Règles particulières en fonction des schémas de certification

Certification HDS

Paragraphe concerné	Règles supplémentaires
1.1	Pour obtenir une certification HDS, un candidat doit : • être certifié ISO 27001 sur un périmètre couvrant au moins celui pour lequel il demande une certification HDS (le candidat peut obtenir sa certification ISO 27001 dans le cadre de la certification HDS et inversement la certification HDS peut être obtenue à l'occasion d'une certification ISO 27001) ; • prendre en compte dans son système de management de la sécurité de l'information les exigences du référentiel de certification HDS applicables au type de certificat demandé (exigences issues des normes ISO 20000-1, ISO 27018, ISO 27017 et des exigences spécifiques santé). Un hébergeur qui a déjà obtenu une certification ISO 27001 ou une certification ISO 20000-1 peut faire prévaloir ces certifications s'il remplit les conditions citées dans le chapitre Equivalence ci-dessous. Un candidat disposant déjà de ces certifications est évalué sur le périmètre des exigences non couvertes par ces certifications. Les certifications déjà obtenues font l'objet d'une vérification selon les modalités définies dans le chapitre Equivalence ci-dessous. Dans ce cas, l'hébergeur devra réaliser un audit sur les seules exigences couvertes par les certifications existantes. Cet audit aura pour objectif de réaliser un examen de niveau modéré, sur la base de diligences ne mettant toutefois pas en œuvre toutes les procédures requises pour un audit. Les normes ISO 27017 et ISO 27018 ne sont pas prévues pour la délivrance d'une certification mais uniquement comme guide d'implémentation. Elles ne s'inscrivent pas dans un schéma d'accréditation et la notion d'équivalence ne s'applique pas. <u>Equivalence</u> Si le candidat souhaite faire prévaloir la ou les certification(s) selon les normes ISO 27001 et ISO 20000-1 qu'il a déjà obtenues, ces certifications doivent remplir toutes les conditions ci-dessous : • le périmètre d'application de la certification dont dispose l'hébergeur doit inclure le périmètre pour lequel le candidat demande une certification HDS ; • les rapports d'audit : rapport d'audit initial et rapports d'audit de surveillance de la certification dont l'équivalence est demandée doivent être fournis sur demande de l'organisme de certification; • pour un candidat disposant d'une certification ISO 27001, la déclaration d'applicabilité (DdA) du système de gestion de la sécurité des informations de l'organisation doit expressément inclure : - la justification détaillée de toute exclusion de contrôles de l'ISO 27001 ; - la justification détaillée de tout contrôle non applicable ;

8	Les hébergeurs certifiés doivent déposer auprès de l'organisme de certification une demande de recertification au plus tard 3 mois avant la date de fin de validité de la certification.
10	L'autorité compétente est informée de tout transfert de certificat, en indiquant également le nom de l'organisme de certification émetteur.
17	Avant toute intervention de la part de l'équipe d'audit, une vérification est effectuée avec le candidat pour s'assurer que : • les informations qui seront communiquées durant l'audit ne contiennent aucune donnée de santé à caractère personnel, ni aucune donnée confidentielle ou sensible • le système d'information du candidat est auditable de manière adéquate. Dans le cas où le système d'information n'est pas auditable sans accéder à des données de santé à caractère personnel ou d'autres données confidentielles ou sensibles, le candidat est informé, un accord de confidentialité est établi et un professionnel de santé côté client est informé. Les données de santé à caractère personnel et toutes autres données confidentielles ou sensibles auxquelles le personnel de BVC habilité a pu accéder, dans le cadre de l'audit, ne sont en aucun cas divulguées ou réutilisées. Les accès éventuels à des données de santé sont tracés. Ces traces sont horodatées et comportent l'identification nominative de l'auditeur.
20	***Echange d'informations avec l'autorité compétente*** L'envoi des informations (décrites dans les paragraphes ci-dessous) est réalisé par voie électronique en complétant le modèle de l'Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente. **Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente** **Rapport annuel HDS** Nom de l'organisme de certification : *XXXX* Date : *jj/mm/aaaa* **Synthèse des certifications HDS, des audits réalisés et des non-conformités relevées** **Synthèse des difficultés rencontrées lors de la certification HDS** **Propositions d'amélioration de la certification HDS** **Indicateurs sur la procédure de certification HDS** Nombre de certifiés "hébergeur d'infrastructure physique" **(A)** — *XXXX* Nombre de certifiés "hébergeur infogéreur" **(B)** — *XXXX* Nombre de certifications délivrées **(A+B)** — *XXXX* Nombre d'échecs — *XXXX* Nombre de renouvellements — *XXXX* Nombre de suspensions — *XXXX* Nombre de retraits — *XXXX* Nombre de certifications transférées — *XXXX*

Rapport de suspension HDS

Toute décision de suspension de certification d'un hébergeur de données de santé est communiquée en français ou en anglais à l'autorité compétente.
Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été suspendue sont communiquées :

- désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été suspendue ;
- numéro d'identifiant du certificat suspendu ;
- date de suspension du certificat ;
- raisons de la suspension de la certification HDS.

L'envoi des informations est réalisé par voie électronique en complétant le modèle proposé en Annexe C : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

Annexe C : Notification de suspension de certification

Rapport de suspension HDS

Nom de l'organisme de certification : *XXXX* | Date : *jj/mm/aaaa*

Nom hébergeur de données de santé	*XXXX*
Numéro d'identifiant du certificat	*No. XXXX*
Date de suspension	*jj/mm/aaaa*
Raisons de la suspension	*XXXX*

Rapport de retrait HDS

Toute décision de retrait de certification d'un hébergeur de données de santé est communiquée en français ou en anglais à l'autorité compétente.
Les informations ci-dessous relatives à l'hébergeur de données de santé dont la certification a été suspendue sont communiquées :

- désignation ou raison sociale de l'hébergeur de données de santé pour lequel la certification a été retirée ;
- numéro d'identifiant du certificat retiré ;
- date de retrait du certificat ;
- raisons du retrait de la certification HDS.

L'envoi des informations est par voie électronique en complétant le modèle de l'Annexe D : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

Annexe D : Notification de retrait de certification

Rapport de retrait HDS

Nom de l'organisme de certification : *XXXX*	Date : *jj/mm/aaaa*

Nom hébergeur de données de santé	*XXXX*
Numéro d'identifiant du certificat	*No. XXXX*
Date de retrait	*jj/mm/aaaa*
Raisons du retrait	*XXXX*

Répertoire clients HDS

Un rapport des certifications **mensuel** valides, suspendues et retirées est communiquée en français ou en anglais à l'autorité compétente. Ce répertoire doit contenir les données suivantes pour chaque hébergeur de données de santé :

- désignation ou raison sociale de l'hébergeur de données de santé ;
- numéro d'identifiant du certificat ;
- type de certificat ;
- périmètre de la certification ;
- adresse du site certifié et dans le cas d'une certification multi-sites, indiquer l'adresse du siège social ainsi que celles de tous les sites rattachés ;
- état de la certification (valide, suspendue ou retirée) ;
- date de la certification.

L'envoi du répertoire doit être réalisé par voie électronique en complétant le modèle de l'Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente.

Rapport annuel HDS

Chaque année, entre le 1er et le 31 janvier, un rapport annuel en français ou en anglais est fourni à l'autorité compétente comprenant :

- une synthèse anonymisée des certifications HDS, des audits réalisés et des nonconformités relevées.
- une synthèse des difficultés rencontrées lors de la certification des hébergeurs et des éventuelles propositions de modifications à apporter aux référentiels de certification et d'accréditation ;
- des indicateurs sur la procédure de certification HDS, tels que :
  - nombre d'hébergeurs de données de santé en cours de certification ;
  - nombre d'hébergeurs de données de santé ayant échoué à la certification ;
  - nombre de renouvellements de certification.

	L'envoi du rapport annuel est réalisé par voie électronique entre le 1er et le 31 janvier en complétant le modèle proposé en Annexe B : Echanges d'informations entre l'organisme de certification et l'autorité compétente