Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

Licence SPS

C4 : Usages digitaux et numériques

Session 2026 • Code sujet : **2026-LSPS-C4** • Durée : **2 heures** • Coefficient : **3,0**
indicatif

Sommaire

Cliquez sur une partie pour y accéder directement

1. Analyse fonctionnelle et réglementaire des données de santé (3 questions) **Page 3**

2. Étude technologique, calculs de transfert et équipements numériques (3 questions) **Page 5**

3. Préparation du traitement et protocole opératoire traçable (3 questions) **Page 6**

4. Prévention et sécurité numériques (3 questions) **Page 9**

5. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 11**

Sujet officiel (PDF) : https://licencesps.fr/assets/annales/licence-sps/C4 - Usages digitaux et numériques/2026/Licence Sciences Pour la Santé - C4 - Usages digitaux et numériques - Session 2026 - 1-Sujet.pdf

1. Analyse fonctionnelle et réglementaire des données de santé

Dans une étude fictive de suivi de patients au CHU Grenoble Alpes, l'équipe prépare un export contenant des identifiants, des données de santé et des informations de suivi. Il faut qualifier les champs et appliquer les mesures de protection et de partage avant de transmettre un compte rendu à quatre collaborateurs habilités.

Question 1.1. Classez le numéro de dossier, la date de naissance, la date d'intervention, le groupe d'âge, le type d'intervention et la durée de séjour comme identifiant direct, donnée de santé ou donnée potentiellement réidentifiante. Justifiez brièvement le classement des données de santé.

Un champ peut relever de plusieurs catégories : une donnée de santé décrit les soins ou le parcours de santé, tandis qu'une donnée potentiellement réidentifiante peut contribuer à retrouver une personne, surtout par recoupement.

Champ	Classement
Numéro de dossier	Identifiant direct
Date de naissance	Potentiellement réidentifiante
Date d'intervention	Donnée de santé et potentiellement réidentifiante
Groupe d'âge	Potentiellement réidentifiant par recoupement
Type d'intervention	Donnée de santé
Durée de séjour	Donnée de santé

Le type d'intervention et la durée du séjour renseignent sur les soins reçus. La date d'intervention indique également un événement de prise en charge et peut aider à identifier une personne si elle est croisée avec d'autres informations.

> **✓ RÉPONSE À RETENIR**
>
> Identifiant direct : numéro de dossier. Données de santé : date et type d'intervention, durée de séjour. Données potentiellement réidentifiantes : date de naissance, date d'intervention et groupe d'âge.

Question 1.2. Au regard du DT 2, relevez trois mesures à appliquer avant de transmettre le compte rendu. Pour chacune, indiquez le risque auquel elle répond.

Avant l'envoi, appliquer trois mesures :

- **Minimiser le contenu :** retirer les identifiants directs et ne garder que les données utiles. Cela réduit le risque d'identification directe et de divulgation excessive.
- **Contrôler les effectifs :** supprimer ou regrouper toute cellule de moins de 5 personnes. Cela limite le risque de réidentification par recoupement.
- **Sécuriser le partage :** utiliser l'espace institutionnel approuvé et vérifier les droits ainsi que les destinataires. Cela évite l'accès ou l'envoi à une personne non autorisée.

Les données agrégées peuvent aussi permettre une réidentification si les groupes sont trop petits.

✓ RÉPONSE À RETENIR

Minimiser les données, masquer les cellules de moins de 5 personnes et partager uniquement par l'espace institutionnel approuvé après vérification des droits et des destinataires.

Question 1.3. Expliquez la différence entre pseudonymisation et anonymisation. Indiquez laquelle des deux notions décrit le mieux un fichier de travail conservant un code de remplacement dont la table de correspondance reste séparément accessible.

La **pseudonymisation** remplace les identifiants directs par un code. Une réattribution reste possible grâce à une information complémentaire, qui doit être séparée et protégée. L'**anonymisation** empêche de retrouver une personne à partir des données, y compris par recoupement raisonnablement possible.

Un fichier de travail avec un code de remplacement et une table de correspondance accessible est donc pseudonymisé, et non anonymisé. La table doit être conservée séparément et son accès limité aux personnes habilitées.

✓ RÉPONSE À RETENIR

Le fichier de travail est pseudonymisé : la table de correspondance permet encore une réidentification. L'anonymisation rend cette réidentification impossible.

2. Étude technologique, calculs de transfert et équipements numériques

Le dossier présente l'architecture numérique utilisée pour accéder aux données de recherche, avec un serveur de fichiers et un onduleur représentés dans un coffret. Les candidats calculent le volume et la durée de transfert d'un export de 2 400 lignes, puis interprètent les rôles des équipements et une précaution d'installation.

Question 2.1. Calculez le volume du fichier source, en MB, à partir de 2 400 lignes de 18 kB chacune, en retenant 1 kB = 1 000 octets.

Une ligne représente $18\,\text{kB} = 18\,000$ octets. Pour $2\,400$ lignes, le volume est $2\,400 \times 18\,000 = 43\,200\,000$ octets. La conversion en MB utilise la convention décimale du sujet : $1\ \text{MB} = 1\,000\,000$ octets. Le calcul porte sur le fichier source uniquement, sans la documentation d'accompagnement.

✓ RÉPONSE À RETENIR

Volume : 43,2 MB.

Question 2.2. Pour un débit nominal de transfert de 20 Mbit/s, calculez le débit utile en MB/s puis estimez la durée de transfert du fichier source. Utilisez Dutile = 0,70 × Dnominal et t = V / Dutile, après conversion cohérente des unités. Donnez la durée en secondes, arrondie au dixième.

Le débit utile vaut $0{,}70 \times 20 = 14$ Mbit/s. En divisant par 8 bits par octet, on obtient $14/8 = 1{,}75$ MB/s, avec les unités décimales du sujet. La durée s'obtient en divisant le volume de $43{,}2$ MB par ce débit utile. Le résultat est arrondi au dixième de seconde et suppose un débit constant.

✓ RÉPONSE À RETENIR

Débit utile : 1,75 MB/s ; durée : 24,7 s.

Question 2.3. À partir du DT 1, indiquez le rôle de l'équipement repéré 3 et celui de l'équipement repéré 4. Donnez une raison opérationnelle de ne pas placer un équipement réseau ou un serveur directement sur le sol du local.

L'équipement 3 est le serveur de fichiers : il stocke les fichiers et les rend accessibles aux utilisateurs autorisés. L'équipement 4 est l'onduleur : il protège temporairement l'alimentation électrique des équipements raccordés en cas de coupure, sans remplacer une sauvegarde.

Ne pas poser un serveur ou un équipement réseau directement au sol limite son exposition à l'eau, à la poussière et aux chocs. Cela contribue aussi à préserver le matériel et à faciliter son entretien.

✓ RÉPONSE À RETENIR

3 : stockage et accès aux fichiers. **4 :** alimentation électrique temporaire en cas de coupure. Installation hors du sol pour protéger le matériel.

3. Préparation du traitement et protocole opératoire traçable

L'équipe doit préparer un fichier de travail à partir d'un export source de 2 400 lignes, sans modifier l'original, et traiter les anomalies relevées lors du contrôle initial. Le protocole doit être tracé, les données pseudonymisées protégées et les résultats vérifiés avant diffusion, avec un accès au fichier de travail limité à deux personnes habilitées.

Question 3.1. Rédigez, dans l'ordre, un protocole d'au moins cinq opérations depuis la réception de l'export jusqu'à la préparation du fichier de travail. Intégrez la conservation du fichier source, le contrôle des doublons et des valeurs manquantes, la pseudonymisation, la vérification des dates et la consignation des opérations.

1. À réception, enregistrer l'export dans l'espace institutionnel sécurisé, le conserver en lecture seule et créer une copie de travail.
2. Après import, vérifier la présence des 2 400 lignes.
3. Examiner les 12 identifiants en doublon avec la source et les résoudre dans la copie.
4. Signaler les 36 durées manquantes, sans imputation non validée.
5. Vérifier les 8 dates hors période auprès de la source ou du responsable de l'étude.
6. Remplacer les identifiants par des codes, protéger séparément la table de correspondance et limiter le fichier aux deux personnes habilitées.
7. Consigner les contrôles, anomalies, décisions et validations.

DR 1 : protocole ordonné



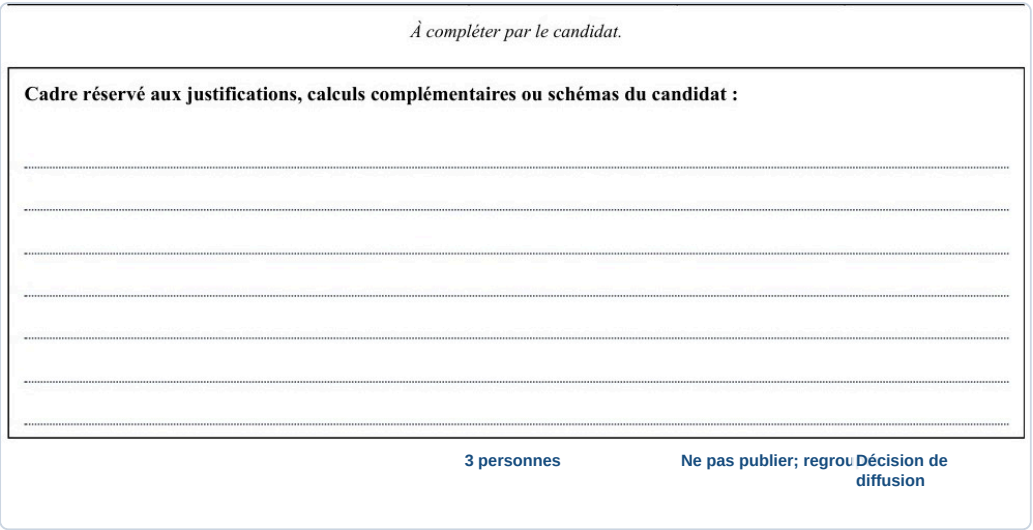
✓ RÉPONSE À RETENIR

Original en lecture seule, copie contrôlée et pseudonymisée, accès limité aux deux personnes habilitées, opérations consignées.

Question 3.2. Décidez si un groupe d'âge comportant trois personnes peut être publié dans un compte rendu destiné à quatre collaborateurs. Justifiez la décision au regard du seuil fourni et indiquez une action possible pour réduire le risque de divulgation.

La cellule de 3 personnes ne peut pas être publiée isolément : elle est sous le seuil de 5 personnes et peut faciliter une divulgation. Le fait que le compte rendu soit destiné à quatre collaborateurs ne change pas cette règle. Regrouper cette tranche d'âge avec une autre peut réduire le risque, à condition que la cellule diffusée atteigne au moins 5 personnes. Il faut aussi vérifier que les autres résultats ne permettent pas de retrouver indirectement ce petit effectif.

DR 1 : décision pour la cellule de faible effectif



À compléter par le candidat.

Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :

3 personnes	Ne pas publier; regrou	Décision de diffusion

✓ RÉPONSE À RETENIR

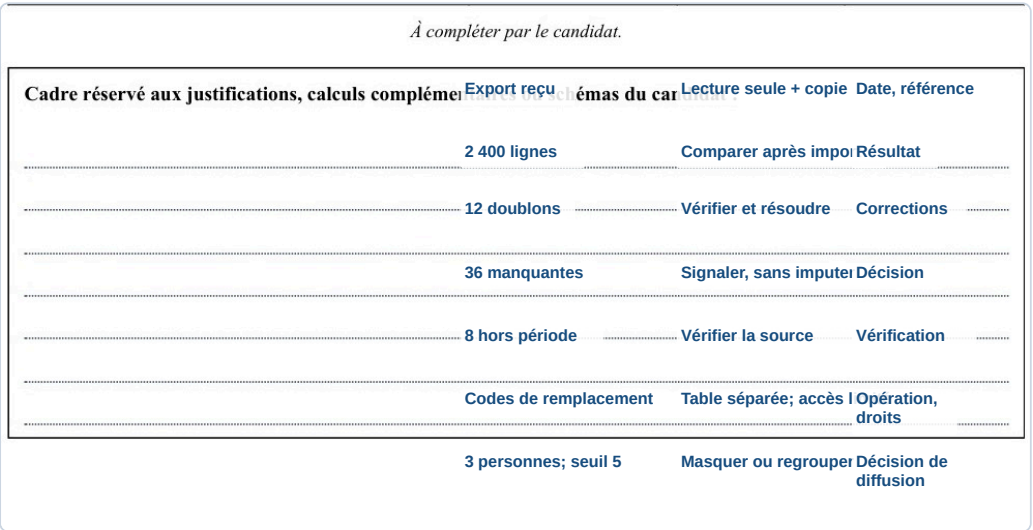
Ne pas publier isolément la cellule de trois personnes; regrouper des catégories pour atteindre au moins cinq personnes.

Question 3.3. Complétez le DR 1 en indiquant les contrôles à réaliser, les anomalies relevées et la décision ou l'action associée. Ne remplacez pas les données manquantes sans règle d'imputation validée.

Le fichier source reste intact et les vérifications portent sur la copie de travail. Comparer le nombre de lignes après import, puis examiner chaque anomalie avant de poursuivre l'analyse. Les valeurs manquantes restent signalées sans imputation non validée; les dates hors période sont vérifiées auprès de la source ou du responsable. Protéger séparément la table de correspondance et réserver le fichier pseudonymisé aux deux personnes habilitées. Consigner les contrôles et décisions dans le suivi.

Étape ou contrôle	Résultat ou anomalie	Action à réaliser	Trace à conserver
Conservation du fichier source	Export reçu	Conserver en lecture seule; créer une copie	Date et référence de réception
Contrôle du nombre de lignes	2 400 lignes attendues	Comparer après import	Résultat du contrôle
Recherche des doublons	12 identifiants en doublon	Vérifier avec la source et résoudre dans la copie	Anomalies et corrections
Traitement des valeurs manquantes	36 durées manquantes	Signaler; ne pas imputer sans règle validée	Nombre et décision
Vérification des dates hors période	8 dates à vérifier	Comparer à la source ou consulter le responsable	Vérifications et décision
Pseudonymisation et protection de la correspondance	Identifiants directs dans la source	Remplacer par des codes; séparer et protéger la correspondance; limiter l'accès à deux personnes habilitées	Opération et droits d'accès
Contrôle des cellules de faible effectif	3 personnes; seuil minimal de 5	Ne pas publier isolément; regrouper des catégories	Contrôle et décision de diffusion

DR 1 complété : contrôles, anomalies et actions



✓ RÉPONSE À RETENIR

DR 1 complété : original préservé, anomalies contrôlées dans la copie et cellule de moins de 5 personnes non diffusée isolément.

4. Prévention et sécurité numériques

Un collaborateur reçoit une demande d'envoi du fichier de travail vers une adresse personnelle, tandis qu'un poste affiche une demande de connexion inhabituelle et propose un logiciel non référencé. Il faut définir les réactions immédiates, organiser un partage avec des droits différenciés et vérifier que les sauvegardes permettent une restauration.

Question 4.1. Décrivez les actions immédiates à prendre face au courriel demandant l'envoi vers une adresse personnelle, à la demande de connexion inhabituelle et à la proposition d'installation d'un logiciel. Précisez à quel interlocuteur ou service signaler l'incident.

Ne transmettez pas le fichier à l'adresse personnelle et n'utilisez aucun canal non approuvé. Ne répondez pas au courriel et n'ouvrez aucun lien ou pièce jointe suspecte. Ne validez pas la demande de connexion et n'installez pas le logiciel proposé. Signalez le courriel, l'authentification inattendue et le logiciel non référencé au service informatique, selon la procédure locale. Conservez les éléments utiles au signalement sans poursuivre l'interaction.

> ✓ **RÉPONSE À RETENIR**
>
> Refuser l'envoi, ne pas valider la connexion ni installer le logiciel, puis signaler les trois éléments au service informatique.

Question 4.2. Proposez une organisation du partage respectant le cahier des charges : réservez l'accès au fichier pseudonymisé aux deux personnes habilitées et rendez le compte rendu accessible aux quatre collaborateurs. Prévoyez la vérification des destinataires et la conservation d'une trace du partage.

Utilisez uniquement l'espace institutionnel approuvé. Réservez le fichier pseudonymisé aux deux personnes habilitées et protégez séparément la table de correspondance. Rendez le compte rendu accessible aux quatre collaborateurs, après vérification qu'il ne contient aucun identifiant direct ni cellule de moins de cinq personnes. Avant le partage, contrôlez les destinataires et leurs droits. Conservez une trace datée du dépôt, des accès accordés et des destinataires, puis retirez les droits devenus inutiles.

> ✓ **RÉPONSE À RETENIR**
>
> Fichier pseudonymisé : deux personnes habilitées. Compte rendu : quatre collaborateurs, après contrôle des destinataires et des cellules diffusées.

Question 4.3. Complétez le DR 2 avec trois risques, une mesure de prévention adaptée à chacun et la conduite à tenir en cas d'incident. Citez également une vérification à réaliser pour vous assurer que la sauvegarde permet effectivement une reprise de l'activité.

Le DR 2 associe chaque situation à sa conséquence, à une prévention et à une conduite à tenir. En cas d'envoi erroné, d'authentification inattendue ou d'installation non autorisée, interrompez l'action et alertez le service informatique. Pour le partage, appliquez des droits adaptés à la mission et vérifiez les destinataires. Pour limiter la perte ou la corruption, vérifiez que les sauvegardes sont protégées. Testez la restauration d'une sauvegarde, puis contrôlez l'intégrité et l'ouverture des données récupérées.

DR 2 complété : risques et réponses

Situation ou risque	Conséquence possible	Prévention ou réponse immédiate	Signalement ou vérification
Envoi demandé vers une adresse personnelle	Divulgation	Refuser l'envoi	Alerter le service informatique
Demande d'authentification inattendue	Compte comprom	Ne pas valider	Signaler au service informatique
Installation d'un logiciel non référencé	Maliciel, fuite	Ne pas installer	Alerter le service informatique
Partage du fichier de travail	Accès indu	Droits limités; contrôler les accès	Tracer; signaler toute erreur
Perte ou corruption des données	Perte de données	Sauvegarde protégée	Tester la restauration; contrôler l'intégrité

✓ RÉPONSE À RETENIR

Refuser les actions suspectes, limiter les accès, signaler les incidents au service informatique et tester la restauration des sauvegardes.

Ce qu'il faut retenir de ce sujet (Session 2026)

Bilan de l'épreuve : L'épreuve C4 Usages digitaux et numériques, session 2026, code 2026-LSPS-C4, dure deux heures et porte un coefficient indicatif de 3. À partir d'une étude fictive de suivi de patients au CHU Grenoble Alpes, elle évalue la qualification des données de santé, les calculs de transfert, le contrôle et la traçabilité des données, ainsi que la sécurité des accès, du partage et des sauvegardes.

Notions-clés, formules & règles à maîtriser

- Les données concernant la santé constituent une catégorie particulière de données personnelles au sens de l'article 9 du RGPD.
- La pseudonymisation remplace les identifiants directs par un code, mais les données restent réattribuables si une table de correspondance existe.
- Débit utile = 0,70 × débit nominal ; convertir les bits en octets avant d'exprimer le débit en MB/s.
- Ne pas diffuser une cellule statistique de moins de cinq personnes ; les valeurs manquantes ne s'imputent qu'avec une règle validée.

Points de vigilance & attentes du jury

- Distinguer identifiant direct, donnée de santé et donnée potentiellement réidentifiante, en justifiant le classement des données de santé.
- Présenter les conversions d'unités avant le calcul du volume et de la durée de transfert.
- Conserver la source en lecture seule, documenter les transformations et signaler les anomalies sans correction injustifiée.
- Vérifier les habilitations et les destinataires, utiliser un espace approuvé et signaler les connexions ou logiciels inattendus.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment convertir le débit de transfert en MB/s ?

Appliquez d'abord le rendement : 20 Mbit/s × 0,70 = 14 Mbit/s. Comme un octet vaut huit bits, divisez ensuite par huit : le débit utile est de 1,75 MB/s avec les unités décimales indiquées.

Q : Quelle est la différence entre pseudonymisation et anonymisation ?

La pseudonymisation remplace les identifiants par un code, mais une réattribution reste possible grâce à une information complémentaire protégée. L'anonymisation empêche cette réattribution de façon irréversible dans les conditions considérées.

Q : Que faire des durées de séjour manquantes pendant le contrôle ?

Signalez les 36 valeurs manquantes et conservez-en la trace. Ne les remplacez pas par une valeur estimée ou moyenne sans règle d'imputation préalablement validée, puis vérifiez les résultats avant diffusion.

Q : Quels critères de sécurité doivent guider le partage et la restauration ?

Partagez les données uniquement dans un espace institutionnel approuvé, avec des droits adaptés à la mission et après vérification des destinataires. Gardez une trace du partage et testez la restauration d'une sauvegarde protégée.

Sujet officiel associé (PDF) : https://licencesps.fr/assets/annales/licence-sps/C4 - Usages digitaux et numériques/2026/Licence Sciences Pour la Santé - C4 - Usages digitaux et numériques - Session 2026 - 1-Sujet.pdf
Ressources Licence Sciences Pour la Santé : Toutes les annales & corrigés • Fiches de révision complètes • Simulateur de notes d'examen

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.