| MODÈLE DE CHARTE DES BONNES PRATIQUES D'UTILISATION DES APPAREILS MOBILES DE [Nom de l'Organisation] |
| --- |

| Version |  |
| --- | --- |
| Classification |  |
| Diffusion |  |

| Cycle de vie du document |
| --- |
| **Date** | **Révision** | **Rédacteur** | **Note** |
| 00/00/2025 | 1.0 | Prénom Nom | Création du document |
|  |  |  |  |

| **Voici une version spécialisée de la charte des bonnes pratiques d'utilisation des appareils mobiles, adaptée spécifiquement au contexte d'un établissement de santé. L'accent est mis sur la protection des données de santé et le respect du secret médical.****Points Cruciaux à Adapter et Valider IMPÉRATIVEMENT :**1. **Validation Juridique et RSSI** : Ce document DOIT être relu, adapté et validé par le service juridique, le Délégué à la Protection des Données (DPO) et le Responsable de la Sécurité des Systèmes d'Information (RSSI) de votre établissement.
2. **Politique BYOD** : La section 4 doit être précisément adaptée à la politique réelle de votre établissement concernant l'utilisation des appareils personnels. Si le BYOD n'est absolument pas autorisé pour l'accès aux données professionnelles/patients, cette section doit le stipuler clairement et interdire cet usage.
3. **Outils spécifiques** : Mentionnez les outils de sécurité et de gestion des appareils mobiles (MDM, VPN, applications métier sécurisées) spécifiquement utilisés par votre établissement.
4. **Processus** : Détaillez les procédures de signalement (à qui s'adresser précisément en cas de perte, vol ou incident de sécurité), les procédures de demande d'accès, etc.
5. **Exemples concrets** : Adaptez les exemples (types de données sensibles, situations à risque) au contexte spécifique de vos services.
6. **Articulation avec d'autres documents** : Faites le lien avec le règlement intérieur, la politique de sécurité des systèmes d'information globale (PSSIS), les chartes spécifiques à l'accès au DPI si elles existent.
7. **Accusé de réception** : Prévoyez un mécanisme formel par lequel chaque utilisateur atteste avoir reçu, lu et compris la charte (signature électronique ou papier).
 |
| --- |

**CHARTE DES BONNES PRATIQUES D'UTILISATION DES APPAREILS MOBILES** **DE [Nom de l'Organisation]**

Préambule

Dans un établissement de santé, l'utilisation d'appareils mobiles (smartphones, tablettes) par le personnel est de plus en plus courante, offrant de nouvelles opportunités pour l'accès à l'information, la communication et potentiellement l'amélioration de la prise en charge des patients. Cependant, ces appareils représentent également des points d'entrée potentiels pour des risques majeurs, notamment la compromission de la sécurité des données de santé, la violation du secret médical et la perturbation de nos systèmes d'information.

La présente charte vise à établir un cadre clair et des règles strictes pour l'utilisation des appareils mobiles (qu'ils soient fournis par l'établissement ou personnels utilisés dans un cadre autorisé - BYOD) afin de garantir la sécurité des informations de santé, le respect de la confidentialité des patients, et le bon fonctionnement de nos systèmes, conformément aux exigences légales et éthiques (Secret Médical, RGPD, Code de la Santé Publique).

[**Article 1 : Objet et Champ d'Application 5**](#_wnjl8euyy41h)

[1.1. Objet : 5](#_p5lp2t1q07hj)

[1.2. Champ d'Application : 5](#_iifzyi2fabha)

[**Article 2 : Principes Fondamentaux 5**](#_69fiqk2zh0vf)

[**Article 3 : Bonnes Pratiques d'Utilisation Quotidienne et Protection des Données Patients 5**](#_5ntvtrlja1n)

[3.1. Sécurité du Terminal : 5](#_wzb8d1b8nfmb)

[3.2. Protection des Données de Santé et Confidentialité : 6](#_ttmomwdydwsq)

[3.3. Connectivité et Accès Réseau : 6](#_ze5s0npkk7mz)

[3.4. Manipulation Physique et Signalement : 6](#_3bzcodyrpdo9)

[**Article 4 : Règles Spécifiques au BYOD (Utilisation d'Appareils Personnels) 7**](#_e77fyary4tix)

[**Article 5 : Contrôle et Surveillance 7**](#_uw9zkoxu0a1k)

[**Article 6 : Non-respect de la Charte et Sanctions 7**](#_cxmdyaa6yxl0)

[**Article 7 : Formation et Sensibilisation 7**](#_w4g9yv2xsj9x)

[**Article 8 : Révision de la Charte 7**](#_1lgxfpynyf0l)

[**Article 9 : Prise d'Effet 7**](#_fyp9egj3qnw7)

# Article 1 : Objet et Champ d'Application

## 1.1. Objet :

Définir les règles et les bonnes pratiques d'utilisation des smartphones et tablettes utilisés à des fins professionnelles ou connectés aux ressources de [Nom de l'Établissement], avec un focus particulier sur la manipulation des données de santé.

## 1.2. Champ d'Application :

Cette charte s'applique à l'ensemble du personnel de [Nom de l'Établissement] (personnel médical, paramédical, administratif, technique, stagiaires, médecins libéraux intervenant, prestataires externes, etc.) utilisant un appareil mobile pour accéder aux informations, applications ou réseaux de l'établissement, que cet appareil soit fourni par l'établissement ou personnel (dans le cadre d'une politique BYOD autorisée et définie).

# Article 2 : Principes Fondamentaux

L'utilisation des appareils mobiles dans un établissement de santé doit respecter les principes fondamentaux suivants :

* **Secret médical et professionnel** : Le respect absolu du secret médical et du secret professionnel est impératif. Les données patients sont les plus sensibles et doivent être protégées en tout temps et en tout lieu.
* **Confidentialité** : Assurer la confidentialité de toutes les informations consultées ou traitées, qu'elles soient d'ordre médical, administratif ou interne à l'établissement.
* **Sécurité** : Protéger l'appareil contre l'accès non autorisé, les pertes de données, et les logiciels malveillants pour éviter de compromettre les systèmes de l'établissement.
* **Intégrité** : Garantir l'exactitude et la fiabilité des données accessibles via les appareils mobiles.
* **Disponibilité** : Contribuer au maintien de l'accès aux informations et aux applications nécessaires à la prise en charge des patients.
* **Conformité** : Respecter scrupuleusement les lois et réglementations en vigueur (RGPD, Code de la Santé Publique, Code Pénal) ainsi que les politiques internes de l'établissement (règlement intérieur, PGSSI-S).
* **Besoin d'en connaître** : L'accès aux données patients via un appareil mobile (ou tout autre terminal) doit être strictement limité aux informations nécessaires à la prise en charge ou au suivi direct du patient par l'utilisateur dans le cadre de ses fonctions.

# Article 3 : Bonnes Pratiques d'Utilisation Quotidienne et Protection des Données Patients

## 3.1. Sécurité du Terminal :

* **Verrouillage Immédiat** : Activez impérativement et utilisez un mécanisme de verrouillage robuste (code PIN complexe, empreinte digitale, reconnaissance faciale). Le délai de verrouillage automatique doit être paramétré pour se déclencher très rapidement (quelques secondes à 1 minute maximum), afin d'éviter l'accès aux données en cas d'oubli de l'appareil. Verrouillez systématiquement votre session avant de vous éloigner de votre appareil, même brièvement, surtout dans les zones accessibles aux patients ou visiteurs.
* **Mises à jour** : Maintenez constamment le système d'exploitation et les applications (en particulier celles liées à l'accès aux données professionnelles) à jour.
* **Applications** : Installez uniquement des applications provenant des stores officiels. Soyez extrêmement prudent avec les autorisations demandées. Il est interdit d'installer des applications permettant un transfert non sécurisé de données (ex: applications de messagerie instantanée non validées par l'établissement pour un usage professionnel, applications de stockage cloud non autorisées).
* **Antivirus/Sécurité** : Si une solution de sécurité mobile est fournie ou recommandée par l'établissement, assurez-vous de son bon fonctionnement.

## 3.2. Protection des Données de Santé et Confidentialité :

* **INTERDICTION FORMELLE de Stocker des Données Patients** : Il est strictement interdit de stocker des données de santé à caractère personnel (noms de patients, numéros de dossier, résultats d'examens, diagnostics, photos cliniques non gérées par une application dédiée et sécurisée, etc.) directement sur la mémoire interne ou une carte mémoire de l'appareil mobile personnel, ou sur des services de stockage cloud personnels non autorisés.
* **Accès au DPI et applications Métiers** : L'accès au Dossier Patient Informatisé (DPI) et aux autres applications métiers contenant des données patients via un appareil mobile n'est autorisé qu'à travers les applications officielles et sécurisées déployées ou validées par l'établissement, et en respectant scrupuleusement le principe du "besoin d'en connaître".
* **Communication de Données Patients** : Il est strictement interdit de communiquer des informations patients (même anonymisées si elles permettent l'identification) via des canaux de communication non sécurisés et non validés par l'établissement pour cet usage (ex: SMS, applications de messagerie instantanée grand public comme WhatsApp, Messenger, etc., messagerie électronique personnelle). Utilisez uniquement les outils de communication professionnels sécurisés mis à disposition (messagerie professionnelle sécurisée, applications de communication validées).
* **Photos et Vidéos Cliniques** : La prise de photos ou de vidéos de patients (plaies, pathologies, examens, etc.) avec un appareil mobile personnel est FORTEMENT DÉCONSEILLÉE ET TRÈS RÉGLEMENTÉE, voire INTERDITE si l'établissement ne dispose pas d'une politique claire et d'outils sécurisés dédiés. Si de telles pratiques sont autorisées et encadrées (uniquement via des appareils professionnels et/ou des applications sécurisées dédiées) :
	+ Le consentement éclairé du patient (ou de son représentant légal) doit avoir été obtenu, documenté et traçable.
	+ Les photos/vidéos doivent être transférées immédiatement et de manière sécurisée vers le dossier patient informatisé ou un système de stockage sécurisé dédié, puis supprimées de l'appareil mobile dans les plus brefs délais.
	+ Ne JAMAIS stocker ces éléments dans la galerie photo/vidéo personnelle de l'appareil.
* **Manipulation en Public** : Évitez de consulter des informations patients sur votre appareil mobile dans des lieux publics ou potentiellement visibles par des tiers non autorisés (transports en commun, cafés, etc.).
* **Impression** : Évitez si possible d'imprimer des documents contenant des données patients depuis un appareil mobile. Si nécessaire, utilisez uniquement les systèmes d'impression sécurisés de l'établissement.

## 3.3. Connectivité et Accès Réseau :

* **Wi-Fi Public** : Soyez extrêmement prudent avec les réseaux Wi-Fi publics. Ne jamais accéder aux applications métier critiques ou manipuler des données patients via un réseau Wi-Fi public non sécurisé. Utilisez le réseau Wi-Fi interne sécurisé de l'établissement ou un VPN fourni par l'établissement.
* **Bluetooth** : Désactivez le Bluetooth lorsque vous ne l'utilisez pas. Soyez vigilant avec les demandes d'appairage inconnues.

## 3.4. Manipulation Physique et Signalement :

* **Perte ou Vol** : En cas de perte ou de vol de votre appareil mobile utilisé professionnellement, signalez-le IMMÉDIATEMENT au service informatique ou à la personne désignée. Le temps est critique pour initier les procédures de localisation, de verrouillage et d'effacement à distance des données professionnelles.
* **Ne pas laisser sans surveillance** : Ne laissez jamais votre appareil sans surveillance, même un court instant, dans l'enceinte de l'établissement ou à l'extérieur.
* **Signalement d'incidents** : Tout comportement suspect de l'appareil, message d'erreur inhabituel lié à la sécurité, suspicion de virus, tentative de hameçonnage (phishing), ou toute situation pouvant compromettre la sécurité ou la confidentialité des données (ex: consultation indue remarquée), doit être immédiatement signalé au service informatique ou au RSSI/référent sécurité.

# Article 4 : Règles Spécifiques au BYOD (Utilisation d'Appareils Personnels)

Si l'établissement autorise l'utilisation d'appareils personnels à des fins professionnelles (BYOD), les règles suivantes s'appliquent en sus des règles générales :

* L'utilisation d'un appareil personnel pour accéder aux ressources de l'établissement (notamment le DPI ou des données patients) est soumise à une validation formelle et à l'application de mesures de sécurité strictes (ex: installation obligatoire d'un agent de gestion de flotte mobile (MDM) ou d'un profil professionnel sécurisé).
* Vous consentez à ce que l'établissement puisse gérer et, si nécessaire, effacer à distance les données et applications contenues dans le "profil professionnel" ou le "conteneur sécurisé" dédié sur votre appareil personnel, notamment en cas de perte/vol, de suspicion de compromission ou de départ de l'établissement. Ces actions ne cibleront, dans la mesure du possible et des capacités techniques, que les données et applications professionnelles.
* Vous êtes responsable de la sécurité physique de votre appareil personnel et de sa conformité avec les exigences techniques minimales définies par l'établissement.

# Article 5 : Contrôle et Surveillance

L'établissement, en sa qualité de responsable de traitement (et dans le respect de ses obligations légales, notamment de traçabilité des accès aux données de santé), se réserve le droit de contrôler l'utilisation des appareils mobiles connectés à son réseau ou utilisés pour accéder aux ressources professionnelles. Ces contrôles sont effectués dans le strict respect de la vie privée des utilisateurs et de la réglementation en vigueur (RGPD, droit du travail, jurisprudence). La traçabilité des accès aux données patients via les applications métiers est une obligation légale.

# Article 6 : Non-respect de la Charte et Sanctions

Tout manquement aux règles énoncées dans la présente charte, particulièrement celles relatives à la confidentialité des données de santé et au secret médical, constitue une faute grave et expose l'utilisateur à des sanctions disciplinaires pouvant aller jusqu'au licenciement. En fonction de la gravité du manquement et des conséquences (par exemple, une violation de données de santé), l'utilisateur s'expose également à des poursuites pénales (violation du secret professionnel, accès frauduleux, etc.) et civiles, ainsi qu'à des conséquences hiérarchiques pour les professionnels de santé.

# Article 7 : Formation et Sensibilisation

Chaque utilisateur s'engage à participer aux actions de formation et de sensibilisation à la sécurité des systèmes d'information et à la protection des données organisées par l'établissement.

# Article 8 : Révision de la Charte

La présente charte pourra être modifiée ou complétée par l'établissement en fonction de l'évolution des techniques, de l'organisation, de la législation et des risques identifiés, notamment ceux liés aux appareils mobiles et à l'utilisation du numérique en santé.

#

# Article 9 : Prise d'Effet

La présente charte prend effet à compter du [Date].