH, les versions livrées de l'application ne doivent pas comporter de vulnérabilités connues présentant un niveau de sévérité **moyen, élevé ou critique** au

regard du standard **Common Vulnerability Scoring System (CVSS)**, tel que publié dans les bases publiques de vulnérabilités.

4.3.6 Documentation et audits

La documentation technique nécessaire à l'exploitation sécurisée de l'application est produite, comprenant notamment :

- l'architecture fonctionnelle et technique de la solution ;
- la liste des dépendances logicielles utilisées ;
- les recommandations de configuration sécurisée.

L'ATIH peut faire réaliser des audits de sécurité ou des tests d'intrusion avant mise en production. Les personnes ou entités concernées coopèrent pleinement et, lorsqu'une activité est confiée à un **organisme prestataire**, celui-ci met en œuvre les corrections nécessaires relevant de son périmètre.

4.3.7 Veille de sécurité et gestion des incidents

Pendant la durée de maintenance ou de garantie de l'application, une veille relative aux vulnérabilités affectant le code applicatif et les composants logiciels est assurée. Cette veille porte sur l'ensemble du code applicatif et des composants logiciels utilisés, qu'ils aient ou non fait l'objet de développements ou de modifications dans le cadre des activités concernées.

Lorsqu'une vulnérabilité de sécurité présentant un niveau de sévérité moyen, élevé ou critique au regard du standard **Common Vulnerability Scoring System (CVSS)** est identifiée, la personne ou l'entité concernée :

- informe l'ATIH dans les meilleurs délais ;
- propose les mesures correctives appropriées ;
- met en œuvre les correctifs nécessaires dans le cadre des activités de maintenance ou de correction relevant de son périmètre.

Tout **organisme prestataire** intervenant pour le compte de l'ATIH informe également l'ATIH dans les meilleurs délais de tout **incident de sécurité** susceptible d'affecter :

- le code source de l'application ;
- les environnements de développement ;
- la chaîne de développement ou de déploiement.

Chacun, dans son périmètre d'intervention, coopère avec l'ATIH afin de permettre l'analyse de l'incident et la mise en œuvre des mesures correctives nécessaires.

4.4 Activités informatiques relatives aux infrastructures et réseaux

Les activités réalisées sur des éléments d'infrastructure informatique ou de réseau comprennent notamment l'administration, la configuration, la personnalisation, l'automatisation, le scripting, le

paramétrage, le déploiement, la supervision, le maintien en condition opérationnelle ou de sécurité, ainsi que la gestion des flux, accès, comptes techniques, sauvegardes et composants associés.

Toutes ces activités sont soumises, lorsqu'elles sont applicables, aux exigences prévues pour les activités informatiques de développement et de maintenance à la section 4.3, notamment en matière de développement et de configuration sécurisés, de gestion des composants, de vérification de sécurité, de documentation, de veille et de gestion des incidents.

4.5 Assurance qualité, tests et assistance utilisateur

4.5.1 Outillage des activités d'assistance, de test et d'assurance qualité

Les activités d'assistance, de test et d'assurance qualité peuvent s'appuyer sur des outils, environnements, scripts, automatisations, configurations, paramétrages, jeux de tests, procédures, tableaux de suivi ou dispositifs de qualification et de traçabilité.

Lorsque ces activités impliquent la configuration, la personnalisation, l'automatisation, le scripting, le paramétrage, le développement ou la modification d'un outil, d'un environnement ou d'un composant technique, elles sont soumises, lorsqu'elles sont applicables, aux exigences prévues pour les activités informatiques de développement et de maintenance à la section 4.3, notamment en matière de développement et de configuration sécurisés, de gestion des composants, de vérification de sécurité, de documentation, de veille et de gestion des incidents.

4.5.2 Assistance utilisateur pouvant impliquer des données personnelles, en particulier de santé

Les activités d'assistance utilisateur font l'objet d'un encadrement spécifique en raison du risque de transmission de données à caractère personnel, en particulier de données de santé, ou d'informations techniques sensibles dans les tickets, pièces jointes, captures d'écran, exports applicatifs, fichiers issus de logiciels de recueil ou autres échanges avec le service d'assistance.

La ligne encadrante de l'ATIH définit les règles applicables aux activités d'assistance placées sous sa responsabilité : accès autorisés, niveaux d'assistance compétents, modalités de transmission sécurisée, règles de conservation et modalités de suppression des données reçues.

L'organisme prestataire, lorsqu'il intervient dans une activité d'assistance, applique les consignes de l'ATIH et s'assure que les personnes intervenant pour son compte respectent les exigences applicables. Il ne doit ni solliciter, ni copier, ni conserver, ni réutiliser de données personnelles, en particulier de données de santé, en dehors des instructions de l'ATIH.

Chacun, lorsqu'il assure une activité d'assistance, traite les demandes dans le strict périmètre nécessaire à leur qualification, leur suivi et leur résolution. Il limite les informations demandées à ce

qui est strictement nécessaire et privilégie, chaque fois que possible, l'utilisation d'éléments expurgés, anonymisés ou remplacés par des données fictives.

Chacun n'accède qu'aux informations nécessaires à son intervention, selon le principe du besoin d'en connaître et du moindre privilège. Dans ce cadre, **chacun** :

- **privilégie par défaut l'accès aux informations de suivi, aux statuts, aux messages d'erreur, aux métadonnées techniques et aux journaux nécessaires au diagnostic**, sans accès aux données métier traitées par les systèmes d'information de l'ATIH ;
- **n'accède aux données métier traitées par les systèmes d'information de l'ATIH que lorsque cela est nécessaire à la résolution d'un incident ou d'une demande**. Cet accès reste limité au besoin identifié. Les éventuelles copies ou extractions réalisées pour traiter la demande sont **supprimées dès qu'elles ne sont plus nécessaires**, sauf instruction contraire de l'ATIH ;
- utilise exclusivement des **comptes nominatifs et des habilitations adaptées**. Les accès sont journalisés et les droits sont retirés lorsqu'ils ne sont plus nécessaires.

L'ATIH informe les utilisateurs qu'ils ne doivent pas transmettre de données personnelles au service d'assistance, en particulier de données de santé, sauf indication contraire donnée pour les besoins du traitement d'une demande. Dans ce cadre :

- **en cas de dépôt de telles données en clair dans un ticket**, une pièce jointe ou un canal non prévu, **chacun** prend les mesures nécessaires pour en limiter la diffusion dans son périmètre d'intervention : il supprime ou fait supprimer les données, informe le demandeur de la conduite à tenir et signale la situation si elle est susceptible de constituer un incident de sécurité ou une violation de données à caractère personnel ;
- **lorsque de telles données sont nécessaires à la résolution d'un ticket**, y compris des données locales auxquelles l'ATIH n'accède pas normalement, notamment des fichiers produits ou conservés localement par un établissement, **chacun** veille au respect des consignes de l'ATIH dans son périmètre d'intervention : chiffrement préalable des données, transmission du mot de passe ou de la clé de déchiffrement par un canal séparé, absence de dépôt de données en clair dans le ticket et suppression des copies ou extractions dès qu'elles ne sont plus nécessaires, sauf instruction contraire de l'ATIH.

4.6 Usage de l'IA

4.6.1 Principes généraux d'usage de l'IA

Lorsqu'un **organisme prestataire** envisage de recourir à une solution d'IA dans le cadre de l'exécution d'une prestation confiée par l'ATIH, ce recours doit être porté à la connaissance de l'ATIH dans les documents remis ou applicables à la prestation.

La ligne encadrante de l'ATIH, ainsi que les **organismes prestataires** lorsqu'une activité leur est confiée, veillent à ce que l'usage des solutions d'IA respecte les consignes précisées ci-dessous.

4.6.2 Solutions d'IA maîtrisées et non maîtrisées

Dans la présente section, **une solution d'IA maîtrisée** désigne une solution, qu'elle soit hébergée dans le cloud, installée localement ou exécutée dans un environnement interne, dont les conditions d'usage, les garanties de confidentialité, de sécurité, de non-réutilisation des contenus, de conservation, de sous-traitance et de localisation sont connues et jugées suffisantes.

Le caractère maîtrisé d'une solution d'IA repose sur des garanties suffisantes, notamment sur :

- l'absence d'utilisation des contenus fournis ou générés pour entraîner des modèles, enrichir une base mutualisée, améliorer un service au bénéfice de tiers ou poursuivre une finalité étrangère à l'usage autorisé par l'ATIH ;
- une conservation des contenus limitée aux durées nécessaires à la fourniture du service, à la sécurité, à la traçabilité, à la conformité ou au respect d'obligations applicables, avec des durées ou règles de conservation connues ou justifiables ;
- la limitation de tout accès humain aux contenus aux seuls cas strictement nécessaires, notamment pour le support, la sécurité ou le respect d'obligations applicables, par des personnes habilitées, soumises à des obligations de confidentialité et dans des conditions encadrées ;
- des mesures de sécurité adaptées au mode d'hébergement ou d'exécution de la solution, incluant notamment la maîtrise de son administration, de ses accès, de ses mises à jour, de sa journalisation éventuelle, de ses connexions à des services externes et de la protection des contenus traités ;
- la connaissance et l'encadrement de la localisation des traitements, des éventuels transferts hors Union européenne et des garanties juridiques associées, dans des conditions compatibles avec les exigences de l'ATIH ;
- la maîtrise de la chaîne de sous-traitance, incluant l'identification des sous-traitants, l'encadrement de leurs interventions et la répercussion des obligations de sécurité, de confidentialité et de protection des données applicables ;
- la possibilité pour l'ATIH d'obtenir les justificatifs nécessaires, notamment la documentation contractuelle, les engagements du fournisseur, les informations relatives à la sécurité, à la localisation des traitements, à la sous-traitance, aux durées de conservation et, le cas échéant, aux paramètres d'administration applicables.

Pour un **organisme prestataire**, une solution d'IA maîtrisée est une solution dont il s'assure qu'elle respecte les présentes exigences et dont il peut justifier auprès de l'ATIH.

L'**organisme prestataire** doit être en mesure de démontrer, sur demande de l'ATIH, que la solution d'IA utilisée respecte ces exigences au moyen de la documentation contractuelle, des engagements du fournisseur et, le cas échéant, des paramètres de configuration ou d'administration permettant d'assurer ce niveau de protection.

Le caractère maîtrisé d'une solution d'IA ne vaut pas autorisation de tous les usages. Chaque utilisation doit rester conforme aux finalités prévues, à la nature et à la sensibilité des informations traitées, au principe de minimisation et aux instructions applicables.

4.6.3 Règles d'utilisation selon la nature des contenus

Le tableau ci-dessous précise les usages autorisés selon le type de solution d'IA utilisé et la catégorie de contenu.

Tableau de synthèse — usages autorisés selon le type d'IA et la catégorie de contenu
✅ : utilisation autorisée | ❌ : utilisation non autorisée

Niveau	Type de contenu	IA grand public ou non maîtrisée	IA maîtrisée
🟢 Public	Informations officiellement publiées, diffusées ou mises à disposition du public	✅	✅
🟢 Fictif	Données inventées de toutes pièces, sans lien avec des personnes, situations, données réelles ou informations confidentielles identifiables	✅	✅
🟠 Autres contenus nécessaires à l'activité	Informations internes, données personnelles, données économiques, financières, stratégiques, contractuelles, RH ou techniques ne relevant pas des interdictions ci-dessous	❌	✅*
🔴 Données de santé à caractère personnel	Données relatives à l'état de santé, au parcours de soins, à la prise en charge, aux données PMSI, ENC, médico-sociales ou SNDS, y compris lorsqu'elles sont pseudonymisées	❌	❌**
🔴 Informations SSI ou techniques très sensibles	Secrets, mots de passe, clés SSH, clés d'API, jetons, certificats, comptes techniques, fichiers de configuration exposant un accès, éléments permettant d'accéder directement à un système d'information de l'ATIH	❌	❌**

* Usage possible avec une solution d'IA maîtrisée uniquement si la finalité est légitime, si les éléments transmis sont limités au strict nécessaire, si les instructions applicables sont respectées et si le contenu ne relève pas des interdictions prévues ci-dessus.
** Par dérogation, ces contenus peuvent être traités par une solution d'IA maîtrisée uniquement lorsque l'ATIH l'a expressément autorisé au préalable dans un cadre documenté.

La dérogation mentionnée ci-dessus ne peut être mise en œuvre qu'après autorisation expresse préalable de l'ATIH dans un cadre documenté. Elle doit préciser le périmètre de l'usage autorisé, les contenus concernés, la solution utilisée, les mesures de protection applicables et, le cas échéant, la durée de l'autorisation.

En cas de doute sur la qualification d'un contenu, sur le niveau de sensibilité applicable ou sur le caractère anonymisé, fictif ou effectivement non réidentifiant de sa transformation, **chacun** sollicite préalablement le responsable de la sécurité du système d'information, le délégué à la protection des données ou la Direction DATA de l'ATIH lorsqu'une question porte sur l'anonymisation de données.

Exemples et précisions d'interprétation

Les exemples sont indicatifs. L'utilisation d'une IA maîtrisée ne dispense pas du respect des obligations de confidentialité, de secret professionnel, de secret des affaires, de commande publique, de protection des données personnelles, de sécurité des systèmes d'information et des instructions applicables.

🟢 **Public** : textes réglementaires publiés, documentation publique de l'ATIH, communiqués de presse, rapports publics, pages publiées sur les sites institutionnels, données ouvertes officiellement mises à disposition.
🟢 **Fictif** : cas métier inventés, jeux de test créés de toutes pièces, maquettes de processus, faux établissements, faux utilisateurs, faux identifiants, exemples de code générique sans donnée réelle, scénarios de formation ne reproduisant pas une situation identifiable.
🟠 **Autres contenus nécessaires à l'activité** : notes de travail internes, projets de procédures, supports de réunion, documents préparatoires, comptes rendus internes, données personnelles hors données de santé, informations RH, éléments économiques, financiers, stratégiques ou contractuels, offres, mémoires techniques, propositions commerciales, éléments de réponse à un appel d'offres, extraits de code, messages d'erreur, rapports SAST ou SonarQube, journaux applicatifs, captures d'écran ou exports techniques, dès lors qu'ils sont nécessaires à l'activité, limités au strict nécessaire et ne comportent ni données de santé à caractère personnel, y compris pseudonymisées, ni informations ou éléments techniques dont la divulgation pourrait permettre l'accès à un système d'information de l'ATIH.
🔴 **Données de santé à caractère personnel** : données PMSI, ENC, données médico-sociales, données SNDS, données relatives à l'état de santé, au parcours de soins ou à la prise en charge, verbatims révélant une situation de santé, données pseudonymisées ou comportant des quasi-identifiants combinés pouvant permettre une réidentification.
🔴 **Informations SSI ou techniques sensibles** : mots de passe, clés SSH, clés d'API, jetons, certificats, comptes techniques, fichiers de configuration exposant un accès, éléments permettant d'accéder directement à un système d'information de l'ATIH.

4.6.4 Transformation préalable des contenus non autorisés

Les contenus qui ne peuvent pas être transmis à une IA grand public ou non maîtrisée peuvent être utilisés dans ce type de solution uniquement s'ils deviennent effectivement publics, strictement fictifs ou anonymisés sans ambiguïté.

Dans le présent document, un contenu est considéré comme anonymisé uniquement lorsque les personnes concernées ne peuvent plus être identifiées, directement ou indirectement, par l'ATIH, par le destinataire ou par un tiers raisonnablement susceptible d'accéder aux informations, y compris par recoupement avec d'autres données disponibles. L'anonymisation doit être effective, irréversible en pratique et adaptée au contexte d'utilisation.

La pseudonymisation, le masquage partiel, le remplacement d'un identifiant par un code, la suppression du nom ou la modification isolée de quelques champs ne suffisent pas nécessairement à rendre un contenu anonyme. Un contenu pseudonymisé ou comportant des quasi-identifiants doit rester traité comme une donnée personnelle tant qu'un risque raisonnable de réidentification subsiste.

Les données de santé à caractère personnel, y compris lorsqu'elles sont pseudonymisées, ainsi que les informations ou éléments techniques dont la divulgation pourrait permettre l'accès à un système d'information de l'ATIH, ne peuvent être utilisés avec une IA maîtrisée que dans le cadre d'une autorisation expresse préalable de l'ATIH ou après une transformation suffisante supprimant le risque qui justifiait leur interdiction.

4.6.5 Responsabilités individuelles et validation des productions

Chacun, lorsqu'il utilise une solution d'IA, veille notamment à :

- utiliser uniquement une solution autorisée par l'ATIH ou, pour un **organisme prestataire**, une solution dont le niveau de maîtrise peut être justifié ;
- vérifier que les contenus transmis sont compatibles avec le type de solution utilisée et avec les règles applicables selon leur nature et leur sensibilité ;
- ne pas transmettre de données de santé à caractère personnel, y compris lorsqu'elles sont pseudonymisées, ni d'informations ou éléments techniques dont la divulgation pourrait permettre l'accès à un système d'information de l'ATIH, sauf autorisation expresse préalable de l'ATIH dans un cadre documenté ;
- transmettre uniquement les éléments strictement nécessaires à l'objectif poursuivi ;
- privilégier, lorsque cela est possible, des contenus publics, strictement fictifs ou anonymisés sans ambiguïté ;
- solliciter un avis en cas de doute sur la nature du contenu, son niveau de sensibilité, son anonymisation ou le caractère maîtrisé de la solution ;
- considérer toute réponse produite par une IA comme une aide nécessitant une vérification humaine avant utilisation, transmission ou intégration dans un livrable, un document, un code applicatif ou une décision ;
- ne diffuser que des productions qu'il est en mesure d'expliquer, de justifier, de maintenir et d'assumer dans son périmètre de responsabilité ;
- mentionner le recours significatif à l'IA lorsque celle-ci a contribué de manière substantielle à la rédaction, à l'analyse, à la production de code, à la préparation d'un livrable ou à l'aide à la décision, conformément aux règles définies par l'ATIH.

Les contenus produits avec l'assistance d'une IA demeurent sous la responsabilité de leur auteur ou de leur valideur. Ils sont soumis aux mêmes exigences de qualité, de sécurité, de confidentialité, de conformité, de validation et de traçabilité que toute autre production réalisée par l'ATIH ou pour son compte par un **organisme prestataire**.