**ANNEXE 2 : FICHES THÉMATIQUES RELATIVES AUX OBLIGATIONS LÉGALES DE L’INSTITUTION DE SANTÉ : HÔPITAL, CLINIQUE, LABORATOIRE, RADIOLOGIE, …**

Sources: [*Dépliant*](https://www.sfh-tr.nhs.uk/media/1964/code-of-conduct-leaflet-gdpr-compliant.pdf) *à destination du personnel des Sherwood Forest Hospitals,* [*Code*](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=2ahUKEwiLuZXFkYboAhXNDewKHSieAAIQFjATegQIBhAB&url=https%3A%2F%2Fwww.gloshospitals.nhs.uk%2Fdocuments%2F8000%2FData_Protection__Confidentiality_Policy_B0734.pdf&usg=AOvVaw2xc0Qd5OYybPoEFC18RyOn) *des Gloucestershire Hospitals*

|  |  |  |
| --- | --- | --- |
| **LEGISLATION** | **POUR TOUT CONSEIL COMPLÉMENTAIRE OU CONTACT** |  |
| * [Loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel](http://www.inpdp.nat.tn/ressources/loi_2004.pdf), telle que modernisée à la lumière de [la convention n°108 pour la protection des personnes à l’égard du traitement des données à caractère personnel](https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726) * [Délibération n°4 du 5 septembre 2018 concernant le traitement des données à caractère personnel liées à la santé](http://www.inpdp.nat.tn/4_sante.pdf)   **L’organisme de santé doit se conformer à six principes clés de traitement des données à caractère personnel**.  Les données doivent être :   1. Traitées de manière équitable, loyale et légale ; 2. Traitées uniquement pour des finalités licites, déterminées et explicites ; 3. Adéquates, pertinentes et non excessives ; 4. Conservées de manière exacte et à jour ; 5. Ne pas être conservées plus longtemps que nécessaire ; 6. Conservées en toute sécurité et protégées contre toute divulgation, perte ou dommage accidentels.   **Le code de conduite**  Le code de conduite définit les règles qui régissent l'utilisation des informations relatives aux patients au sein de l’hôpital XXX et le contrôle que le patient peut exercer à cet égard. Elle porte sur les droits d'accès des individus à leurs propres informations, sur la manière dont les informations seront partagées et sur la manière dont les décisions relatives au partage des informations seront prises. Toute personne travaillant pour l’hôpital XXX doit se conformer à ces directives. | **Gouvernance de l'information**  ……………………………………………………  **RSSI**  ……………………………………………………  SITES WEB UTILES  [INPDP](http://www.inpdp.nat.tn/)  l’hôpital XXX Département de santé Code de conduite  l’hôpital XXX  Adresse  Tel: …………  Site: …………….. | **\*Logo de l’hôpital\***  **Protection et confidentialité des données à caractère personnel** |

|  |  |  |
| --- | --- | --- |
| **INTRODUCTION** | **PRINCIPES ESSENTIELS** | **SECURITE DE L’INFORMATION** |
| Tous les employés de l’hôpital XXX sont responsables du maintien de la confidentialité des données du personnel et des patients, et ce devoir de confidentialité est inscrit dans les contrats de travail.  Le personnel est autorisé à accéder aux données à caractère personnel selon le principe du besoin d'en connaître, afin de permettre l’exercice des fonctions. L'accès à des données qui ne sont pas nécessaires à l'exécution du travail ou la transmission de données à une personne qui n'est pas autorisée à les recevoir constitue une violation de la confidentialité qui peut entraîner des mesures disciplinaires.  Les violations graves de la [loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel](http://www.inpdp.nat.tn/ressources/loi_2004.pdf) et de la [délibération n°4 du 5 septembre 2018 concernant le traitement des données à caractère personnel liées à la santé](http://www.inpdp.nat.tn/4_sante.pdf) peuvent entraîner des sanctions pécuniaires.  **Recommandations complémentaires de bonnes pratiques :**  Le principe de responsabilitisation est au cœur de bonne pratique de l’hopital XXX. Il recouvre notamment les pratiques suivantes:   1. Traiter les données d'une manière transparente et légitime. 2. Collecter les données pour des finalités spécifiques, claires et légitimes. 3. Traiter les données conformément à la finalité assignée et sur la base du consentement de la personne concernée tel que défini par la délibération n°4 ou des fins légitimes mentionnées dans ladite délibération. 4. Collecter les données auprès de la personne concernée dans la mesure du possible, ou le cas échéant, auprès d'autres sources, à condition de respecter les principes de transparence, de légitimité et de secret professionnel stipulés dans la législation en vigueur. 5. Assurer l’exactitude des données, les mises à jour et la cohérence avec la finalité du traitement et dans ses limites. 6. Prendre dès la conception les mesures techniques nécessaires pour protéger ces données. 7. Respecter les droits de la personne concernée. 8. Protéger les données personnelles et les incorporer dans le système de traitement existant, ou les prendre en compte lors de la conception de ce système. 9. Le responsable du traitement et son sous-traitant doivent prouver à l'Instance qu'ils ont pris toutes les mesures appropriées pour réaliser cette protection conformément aux obligations qui leur incombent et énoncées dans la délibération n°4. 10. Le responsable de traitement et son sous-traitant, qui ne font pas partie des professions de santé, traitent les données à caractère personnel liées à la santé dans le cadre du respect des règles du secret professionnel et avec le même niveau de protection accordé aux membres des professions de santé.   Le terme "données à caractère personnel" fait référence à toutes les informations, quelle que soit leur origine ou leur forme et qui permettent d'identifier une personne physique ou la rendent identifiable, directement ou indirectement à travers plusieurs informations ou symboles, et notamment à travers un élément d'identité spécifique. Par exemple, le nom, l'adresse, le code postal, le numéro d'identité ou la situation familiale, etc. Toute donnée à caractère personnel, qu'elle soit sensible ou non, doit être traitée de manière confidentielle. | Toute donnée à caractère personnel collectée dans un but précis ne doit pas être utilisée dans un autre but sans le consentement de la personne concernée.  Le droit d'un individu à la confidentialité est protégé par l'éthique et la loi. Les personnes qui font appel aux services de l’hôpital XXX ou qui sont employées par l’hôpital XXX ont le droit de savoir quelles données sont collectées et pourquoi, ainsi que les objectifs du partage de ces données.  Une personne a le droit de choisir de divulguer ou non ses données et peut modifier sa décision à tout moment.  Chaque membre du personnel a l'obligation de protéger la confidentialité et le devoir de vérifier l'autorisation d'une autre personne demandant des données. Cela permet de garantir que les données ne sont transmises qu'aux personnes qui ont le droit de les consulter. Tous les membres du personnel doivent comprendre qu'il leur incombe de protéger les données qu'ils recueillent et suivre les règles et les conseils qui leur sont donnés.  Les données concernant la santé des patients ne peuvent être utilisées à des fins commerciale.  Les règles sont là pour protéger à la fois le patient et le personnel contre les violations de confidentialité. Toutefois, les règles ne doivent pas être appliquées de manière si rigide qu'elles ne soient pas pratiques à suivre ou qu'elles nuisent à la santé et aux soins de la personne concernée.  **Consentement**  Pour être valable, le consentement doit être donné volontairement et librement. Un patient/employé doit être pleinement informé et savoir quelle sera l'utilisation ou la divulgation envisagée de ses données personnelles.  Le consentement explicite d'un patient doit toujours être demandé en cas d’utilisation de ses données d'une manière qui ne contribue pas directement à ses soins de santé.  Dans certaines circonstances, il peut être légal de partager des données à caractère personnel sans le consentement du patient (par exemple, dans le cadre d'une enquête sur un crime grave, pour protéger les enfants ou pour des raisons d'intérêt public). | Toutes les précautions raisonnables doivent être prises pour protéger la sécurité physique des données contre la perte, la détérioration ou la destruction accidentelle et contre la divulgation non autorisée ou accidentelle.   * N'utilisez pas le mot de passe de quelqu'un d'autre pour accéder aux informations contenues dans les ordinateurs. * Aucune donnée personnelle ne doit être conservée sur un appareil mobile (par exemple, un ordinateur portable, un PDA, une clé USB), à moins qu'elle ne soit cryptée selon une norme approuvée. * La télécopie n'est pas sécurisée. Les données personnelles ne doivent être faxées que lorsqu'il n'y a pas d'autre solution et que leur réception immédiate est nécessaire à des fins cliniques. Des procédures spécifiques doivent être respectées en cas de transfert vers l’étranger. * Les enveloppes contenant des données personnelles doivent être scellées de manière sûre, porter la mention "confidentiel" et être clairement adressées à un contact identifié. * Les procédures de validation des appels téléphoniques doivent être suivies pour confirmer l'identité des appelants avant que des informations ne leur soient communiquées. * Le personnel doit toujours s'assurer que la politique de l’hôpital XXX est respectée lors de l'envoi de données à caractère personnel par courrier électronique. * Suivez les politiques et procédures de l’hôpital XXX en matière de protection des données, de confidentialité et de sécurité des informations et demandez conseil en cas de doute.   Si vous n'êtes pas sûr de devoir divulguer des informations, consultez votre supérieur hiérarchique et/ou, si nécessaire, demandez conseil au chargé de protection des données personnelles (DPO). |