



GUIDE POUR LA MISE EN ŒUVRE D'UNE STRATÉGIE « APPORTEZ VOTRE PROPRE APPAREIL » (BRING YOUR OWN DEVICE, BYOD) DANS LE CADRE DE LA NUMÉRISATION DES CAMPAGNES DE DISTRIBUTION DE MOUSTIQUAIRES IMPRÉGNÉES D'INSECTICIDE (MII)



CONTENTS

Glossaire	4
1. Contexte	5
1.1 Qu'est-ce que le BYOD dans les campagnes de MII ?	5
1.2 Préparation au BYOD	7
1.3 Modèles de stratégie relative aux appareils	8
1.4 Avantages et risques	9
1.5 Éléments à prendre en compte pour choisir une stratégie en matière d'appareils	10
2. Portée et cas d'utilisation du BYOD dans les campagnes de MII	13
2.1 Dans quels cas le système BYOD est-il approprié ou inapproprié ?	13
2.2 Évaluation de la faisabilité et du niveau de préparation au BYOD	15
3. Politique, confidentialité et sécurité	25
3.1 Élaboration de la politique BYOD	25
3.2 Définir les conditions d'utilisation acceptables et les responsabilités	25
3.3 Définir des contrôles minimaux de sécurité et d'accès	26
3.4 Mettre en place des règles de gouvernance et de stockage des données	26
3.5 Gestion des incidents liés à la perte, au partage ou à la compromission d'appareils	27
4. Mise en œuvre du BYOD	28
4.1 Dispositions de secours	28
4.2 Formation	28
4.3 Accompagnement et surveillance pendant la mise en œuvre	29
4.4 Contrôles opérationnels quotidiens	29
4.5 Désactivation du matériel après la campagne	30
5. Conclusion	31
Annexe 1 : Liste de contrôle pour l'évaluation de l'état de préparation au BYOD	32
Annexe 2 : Inscription au programme BYOD, vérification des appareils et formulaire de consentement	35
Annexe 3 : Modèle d'inventaire des appareils	38
Annexe 4 : Exemple de politique BYOD et de conditions d'utilisation pour les campagnes de MII	39

GLOSSAIRE

Terme	Définition
API	Interface de programmation d'applications (interface Android entre l'application et le serveur). Elle permet d'identifier les fonctions et les fonctionnalités disponibles dans une version spécifique du système d'exploitation.
« Apportez votre propre appareil » (BYOD)	Une politique autorisant les collaborateurs à utiliser leurs appareils personnels pour effectuer des tâches liées à la campagne, dans le cadre de dispositions bien définies en matière de gouvernance, de consentement et d'assistance.
Applications de la campagne (applications)	Outils numériques agréés utilisés dans le cadre des activités de la campagne de distribution de MII, notamment pour l'enregistrement des ménages, le suivi des distributions, les listes de contrôle de la supervision ou la gestion des stocks.
Analyse d'impact relative à la protection des données (AIPD)	Processus visant à identifier et à réduire le plus possible les risques liés à la protection des données associés à un projet, à un système ou à une activité de traitement des données.
GPS	Système de positionnement global
BYOD hybride	Un modèle dans lequel la mise en œuvre de la campagne repose sur une combinaison d'appareils personnels et d'appareils appartenant au programme.
Gestion des appareils mobiles (GAM)	Logiciel permettant à un programme de gérer, de surveiller et de contrôler à distance certains aspects des appareils enregistrés dans le cadre d'une campagne. Dans le cadre du BYOD, cela se limite généralement à des contrôles au niveau des applications.
Priorité au mode hors ligne	Une architecture d'application dans laquelle les fonctions essentielles et la saisie de données s'effectuent sans connexion internet active, les données étant synchronisées dès qu'une connexion est disponible.
Appareil appartenant au programme (POD)	Un appareil acheté et détenu par le programme, par un autre service du ministère de la Santé, par une autre entité gouvernementale ou par un partenaire de mise en œuvre, configuré et remis aux collaborateurs pour être utilisé dans le cadre de la campagne.
BYOD pur et simple	Un modèle dans lequel les collaborateurs de campagne utilisent leurs propres téléphones et cartes SIM à travers certaines phases et fonctions numérisées de la campagne
Effacement à distance	La possibilité de supprimer à distance les données de campagne d'un appareil.
Root (Android) et jailbreak (iOS)	Procédés permettant de lever les restrictions imposées par le fabricant ou l'opérateur, et d'accorder aux utilisateurs un accès « root » ou de niveau administrateur au système d'exploitation.
Accès basé sur les fonctions	Une approche de sécurité dans laquelle les utilisateurs ne peuvent accéder qu'aux données et aux fonctionnalités correspondant à la (aux) fonction(s) qui leur a (ont) été attribuée(s).
Synchronisation (sync)	Processus consistant à transférer des données stockées localement depuis un appareil vers un serveur central.
Données sans frais	Accès aux données mobiles pour une application spécifique qui n'utilise pas le forfait de données personnelles de l'utilisateur.

1. CONTEXTE

Le paludisme reste un défi majeur en matière de santé publique dans de nombreux pays où la maladie est endémique. Les moustiquaires imprégnées d'insecticide (MII) restent l'une des mesures les plus efficaces pour réduire la transmission du paludisme et prévenir la morbidité et la mortalité. Dans la plupart des pays où le paludisme est endémique, les campagnes de distribution massive de MII sont généralement menées à grande échelle et dans des délais très courts, afin d'améliorer rapidement l'accès des ménages à ces moustiquaires et de renforcer la protection contre le paludisme au niveau communautaire.

Les exigences opérationnelles de ces campagnes nécessitent des données actualisées, précises et exhaustives. Les délais de mise en œuvre serrés, le nombre important de travailleurs temporaires et la complexité de la logistique du « dernier kilomètre » nécessitent tous

des informations fiables pour faciliter la planification, la surveillance et la mise en œuvre de mesures correctives. La qualité et l'actualité des données sont donc essentielles au bon déroulement des campagnes.

La numérisation de certaines fonctions de campagne peut permettre de relever bon nombre de ces défis. Cependant, l'acquisition et la gestion de grandes quantités d'appareils mobiles standardisés sont coûteuses, prennent beaucoup de temps, et sont exigeantes sur le plan opérationnel. Dans de nombreux contextes, ces contraintes peuvent limiter la faisabilité ou l'évolutivité des campagnes entièrement numérisées. Une solution alternative pratique consiste à faire utiliser par les collaborateurs de la campagne leurs appareils mobiles personnels, une pratique communément appelée « Bring Your Own Device » (BYOD).

1.1 Qu'est-ce que le BYOD dans les campagnes de MII ?

Le BYOD est une stratégie qui permet aux collaborateurs de la campagne d'utiliser leurs appareils personnels, généralement des smartphones, pour effectuer des tâches liées à la campagne qui ont été approuvées. Dans le cadre de l'approche BYOD, les appareils personnels ayant fait l'objet d'une vérification (voir ci-dessous) sont temporairement enregistrés afin de pouvoir exécuter les applications de campagne approuvées. Les collaborateurs de la campagne accèdent aux outils et aux applications de collecte de données depuis les appareils qu'ils possèdent déjà et qu'ils savent utiliser.

Cette approche s'avère particulièrement utile lorsque les budgets alloués aux campagnes rendent difficile, d'un point de vue opérationnel, l'acquisition et la gestion de grandes quantités d'appareils appartenant au programme.

Au-delà des économies financières, il a été démontré que le BYOD permettait d'améliorer la productivité et la satisfaction des utilisateurs, car les collaborateurs sur le terrain peuvent effectuer leurs tâches sur des appareils qu'ils connaissent bien et avec lesquels ils se sentent à l'aise¹.

Plusieurs pays ont mis en œuvre le BYOD dans le cadre de campagnes de distribution de MII. Lors de la réunion de 2023 sur la numérisation des campagnes de l'APP, l'Ouganda a présenté son expérience en matière d'utilisation du BYOD² pour la numérisation des campagnes visant à assurer la couverture universelle en MII. Le Togo a rendu compte de l'utilisation d'appareils personnels lors de ses campagnes de distribution de masse de MII menées en 2020 et 2023, dans une étude de cas publiée sur le site internet de l'APP³. Ces expériences montrent

1. <https://www.tandfonline.com/doi/full/10.1080/08874417.2018.1543001>

2. https://allianceformalariaprevention.com/wp-content/uploads/2024/02/2.8-Rukaari-Medard_Uganda.pdf

3. <https://allianceformalariaprevention.com/resource-library/resource/digitalization-of-the-2020-and-2023-mass-itn-campaigns-in-togo-the-experience-of-bring-your-own-device-byod/>



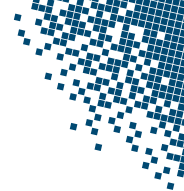
que le BYOD peut être viable sur le plan opérationnel dans le cadre de campagnes, à condition qu'il s'appuie sur des critères d'admissibilité clairs, une stratégie d'utilisation complète, des dispositions en matière de gestion des données et un parc d'appareils de prêt destinés aux travailleurs qui ne possèdent pas de smartphone compatible ou qui ne souhaitent pas utiliser le leur.

Ce guide fournit des recommandations pratiques et des considérations opérationnelles concernant le BYOD dans le cadre des campagnes de distribution de masse de MII. Il est destiné aux programmes nationaux de lutte contre le paludisme (PNLP), à leurs partenaires chargés de la mise en œuvre et du financement, ainsi qu'aux prestataires de services de santé numériques qui contribuent à la planification et à la mise en œuvre des campagnes de distribution de MII.

Les recommandations suivantes résument les principales mesures à prendre pour mettre en œuvre de manière sûre et efficace une stratégie BYOD ; elles sont développées plus en détail dans le guide :

- **Mettez en place une stratégie BYOD avant le début des inscriptions.** Définissez les conditions d'utilisation acceptables, les responsabilités des utilisateurs, les exigences en matière de protection des données, les normes de sécurité, les rétributions, la procédure de signalement des incidents et la responsabilité. Obtenez l'aval des responsables du ministère de la Santé et du programme national de lutte contre le paludisme (Ministère de la Santé/PNLP) et menez à bien l'examen juridique.
- **Définissez et faites respecter les normes minimales en matière d'équipements et de sécurité.** Vérifiez chaque appareil lors de son enregistrement. N'enregistrez pas les appareils qui ne répondent pas aux exigences.

- **Proposez des formations différenciées et pratiques, adaptées au niveau de maîtrise du numérique de chaque groupe d'utilisateurs.** Vérifiez les compétences avant la mise en œuvre. Veillez à ce qu'une assistance technique soit disponible tout au long de cette mise en œuvre.
- **Mettez en place des mesures de sécurité proportionnées.** Au minimum : connexion sécurisée, accès basé sur les fonctions, stockage chiffré, délai d'expiration de la session et possibilité de déconnexion à distance. Mettez en place des contrôles plus stricts pour les processus nécessitant une approche plus délicate.
- **Adoptez une approche hybride.** Le BYOD ne convient pas à toutes les fonctions de campagne ni à tous les utilisateurs. Réservez les appareils appartenant au programme aux processus à haut risque. Ayez en permanence un parc d'appareils de remplacement et une solution de secours sur papier ayant fait ses preuves, ou une solution alternative.
- **Veillez à ce que le BYOD n'entraîne pas de coûts injustifiés pour les collaborateurs.** Définissez les modalités relatives aux forfaits de données et aux conditions de compensation avant le début de la campagne, et communiquez-les clairement lors de la formation.
- **Suivez la mise en œuvre à l'aide d'indicateurs définis dès la phase pilote.** Adaptez le champ d'application, les mesures de protection ou le modèle de mise en œuvre en fonction des données disponibles. Il ne faut pas étendre à plus grande échelle une approche qui n'atteint pas les objectifs fixés pour la phase pilote.



1.2 Préparation au BYOD

La mise en place du BYOD doit être planifiée suffisamment tôt, afin de garantir qu'elle soit adaptée et qu'elle permette d'atteindre les résultats escomptés. La planification exige que les PNLP suivent les étapes suivantes dans l'ordre indiqué ; de plus amples détails à ce sujet sont fournis aux points suivants du guide :

- 1. Réalisez une étude de faisabilité concernant le BYOD et motivez les décisions prises :** Cela devrait permettre de déterminer si le BYOD est pertinent, dans quels contextes il peut être mis en œuvre et quelle approche adopter (point 2.2).
- 2. Définissez les spécifications techniques minimales requises pour les appareils utilisés dans le cadre de la campagne :** Celles-ci doivent tenir compte des besoins de l'application de la campagne et des normes minimales de sécurité requises (point 2.2.1).
- 3. Réalisez l'inventaire des appareils et classez les utilisateurs par niveau de préparation :** Cela permet de déterminer combien de collaborateurs disposent d'appareils adaptés, où se situent les lacunes et quelle serait la taille probable d'un parc d'appareils de prêt pour ceux qui n'en possèdent pas (point 2.2.1).
- 4. Vérifiez et assurez-vous que la plateforme choisie soit adaptée au BYOD :** La plateforme doit fonctionner sur les types d'appareils personnels prévus dans le cadre de la campagne, en particulier les téléphones Android courants. Les tests doivent porter sur un échantillon représentatif d'appareils réels, y compris des modèles d'entrée de gamme, et doivent permettre de vérifier le fonctionnement hors connexion, les résultats de synchronisation et la facilité d'utilisation dans les zones cibles (point 2.2.4).
- 5. Rédigez et validez la politique BYOD ainsi que les formulaires destinés aux utilisateurs :** Cela inclut les formulaires de prise de connaissance ou de consentement des utilisateurs rédigés dans les principales langues locales, selon les besoins (point 3 et annexes 2 et 4).
- 6. Calculez les besoins budgétaires et obtenez l'approbation :** Le BYOD permet de réduire les coûts d'acquisition des appareils, mais d'autres coûts opérationnels subsistent, que l'on utilise des appareils appartenant au programme ou des appareils personnels ; ils doivent donc être pris en compte dans le budget avant la mise en œuvre. Les coûts peuvent inclure la prise en charge des forfaits de données, le temps de communication, les appareils de prêt, les cartes SIM, les batteries externes, la formation et l'assistance technique (point 2.2.6).
- 7. Procurez-vous et configurez le parc d'appareils de prêt ainsi que les autres éléments de support nécessaires :** Cette démarche doit être effectuée suffisamment tôt pour faciliter les enrôlements, permettre la mise en place de solutions alternatives et garantir la pleine intégration des travailleurs.
- 8. Menez un projet pilote dans des circonscriptions représentatives et analysez les résultats avant la mise en œuvre :** Le pilote doit tester l'approche dans des conditions réalistes et évaluer ses résultats au regard des critères de mise à l'échelle convenus. Lorsque les critères convenus ne sont pas respectés, il convient de revoir le périmètre, les mesures de sécurité ou le modèle de mise en œuvre avant le lancement (point 2.2.8).

1.3 Modèles de stratégie relative aux appareils

Les campagnes de distribution de MII peuvent recourir à différentes stratégies en fonction du contexte. Si certains contextes peuvent se prêter à une mise en œuvre exclusivement « BYOD » ou exclusivement sur des appareils

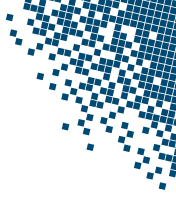
appartenant au programme (POD), la plupart des campagnes ont tout intérêt à adopter une approche hybride combinant les appareils personnels et un parc ciblé d'appareils fournis par le programme (tableau 1).

Tableau 1 : Modèles stratégiques relatifs aux appareils pour la numérisation des campagnes de distribution de MII

Modèle BYOD	Description	Idéal pour
Un BYOD pur et simple	Les membres de l'équipe de campagne utilisent leurs propres téléphones et cartes SIM à certaines étapes de la campagne et pour certaines tâches.	Le contexte caractérisé par un taux de pénétration élevé des smartphones, acteurs de mise en œuvre télécom bien établis, une connectivité fiable et des exigences moindres en matière de normalisation et de contrôle des appareils.
POD	Un appareil standardisé est acheté, configuré et remis à chaque collaborateur de campagne devant utiliser cet outil numérique. Tous les appareils appartiennent au programme et sont gérés tout au long de leur cycle de vie, y compris la distribution, la logistique inverse, le stockage et la maintenance entre les campagnes.	Les campagnes dans lesquelles le taux de possession de smartphones parmi le personnel de campagne cible est faible, celles où les exigences nationales en matière de protection des données limitent l'utilisation d'appareils personnels, celles où toutes les fonctions de la campagne nécessitent des contrôles de sécurité complets au niveau des appareils, ou encore celles où il est prévu de réutiliser les appareils au cours de plusieurs cycles de campagne et interventions.
Le BYOD hybride	La mise en œuvre de la campagne repose à la fois sur des appareils personnels et sur des appareils fournis dans le cadre du programme. Les appareils acquis dans le cadre de ce programme sont attribués dans les zones où le taux de possession de smartphones est faible ou lorsque davantage de standardisation, de fiabilité ou de sécurité est nécessaire.	La plupart des campagnes. Idéal pour les programmes qui souhaitent bénéficier des avantages du BYOD en termes de coûts et de familiarité, tout en réduisant les risques liés à la mise en œuvre et en garantissant une couverture pour les collaborateurs ou les fonctions qui ne peuvent pas compter uniquement sur leurs appareils personnels.

Les PNLP qui ont recours au BYOD devraient prévoir un petit parc d'appareils de prêt, représentant, par exemple, environ 5 à 10 % des effectifs concernés par le BYOD, afin de favoriser l'inclusion et d'assurer la continuité opérationnelle pour les collaborateurs dont les appareils ne répondent pas aux exigences minimales, ou qui

choisissent de ne pas utiliser leur appareil personnel dans le cadre de leurs missions. Dans la mesure du possible, ce parc de matériel de prêt peut être complété grâce à une coordination avec d'autres programmes de santé et d'autres partenaires, afin d'emprunter temporairement ou de réaffecter des appareils existants.



1.4 Avantages et risques

Le BYOD peut offrir des avantages opérationnels et financiers importants, mais uniquement lorsqu'il est adapté au contexte et que les risques associés sont gérés de manière proactive. Le rapport entre les avantages et les risques varie en fonction du contexte de la campagne ; les responsables de programme doivent donc évaluer ces deux aspects avant de décider s'il convient d'utiliser le BYOD et, le cas échéant, comment le mettre en œuvre.

Parmi les avantages potentiels, on peut citer :

- la réduction des coûts liés à l'achat, au stockage et à la distribution des appareils ;
- une mise en œuvre plus rapide, sans avoir à procéder à l'achat ni à la configuration d'un grand nombre d'appareils ;
- les collaborateurs utilisent des appareils qu'ils connaissent bien, ce qui peut réduire la courbe d'apprentissage et le temps de formation ;
- il permet une montée en puissance rapide sans logistique complexe liée aux équipements ;
- le fait d'être propriétaire de l'appareil peut inciter à en prendre davantage soin et à l'utiliser avec plus de précautions ;
- l'utilisation des applications de la campagne peut permettre de se familiariser avec le numérique en vue d'une utilisation future des programmes de santé ;
- il évite la collecte, le stockage et la maintenance des appareils après la campagne, ainsi que la charge liée aux déchets électroniques ;
- les supports de formation et les outils d'aide au travail peuvent être préinstallés sur les appareils des collaborateurs, et les mises à jour ainsi que les consignes de remise à niveau peuvent être facilement partagées au cours de la mise en œuvre, selon les besoins. Il peut s'agir de brefs rappels de formation ou de conseils de dépannage en cas de problème, qui peuvent tous être diffusés par le biais de canaux simples, tels que des liens vers YouTube ou d'autres plateformes numériques couramment utilisées ;

- cela pourrait permettre de réduire les dépenses liées au remplacement des appareils et des accessoires dans certains contextes.

Il convient toutefois de mettre en balance ces avantages et les risques potentiels, qui peuvent notamment inclure :

- des différences au niveau de la qualité des appareils et de leur compatibilité avec l'application de la campagne ;
- des questions d'équité, notamment celles liées au genre et à la fracture numérique au sens large, certains travailleurs ne disposant pas de smartphones adaptés ou n'ayant pas un accès égal aux outils numériques ;
- des risques liés à la protection des données lorsque des données à caractère personnel et des données de campagne coexistent sur un même appareil ;
- une responsabilité incertaine en cas de perte, de détérioration ou de compromission d'un appareil personnel ;
- des problèmes de connectivité et des échecs de synchronisation hors connexion ;
- des besoins d'accompagnement accrus et d'éventuels problèmes de qualité des données lorsque les compétences numériques sont limitées ;
- un risque d'accès non autorisé si les appareils sont partagés ou insuffisamment sécurisés ;
- des litiges concernant les primes ou les compensations peuvent survenir si les modalités ne sont pas clairement définies ;
- des différences entre les systèmes d'exploitation et les paramètres des appareils peuvent compliquer l'assistance technique.

D'autres risques ainsi que les mesures visant à les atténuer sont présentés au [point 2.2.9](#).

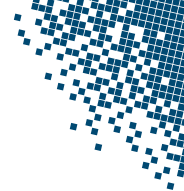
1.5 Éléments à prendre en compte pour choisir une stratégie en matière d'appareils

Avant d'opter pour une stratégie reposant sur un seul type d'appareil, les responsables des programmes de lutte contre le paludisme, ainsi que le personnel chargé des données, du suivi et de l'évaluation, et des technologies de l'information et de la communication (TIC), devraient comparer les modèles « BYOD pur », « POD complet » et « BYOD hybride » sur les principaux

aspects opérationnels et stratégiques pertinents pour leur campagne. Comme l'indique le tableau 1, le modèle hybride BYOD est celui recommandé par défaut pour la plupart des campagnes. Le cadre ci-dessous (tableau 2) a pour but d'aider les responsables de programme à confirmer ou à adapter ce modèle par défaut en fonction de leur contexte spécifique.

Tableau 2 : Cadre décisionnel pour le choix d'une stratégie en matière d'appareils

Dimension décisionnelle	Privilégie le BYOD	Privilégie le POD complet	BYOD hybride
Coût initial	Plus faible, car l'acquisition des appareils est coûteuse et le délai disponible pour les acquérir est souvent limité.	Ce coût diminuera au fil du temps, à mesure que les appareils seront réutilisés dans le cadre de plusieurs cycles de campagne et interventions.	Réduit le coût total d'approvisionnement en limitant les achats dans le cadre du programme à un sous-ensemble défini d'équipements destinés à être réutilisés dans différentes interventions et activités.
Délai d'acquisition	Avantage : aucun processus d'achat n'est nécessaire pour les appareils personnels.	Un délai est nécessaire pour l'acquisition, la configuration et la distribution de tous les appareils.	Moins long à mettre en place qu'un POD complet, car il nécessite l'acquisition et la configuration d'un nombre réduit d'appareils. Les programmes devraient tout de même prévoir un délai pour l'acquisition du parc de matériel de prêt.



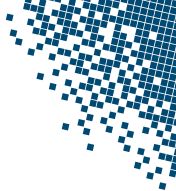
Dimension décisionnelle	Privilégie le BYOD	Privilégie le POD complet	BYOD hybride
Disponibilité des appareils	Cette solution n'est viable que si le taux de pénétration des smartphones est suffisamment élevé parmi les catégories de collaborateurs ciblées dans toutes les zones de campagne.	Garantit que chaque collaborateur enrôlé dispose d'un appareil compatible, qu'il s'agisse ou non de son appareil personnel.	Élargit la couverture en recourant aux appareils personnels lorsque leur taux de possession est élevé, et en affectant les appareils acquis dans le cadre du programme aux cadres, zones ou fonctions où le taux de possession de smartphones est faible ou là où une standardisation des appareils est nécessaire
La familiarité des travailleurs (avec leur appareil)	Les collaborateurs connaissent bien leurs propres appareils ; cela se traduit par une adoption plus rapide par les utilisateurs et une diminution des erreurs liées aux appareils lors des tâches courantes.	Un temps de formation supplémentaire est nécessaire pour se familiariser avec un appareil et un système d'exploitation inconnus.	Permet aux collaborateurs d'utiliser leurs appareils personnels en bénéficiant ainsi d'un environnement familier, tout en fournissant des appareils standardisés et des formations adaptées à certaines fonctions et à certaines zones géographiques.
Contrôle de la sécurité des données	Limites : le programme ne peut pas contrôler entièrement un appareil personnel. Les contrôles au niveau des applications constituent l'approche la plus réalisable.	Permet une gestion complète des appareils mobiles (GAM), le chiffrement et la configuration des appareils sous le contrôle du programme.	Applique des contrôles complets au niveau des terminaux aux appareils fournis par le programme et utilisés pour des processus à haut risque, tels que les paiements et l'administration du système. Les appareils personnels utilisés à d'autres fins sont soumis à des contrôles au niveau des applications.



Dimension décisionnelle	Privilégie le BYOD	Privilégie le POD complet	BYOD hybride
Responsabilité civile en cas de perte et de dommage	Cette situation peut prêter à confusion, à moins que la politique BYOD ne définisse clairement les responsabilités avant l'enrôlement.	Le programme prend en charge l'intégralité des frais liés à la perte et aux dommages subis par tous les appareils.	La responsabilité incombe au propriétaire de l'appareil. Les appareils fournis dans le cadre du programme sont pris en charge par le programme lui-même. Les appareils personnels sont soumis aux conditions définies dans la politique BYOD.
Gestion d'après-campagne	Il n'y a pas de logistique inverse pour les appareils, mais la désinstallation à distance de l'application et la suppression des données sont obligatoires et doivent être vérifiées.	Tous les appareils doivent être récupérés après chaque campagne, stockés en toute sécurité, entretenus et réutilisés pour les campagnes suivantes, le cas échéant.	C'est plus simple qu'un POD complet, car seuls les appareils appartenant au programme doivent être récupérés, stockés et entretenus. La désinstallation à distance des applications et la suppression des données sont obligatoires pour les appareils personnels.
Équité et inclusion	Risque d'exclusion pour certains travailleurs, notamment les femmes et les travailleurs âgés, qui ne disposent pas de smartphones compatibles.	Garantit un accès égal à tous, que l'on possède ou non son propre appareil.	Cette mesure répond directement au risque d'inégalité en attribuant les appareils achetés dans le cadre du programme aux collaborateurs qui ne possèdent pas de smartphone compatible, ou qui choisissent de ne pas participer au programme « BYOD ».

Il n'existe pas de modèle unique qui convienne à toutes les campagnes. Ce choix doit s'appuyer sur les résultats de l'inventaire des appareils ([point 2.2.1](#)), l'analyse des coûts ([point 2.2.6](#)) ainsi que sur l'évaluation de l'état de préparation du personnel, de la sensibilité des données et des risques opérationnels. Dans la plupart des contextes, le modèle hybride BYOD propose le meilleur équilibre entre rentabilité, inclusion et gestion des risques. Le modèle BYOD pur peut s'avérer approprié lorsque le taux de possession de smartphones est très

élevé et qu'aucune fonction de la campagne ne nécessite de mesures de sécurité renforcées. Il convient d'envisager une approche POD complète lorsque le taux de possession de smartphones au sein de la population cible est faible, lorsque les exigences nationales en matière de protection des données limitent le traitement des données sur les appareils personnels, ou lorsqu'il est prévu de réutiliser les appareils au cours de plusieurs cycles de campagne ou dans le cadre d'activités ou d'interventions différentes.



2. PORTÉE ET CAS D'UTILISATION DU BYOD DANS LES CAMPAGNES DE MII

2.1 Dans quels cas le système BYOD est-il approprié ou inapproprié ?

Le BYOD ne convient pas à toutes les campagnes, à toutes les fonctions ni à tous les lieux. Son utilisation dépend du contexte opérationnel, du profil du personnel, des exigences des systèmes numériques, de la capacité de l'équipe de gestion du programme à gérer les risques et de la conformité avec les politiques gouvernementales en matière de données. Les conséquences de la mise en œuvre du BYOD dans des conditions inadaptées vont au-delà des simples perturbations opérationnelles : si la collecte de données échoue en raison de l'incompatibilité des appareils ou de l'incapacité des collaborateurs à les utiliser efficacement, certains ménages risquent de ne pas être recensés et certaines familles pourraient ne pas recevoir les MII dont elles ont besoin.

Dans la plupart des campagnes de distribution de MII, le modèle BYOD est particulièrement adapté aux fonctions opérationnelles présentant un faible niveau de risque, telles que l'enregistrement des ménages, le suivi des distributions, ainsi que les activités de surveillance et de suivi, notamment lorsque le taux d'accès aux smartphones est élevé et que la connectivité est suffisante. Toutefois, le BYOD peut également être utilisé pour des activités impliquant des données à caractère personnel ou sensibles, à condition que des mesures de protection appropriées soient mises en place pour garantir la protection des données, leur sécurité et la responsabilité. La question essentielle n'est pas de savoir s'il s'agit de données à caractère personnel, mais si des contrôles suffisants

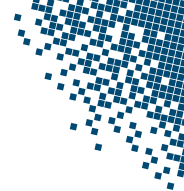
peuvent être mis en place concernant l'accès, le stockage et la transmission de ces données. Lorsque ces contrôles sont plus difficiles à garantir, ou lorsque des niveaux plus élevés d'assurance et de surveillance sont requis, les appareils gérés par le programme peuvent s'avérer plus adaptés.

L'adéquation peut également varier selon la région. Le BYOD est généralement plus facile à mettre en œuvre dans les zones urbaines et péri-urbaines, où la connexion internet est fiable, où l'on dispose de bornes de recharge électrique et où l'utilisation des smartphones est très répandue. Dans les zones rurales, isolées ou touchées par des conflits, où la couverture internet est insuffisante, les possibilités de recharge limitées ou le taux de pénétration des smartphones faible, il peut être plus approprié d'utiliser des appareils appartenant au programme ou d'adopter une approche hybride. Lorsque tous les critères et conditions d'adéquation définis ne peuvent pas être remplis, un modèle hybride constitue généralement la solution la plus pratique.

Avant d'adopter le BYOD, les programmes doivent vérifier si les conditions minimales en matière de technologie, de politique et de mise en œuvre sont réunies. Le tableau 3 présente un cadre simple permettant de réaliser cette évaluation.

Tableau 3 : Cadre d'évaluation de l'adéquation pour la mise en œuvre du BYOD

Recourez au BYOD dans les cas suivants :	Limitez ou évitez le BYOD dans les cas suivants :	N'utilisez pas le BYOD dans les cas suivants :
Le taux de possession de smartphones parmi les collaborateurs de campagne est suffisamment élevé pour couvrir la plupart des fonctions requises.	L'accès à des appareils adaptés est très inégal, et de nombreux cadres ne disposent pas de smartphones répondant aux exigences minimales.	L'appareil ne répond pas aux exigences minimales de sécurité (système d'exploitation débridé, sans verrouillage, pas de prise en charge du chiffrement, pas de verrouillage d'écran).
Les collaborateurs utilisent déjà leurs smartphones dans le cadre d'autres programmes de santé en ligne.	Les écarts en matière de compétence numérique risquent d'avoir un impact significatif sur la qualité de la mise en œuvre et la fiabilité des données.	La législation nationale ou l'Autorité chargée de la protection des données interdisent expressément le traitement des données concernées à l'aide d'appareils personnels.
Le fonctionnement hors connexion et la synchronisation ont été testés et validés.	Les problèmes de connectivité et de synchronisation risquent de compromettre l'exhaustivité ou la fiabilité des données.	Les tâches impliquant le stockage ou le traitement d'un grand nombre d'identifiants financiers ou de coordonnées bancaires doivent être effectuées à l'aide d'appareils appartenant au programme pour l'ensemble des processus de paiement.
Une assistance technique peut être fournie pour une large gamme d'appareils.	Les capacités du support technique sont trop limitées pour gérer efficacement la diversité des appareils.	Le programme ne peut proposer ni possibilité de se désinscrire ni d'indemnisation raisonnable pour l'utilisation d'appareils personnels.
Les délais ou les budgets rendent impossible l'acquisition à grande échelle d'appareils appartenant aux programmes.	Les risques liés à la sécurité ne peuvent pas être réduits à un niveau acceptable avec les ressources disponibles.	
Les mesures minimales de sécurité et de protection des données peuvent être appliquées de manière cohérente.	Les données hautement sensibles ne peuvent pas être suffisamment limitées, protégées ou isolées sur des appareils personnels.	
Un cadre clair en matière d'incitations, de rétribution et de responsabilité est en place.	Certaines exigences politiques, juridiques ou de gouvernance restent en suspens.	



2.2 Évaluation de la faisabilité et du niveau de préparation au BYOD

Le BYOD ne devrait pas être adopté par défaut. Avant d'opter pour le BYOD comme mode de mise en œuvre de leur campagne, les PNLP doivent évaluer le parc d'appareils, l'état de préparation des applications, les contraintes de connectivité, les exigences légales et en matière de protection des données, les implications en termes d'inclusion du personnel, la capacité d'assistance et le risque global lié à la mise en œuvre. Lorsque des failles importantes sont identifiées, il convient de les combler avant la mise en œuvre ou, à défaut, d'opter pour une approche hybride ou reposante sur un dispositif propre au programme.

Dans la pratique, l'évaluation devrait débuter dès la phase de planification globale, et non après que la plateforme de campagne a déjà été choisie. L'annexe 1 présente une liste de contrôle permettant d'évaluer l'état de préparation au BYOD, qui couvre les principaux domaines à examiner lors de la planification globale.

2.2.1 Panorama des appareils et configuration minimale requise

Une évaluation BYOD doit commencer par un inventaire des appareils dont disposent les collaborateurs de la campagne, et par la vérification de la compatibilité de ces appareils avec l'application de la campagne. Le simple fait de posséder un smartphone ne suffit pas. Les

PNLP doivent utiliser le formulaire d'inscription et de consentement BYOD (annexe 2) pour recueillir des informations de base sur le type d'appareil, le modèle, le système d'exploitation, la capacité de stockage, la batterie, le GPS, l'appareil photo et l'état du verrouillage de l'écran, puis classer les utilisateurs par zone et par fonction en les qualifiant d'« entièrement compatibles », de « compatibles sous certaines conditions » ou de « non compatibles ». L'annexe 2, section 2 (Inventaire des appareils et vérification des spécifications) constitue un exemple d'inventaire des utilisateurs et de vérification de la compatibilité.

Les utilisateurs qui ne remplissent pas les conditions minimales requises devraient bénéficier d'un dispositif de prêt d'appareils ou d'une solution alternative. Le tableau 4 présente les exigences minimales indicatives en matière d'appareils pour la participation au programme BYOD, sur la base des exigences fonctionnelles courantes observées dans les outils de collecte de données pour les campagnes numériques et des spécifications types nécessaires pour garantir la compatibilité, la facilité d'utilisation et la sécurité des données lors des opérations sur le terrain. Les seuils définitifs doivent être confirmés lors de la planification de la campagne, en fonction de l'application choisie.

Tableau 4 : Exemple de configuration minimale requise pour les appareils dans le cadre du programme BYOD

Caractéristiques techniques	Conditions minimales requises	Remarques
Système d'exploitation	Android 8.0 ou version ultérieure (niveau API 26 ou supérieur) ou iOS 13 ou version ultérieure	Vérifiez le niveau d'API exact auprès du développeur de l'application.
RAM	2 Go	Les appareils dotés de 1 Go peuvent ouvrir l'application, mais risquent de planter en conditions réelles d'utilisation.
Espace de stockage interne disponible	2 Go au minimum avant l'installation de l'application	Cela devrait comprendre l'application, le cache de données hors connexion pour 2 à 3 jours et les pièces jointes multimédias.



Caractéristiques techniques	Conditions minimales requises	Remarques
Capacité de la batterie	Suffisante pour une journée de travail complète (6 à 8 heures au minimum)	Évaluez l'état réel de la batterie, et pas seulement sa capacité initiale indiquée.
Taille de l'écran	5 pouces au minimum	Les écrans plus petits compliquent la navigation et augmentent le risque d'erreurs lors de la saisie de données.
GPS	Obligatoire lorsque l'application collecte des données de localisation	Vérifiez que le seuil de précision GPS est acceptable, généralement dans une fourchette de 20 mètres.
Appareil photo	Obligatoire lorsque l'application utilise la lecture de codes QR ou de codes-barres	Testez sur des modèles courants d'appareils d'entrée de gamme dans la zone de la campagne.
Chiffrement	L'appareil prend en charge le chiffrement au niveau des applications ou le chiffrement complet	Le chiffrement complet est activé par défaut sur Android 6.0 et versions ultérieures, ainsi que sur iOS 8 et versions ultérieures.
Sécurité	Verrouillage de l'écran activé	L'absence de verrouillage d'écran constitue un critère d'exclusion absolu.
Sécurité	Appareil non débridé, quel que soit le système d'exploitation	Les appareils débridés constituent un critère d'exclusion absolu.

2.2.2 Faisabilité sur le plan juridique, politique et en matière de protection des données

Il convient d'examiner dès le début la faisabilité juridique et politique. Si la législation nationale, la politique du ministère ou les règles du programme n'autorisent pas le traitement des données concernées sur des appareils personnels, le BYOD ne doit pas être utilisé.

Les responsables de programme devraient :

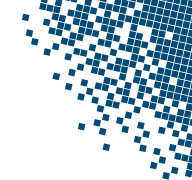
- examiner la réglementation nationale en matière de protection des données et de données de santé ;
- vérifier si l'utilisation d'appareils personnels est autorisée ;
- identifier les éventuelles exigences en matière de localisation des données ou d'hébergement ;
- classer les données de campagne en fonction de leur niveau de sensibilité ;

- réaliser une analyse d'impact relative à la protection des données lorsque des données présentant un risque élevé sont concernées.

Lorsque les données GPS sont susceptibles de présenter un risque, notamment dans des contextes de conflit ou des zones sensibles, les programmes doivent réduire leur précision, en restreindre l'accès, éviter la localisation au niveau des ménages ou se conformer à d'autres politiques nationales ou régionales, le cas échéant.

2.2.3 Équité, inclusion et mécanismes de dérogation

Le BYOD ne doit pas créer ni renforcer les inégalités en matière de participation à la campagne. Le niveau de préparation doit être évalué en fonction du sexe, de la tranche d'âge, de la catégorie professionnelle et de la zone géographique. Dans de nombreux contextes, les femmes bénévoles et les travailleurs âgés affichent des taux de possession de smartphones et de maîtrise du numérique plus faibles.



- La participation au programme BYOD doit être véritablement volontaire ; les collaborateurs ne doivent pas être pénalisés s'ils refusent d'utiliser un appareil personnel.
- Il faut toujours prévoir une solution alternative viable, comme un appareil de prêt fourni par le programme ou une fonction ne nécessitant pas l'utilisation d'un appareil personnel (BYOD) dans le cadre de la campagne.
- Les mécanismes d'incitation ne doivent pas être conçus de manière à obliger les participants à prendre part au programme ; la participation au programme BYOD doit être dissociée des conditions d'admissibilité à la rétribution.
- Il convient de prévoir dans le budget et de constituer à l'avance un parc d'appareils de prêt couvrant au moins 5 à 10 % des effectifs concernés par la politique BYOD.

2.2.4 Connectivité, possibilité de fonctionnement hors connexion et compatibilité avec le plates-forme

La planification doit se fonder sur les conditions de terrain les plus défavorables prévues, et non sur la couverture moyenne du réseau.

- Vérifiez la connectivité par zone de campagne et testez les résultats de synchronisation dans des zones représentatives à faible connectivité.
- L'application doit fonctionner entièrement hors connexion pour tous les processus essentiels. La capacité de stockage local doit être suffisante pour stocker au moins deux à trois jours de dépôt de données sans synchronisation.
- Définissez les points de synchronisation (établissements de santé, écoles, bureaux de district) ainsi que la fréquence de synchronisation prévue, au moins une fois par jour pendant la phase active de distribution.
- Vérifiez que le mécanisme de prévention des doublons fonctionne en mode hors connexion, et pas uniquement lorsque l'appareil est connecté.

- Les responsables doivent pouvoir identifier les appareils qui ne se sont pas synchronisés dans le délai prévu ; il s'agit d'une fonctionnalité obligatoire pour le tableau de bord de suivi.

La plateforme doit être testée sur les types d'appareils que possèdent effectivement les membres des équipes de campagne, y compris les modèles Android d'entrée de gamme courants dans de nombreux contextes.

2.2.5 Dispositions en matière de sécurité et d'assistance

Dans la plupart des contextes de campagnes de MII, les mesures de sécurité au niveau des applications, notamment le chiffrement, l'authentification et la dé-authentification à distance, associées à une surveillance opérationnelle rigoureuse, constituent l'approche la plus viable.

Au minimum :

- Les appareils ayant été modifiés afin de contourner les contrôles de sécurité standard du système d'exploitation (appareils Android ou iPhones débridés) ne devraient pas être autorisés.
- Les données de campagne ne doivent pas être exportées vers des applications personnelles. Des mesures techniques appropriées devraient être mises en œuvre pour empêcher ou limiter ces exportations, dans la mesure du possible.
- Le verrouillage de l'écran doit être activé sur les appareils.
- L'accès doit être défini selon les fonctions.
- Les sessions des utilisateurs devraient expirer automatiquement en cas d'inactivité.

Un parc hétérogène d'appareils personnels impose des exigences plus élevées au service d'assistance technique qu'un parc de POD standardisé. Une structure d'accompagnement à plusieurs niveaux devrait être mise en place avant la mise en œuvre.

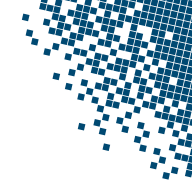
2.2.6 Considérations relatives aux coûts

Le BYOD permet, certes, de réduire les coûts d'acquisition des appareils, mais il ne supprime pas pour autant les coûts liés au programme. Les programmes devraient comparer le coût total du BYOD à celui des appareils apparte-

nant au programme, plutôt que de se concentrer uniquement sur le coût d'achat des smartphones. Le tableau 5 présente une comparaison des coûts entre les deux approches.

Tableau 5 : Comparaison des coûts entre le BYOD et les appareils fournis par le programme (POD)

Type de frais	Approche BYOD	Approche POD	Niveau de variation des ressources (BYOD par rapport à POD)
Acquisition d'appareils	Cela n'entraîne aucun coût direct pour le programme.	Coût intégral pris en charge par le programme.	Inférieur
Forfaits de données/temps de communication	Indemnité, allocation ou remboursement au titre de la campagne.	Le programme fournit des cartes SIM et des forfaits de données pour tous les appareils.	Idem
Assistance technique	Plus élevé, en raison de la diversité des types d'appareils et de leurs configurations.	Moins élevé, car les appareils sont standardisés et préconfigurés.	Plus élevé
Formation	Légèrement plus élevé, car la variabilité des appareils accroît les besoins en formation.	Plus standardisé, car tous les appareils sont identiques.	Plus élevé
Perte ou détérioration de l'appareil	Responsabilité définie par la politique en vigueur ; indemnisation généralement limitée.	Le coût total du remplacement est pris en charge par le programme.	Inférieur
Récupération après la campagne	Aucune collecte d'appareils n'est requise ; l'accès à la campagne et les données doivent être supprimés.	Les appareils sont récupérés après chaque campagne, stockés, entretenus et réutilisés pour d'autres campagnes, le cas échéant.	Inférieur
Gestion des appareils/licences	Généralement limité aux contrôles au niveau de l'application, ce qui réduit les coûts.	Une gestion complète des appareils peut s'avérer nécessaire, ce qui entraîne des coûts plus élevés.	Inférieur
Parc d'appareils de prêt	Généralement requis pour 5 à 10 % des effectifs.	Ce n'est généralement pas obligatoire, mais un stock de réserve est nécessaire pour la mise en œuvre.	Inférieur
Gestion des déchets électroniques	Ne s'applique pas à ce programme.	Obligatoire à la fin de la durée de vie de l'appareil.	Inférieur



2.2.7 Remboursement et rétribution

Les collaborateurs ne devraient pas avoir à financer la numérisation de la campagne sur leurs propres moyens. Les modalités de rétribution doivent être définies avant le début de la mise en œuvre :

- des cartes SIM avec forfait de données pré-chargé remises lors de la formation ;
- une allocation forfaitaire journalière pour les données ou un montant fixe versé au titre du travail effectué, en plus des autres rétributions liées à la campagne ;
- un accès à internet sans frais de données pour la plateforme de campagne, ce qui nécessite des négociations avec l'opérateur national de télécommunications et est réalisable dans certains pays.

2.2.8 Décision relative à la phase pilote et à la mise à l'échelle

Le BYOD devrait faire l'objet d'un projet pilote avant d'être mis en œuvre à plus grande échelle, en particulier lorsqu'il est utilisé pour la première fois ou lorsque la connectivité et la qualité des appareils varient d'un site à l'autre. Les sites pilotes doivent refléter les principales conditions de mise en œuvre prévues dans le cadre de la campagne. Le programme ne devrait être étendu que lorsque le projet pilote aura démontré que :

- la plupart des utilisateurs BYOD enrôlés peuvent collecter des données valides ;
- la synchronisation s'effectue dans les délais prévus ;
- l'exhaustivité des données est acceptable ;
- les problèmes techniques peuvent être résolus rapidement ;
- le recours au format papier ou aux appareils appartenant au programme reste limité.

Lorsque les résultats des projets pilotes mettent en évidence des lacunes importantes, celles-ci doivent être comblées avant de généraliser le programme BYOD ou d'en réduire la portée.

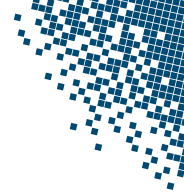
2.2.9 Évaluation des risques et plan d'atténuation

L'utilisation d'appareils personnels comporte des risques opérationnels, techniques et liés à la protection des données qui doivent être identifiés et gérés dès le début. Ces risques doivent être évalués lors de la phase de planification, et des mesures concrètes d'atténuation doivent être mises en place avant la mise en œuvre. Le tableau 6 ci-dessous présente un aperçu des risques courants liés au BYOD ainsi que les mesures d'atténuation recommandées.

REMARQUE : Le tableau des risques et des mesures d'atténuation est également reproduit sous forme de fichier Excel, sous la forme d'un outil adaptable joint en annexe au document. Cet outil peut être téléchargé et adapté par les PNLP qui envisagent de mettre en place une stratégie BYOD afin d'étayer leur évaluation des risques et leur plan d'atténuation.

Tableau 6 : Principaux domaines de risque liés au BYOD, priorités et mesures d'atténuation
(également disponibles sous forme d'outil adaptable dans Excel)

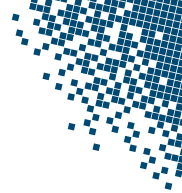
Catégorie	Zone à risque	Exemple de risque	Mesures d'atténuation
Technique	Compatibilité des appareils	Les appareils personnels ne répondent pas aux exigences minimales requises pour les applications	Définissez les spécifications minimales des appareils ; réalisez un inventaire et une vérification des appareils avant leur mise en œuvre ; gardez en réserve un parc d'appareils de prêt
Technique	Capacités de l'appareil	Autonomie réduite, capacité de stockage limitée, plantages d'applications ou précision GPS insuffisante	Testez l'application sur les principaux types d'appareils ; exigez une mémoire vive et un espace de stockage minimums ; fournissez des conseils sur la recharge ou proposez des batteries externes lorsque cela est possible
Technique	Assistance technique	La coexistence de différents types d'appareils entraîne davantage de besoins d'assistance que prévu	Mettez en place un système d'assistance à plusieurs niveaux ; rédigez des guides de dépannage ; formez les responsables à la résolution des problèmes courants
Technique	Stabilité de la plateforme	Une défaillance de la plateforme perturbe la mise en œuvre de la campagne	Testez la plateforme avant sa mise en œuvre ; définissez les procédures de remontée (escalade) ; assurez le suivi de l'assistance assurée par le fournisseur et mettez en place des solutions de secours



Catégorie	Zone à risque	Exemple de risque	Mesures d'atténuation
Opérationnel	Connectivité et synchronisation	Une couverture réseau insuffisante ralentit la synchronisation et nuit au suivi en temps réel	Utilisez des applications fonctionnant par priorité hors connexion ; définissez des points et des calendriers pour la synchronisation ; mettez en place un suivi par un responsable pour les appareils non synchronisés ; prévoyez un système de secours sur papier ou utilisation d'appareils appartenant au programme (POD) si nécessaire
Opérationnel	Qualité des données	Un niveau de maîtrise du numérique insuffisant ou des workflows peu familiers entraînent des soumissions de données incomplètes ou inexactes	Proposez des formations pratiques adaptées aux différentes fonctions ; simplifiez les formulaires ; recourez à la validation intégrée à l'application et au branchement conditionnel ; renforcez le contrôle par les superviseurs
Opérationnel	Doublons et fraude	Envois de données multiples pour un même ménage ou des entrées non autorisées	Utilisez des identifiants uniques, des contrôles anti doublons, des moyens de vérification et une revue par un superviseur ; recourez à la validation du côté du serveur, dans la mesure du possible
Opérationnel	Signalement des incidents	La perte d'un appareil, son utilisation abusive ou les problèmes techniques ne sont pas signalés assez rapidement	Mettez en place une procédure claire de signalement des incidents ; formez les utilisateurs et les superviseurs aux étapes de signalement des incidents ; diffusez largement les coordonnées des services d'assistance



Catégorie	Zone à risque	Exemple de risque	Mesures d'atténuation
Sécurité	Protection des données et vie privée	Les données à caractère personnel et celles liées à la campagne coexistent sur le même appareil, ce qui augmente le risque d'accès non autorisé ou de partage non autorisé	Utilisez une connexion sécurisée, un accès selon les fonctions et le chiffrement ; limitez l'exportation des données ; exigez le verrouillage de l'écran ; établissez des directives claires concernant l'utilisation acceptable
Sécurité	Perte ou vol de l'appareil	Un appareil contenant des données de campagne est perdu, volé ou remplacé au cours de la mise en œuvre	Exigez le signalement immédiat des incidents ; autorisez la désactivation à distance ou l'effacement des données, lorsque cela est possible ; limitez le stockage local des données ; vérifiez les appareils de remplacement avant leur utilisation
Sécurité	Utilisation partagée des appareils	Les membres du ménage ou d'autres utilisateurs accèdent à l'application de la campagne ou aux données depuis un téléphone partagé	Exigez la création de comptes utilisateurs individuels ; interdisez le partage de comptes ; évaluez si le modèle BYOD est adapté lorsque l'utilisation d'appareils privés ne peut être garantie
Sécurité	Configuration non sécurisée de l'appareil	Les appareils débridés contournent les contrôles de sécurité	Interdisez l'utilisation d'appareils débridés pour le programme BYOD ; vérifiez l'état de l'appareil lors de son inscription
Sécurité	Données résiduelles d'après-campagne	Les données de la campagne restent stockées sur les appareils personnels une fois la campagne terminée	Mettez en place une procédure de clôture ; désactivez les comptes ; effacez les données locales si nécessaire ; effectuez des contrôles ponctuels lorsque cela est possible
Sécurité	Données de localisation sensibles	Les données GPS exposent les ménages vivant dans des zones touchées par des conflits ou politiquement sensibles	Réduisez la précision du GPS lorsque cela s'avère nécessaire ; limitez l'exportation des données de localisation ; évaluez les risques par zone avant la mise en œuvre



Catégorie	Zone à risque	Exemple de risque	Mesures d'atténuation
Aspects juridiques et gouvernance	Gouvernance et responsabilité	Responsabilité mal définie en cas d'incidents liés aux appareils, de violations des règles ou de non-conformité	Définissez les responsabilités des utilisateurs, les procédures de signalement des incidents et les conséquences en cas de non-respect dans une politique BYOD simple
Aspects juridiques et gouvernance	Conformité réglementaire	Le traitement des données des ménages sur des appareils personnels est soumis à des restrictions prévues par la législation nationale ou imposées par les autorités nationales	Examinez dès le début les exigences légales ; réalisez une analyse d'impact relative à la protection des données (AIPD), le cas échéant ; consultez les autorités compétentes ; limitez la collecte de données à caractère personnel au strict minimum nécessaire à l'opération
Aspects juridiques et gouvernance	Fonctions à haut risque	Les opérations sensibles, telles que les paiements groupés ou l'administration du système, sont effectuées sur des appareils personnels	Limitez les fonctions à haut risque aux appareils appartenant au programme et contrôlés par celui-ci
Équité/ Ressources humaines	Équité et inclusion	Certains collaborateurs ne possèdent pas de smartphone adapté ou préfèrent ne pas utiliser leurs appareils personnels	Rendez le BYOD facultatif ; fournissez des appareils appartenant au programme ou prêtés ; recourrez à une mise en œuvre hybride si nécessaire
Équité/ Ressources humaines	Contrainte ou pression injustifiée visant à obliger quelqu'un à participer	Les collaborateurs se sentent contraints d'utiliser leurs appareils personnels pour pouvoir continuer à travailler ou à percevoir leur rétribution	Distinguez la participation au programme BYOD de l'éligibilité au paiement ; proposez des options de désinscription ; communiquez clairement la politique lors de la formation



Catégorie	Zone à risque	Exemple de risque	Mesures d'atténuation
Équité/ Ressources humaines	Compréhension des politiques BOYD en vigueur	Les collaborateurs ne comprennent pas pleinement les conditions ni les responsabilités liées au BYOD	Utilisez un langage simple et des expressions adaptées au contexte local ; organisez des exposés oraux et vérifiez la compréhension des participants tout au long de la formation
Finances/ développe- ment durable	Mesures d'incitation et remboursement	Les collaborateurs doivent supporter des frais liés aux données ou à la recharge et se sentent traités de manière injuste	Définissez des modalités de rétribution claires avant le lancement ; fournissez des forfaits de données, des allocations ou d'autres formes de soutien
Finances/ développe- ment durable	Prévisions concernant le remplacement des appareils	Les collaborateurs s'attendent à ce que ce programme remplace leurs appareils personnels endommagés ou perdus	Définissez et communiquez une politique claire en matière de remplacement, de réparation et d'indemnisation avant la mise en œuvre
Finances/ développe- ment durable	Accessibilité financière à long terme	Les indemnités « BYOD » accordées dans le cadre d'une campagne ne sont pas fixées une fois pour toutes pour les campagnes futures	Définissez des niveaux de soutien réalistes ; justifiez les hypothèses de coûts ; accordez-vous sur la budgétisation à long terme du programme
Réputation	Confiance de la communauté	Les communautés s'inquiètent d'une éventuelle utilisation abusive des données lorsque les acteurs utilisent leurs téléphones personnels	Menez des actions de sensibilisation au sein de la communauté ; utilisez des modèles de demande de consentement clairs et des messages relatifs à la protection de la vie privée ; surveillez les rumeurs et répondez-y rapidement

3. POLITIQUE, CONFIDENTIALITÉ ET SÉCURITÉ

Cette partie définit le cadre de gouvernance régissant l'utilisation des appareils personnels dans le cadre des campagnes de MII. Ce document traite de l'élaboration d'une politique relative au BYOD, qui devrait, dans l'idéal, concorder avec les politiques du ministère de la Santé lorsqu'elles existent et être adaptée, si nécessaire, aux exigences spécifiques d'un pro-

gramme ou d'une campagne. Cela comprend les règles d'utilisation acceptable, les normes de sécurité, la gouvernance des données et la gestion des incidents. Une gouvernance claire permet de protéger les données de la campagne, les travailleurs et les communautés auxquelles celle-ci s'adresse.

3.1 Élaboration de la politique BYOD

Une politique BYOD définit les conditions dans lesquelles les appareils personnels peuvent être utilisés dans le cadre du travail lié à la campagne. Elle doit être rédigée, approuvée par la direction du PNLP, faire l'objet d'un examen juridique si nécessaire, et être mise à disposition dans les principales langues utilisées dans la zone de campagne avant le début des inscriptions. Un exemple de politique et de conditions d'utilisation figure à l'[annexe 4](#).

La politique devrait, au minimum, définir :

- qui peut participer et quels sont les appareils et les fonctionnalités de la campagne concernés ;
- ce que les utilisateurs ont le droit de faire et ce qu'ils n'ont pas le droit de faire sur leurs appareils personnels utilisés dans le cadre de leur travail de campagne ;

- les exigences minimales en matière d'équipement et de sécurité ;
- les exigences relatives au traitement des données, notamment en matière de stockage, de transmission, de conservation et de suppression ;
- les dispositions relatives à l'assistance, à l'indemnisation et à la responsabilité ;
- les procédures de signalement des incidents et d'intervention ;
- les conséquences en cas de non-respect.

La politique doit être expliquée oralement lors de la formation, et non pas simplement communiquée par écrit pour signature. Les collaborateurs doivent bien comprendre les règles et les implications du BYOD avant que leur inscription ne soit finalisée.

3.2 Définir les conditions d'utilisation acceptables et les responsabilités

Les utilisateurs ne peuvent utiliser leurs appareils personnels que dans le cadre de missions approuvées. Cela implique notamment d'utiliser les applications approuvées par le programme pour les tâches qui leur sont confiées, de communiquer avec leurs responsables par les canaux autorisés, et d'accéder aux supports de formation ou de référence approuvés. La

prise de photos à des fins de campagne n'est pas recommandée et ne devrait être autorisée que si elle a été expressément approuvée et si des procédures de consentement sont en place.

Les utilisateurs ne doivent pas copier, exporter ou partager les données de campagnes en dehors des canaux autorisés, notamment par le biais de



leur messagerie électronique personnelle, de leur espace de stockage personnel dans le cloud ou d'applications de messagerie personnelles. Ils ne doivent pas réaliser de captures d'écran des données d'un membre de la communauté, ni partager des identifiants de connexion ni permettre à des personnes non autorisées d'accéder aux applications de campagne.

Les agents devraient se voir remettre, lors de leur formation, un modèle de texte standard pour obtenir le consentement oral, et devraient être capables d'expliquer aux ménages, avec leurs propres mots, quelles informations sont collectées, pourquoi elles sont nécessaires et qui y aura accès. En participant au programme BYOD, les utilisateurs s'engagent à respecter les responsabilités suivantes : assurer la sécurité et la mise à jour de leur appareil, traiter les

données des campagnes conformément aux règles du programme, signaler immédiatement tout incident, coopérer avec les instances de contrôle du programme, et traiter les données des membres de la communauté avec respect. La participation au programme BYOD devrait rester facultative. Les collaborateurs qui choisissent de ne pas participer ne devraient pas être pénalisés et devraient pouvoir bénéficier d'une solution alternative.

La direction du programme exerce également des responsabilités. Elle doit communiquer clairement les règles relatives au BYOD, proposer une formation initiale et un accompagnement, appliquer la politique de manière cohérente et protéger autant que possible la vie privée des collaborateurs, tout en garantissant la sécurité des données de la campagne.

3.3 Définir des contrôles minimaux de sécurité et d'accès

Tous les appareils utilisés dans le cadre du BYOD doivent répondre à des exigences minimales en matière de sécurité. Les appareils doivent disposer au minimum d'un verrouillage d'écran activé, ne doivent pas être débriés, doivent respecter les critères requis en matière de système d'exploitation, et l'application de la campagne ne doit être installée qu'à partir d'une source approuvée. Le chiffrement doit être activé lorsque cette fonctionnalité est prise en charge. Voir la fiche technique de l'appareil et la liste de contrôle de vérification figurant à l'[annexe 2](#).

Des contrôles d'accès minimaux devraient également être mis en place. Ces mesures doivent notamment inclure l'authentification

des utilisateurs pour l'application de campagne, un accès basé sur les fonctions, afin que les utilisateurs ne voient que les données et les fonctionnalités dont ils ont besoin, une expiration automatique de la session en cas d'inactivité, ainsi que la désactivation immédiate de l'accès lorsqu'un utilisateur quitte la campagne ou qu'un appareil est corrompu.

Les comptes de campagne ne doivent pas être partagés entre plusieurs utilisateurs. Lorsqu'un appareil est partagé au sein d'un ménage, le mode BYOD ne doit être utilisé que si l'application de la campagne et le compte restent accessibles uniquement à l'utilisateur inscrit. Si cela ne peut être garanti, il convient de trouver une autre solution.

3.4 Mettre en place des règles de gouvernance et de stockage des données

Les PNLP ne doivent collecter que les données nécessaires au bon déroulement des campagnes. Pour chaque champ du formulaire proposé, demandez-vous quelle décision ou action spécifique du programme nécessite ces données. Supprimez tout champ pour lequel il n'existe pas de réponse opérationnelle claire ou

dont les données seront utilisées uniquement à des fins de rédaction de rapports.

Les PNLP doivent préciser quelles données sont collectées, combien de temps celles-ci restent stockées sur l'appareil avant la synchronisation, à quel moment les données locales

doivent être effacées, et qui est autorisé à exporter ou à consulter les ensembles de données après la campagne.

Les données de la campagne comprennent toutes les données à caractère personnel, sensibles et opérationnelles collectées dans le cadre des activités du programme. Les données doivent être stockées dans le conteneur chiffré de l'application et synchronisées automatiquement avec le serveur dès qu'une connexion est disponible. Les données ne doivent pas être conservées sur l'appareil au-delà de ce qui est nécessaire d'un point de vue opérationnel ; la durée maximale recommandée est de 72 heures après la dernière synchronisation réussie. Les collaborateurs ne doivent pas sauvegarder les données de campagne sur leurs comptes cloud personnels, et

les paramètres des applications doivent empêcher cela dans la mesure du possible. Moins il y a de données stockées sur l'appareil à un moment donné, plus le risque est faible en cas de perte, de partage ou de falsification de celui-ci.

Lorsque cela est possible, il convient de définir une procédure de désactivation ou d'effacement à distance des données de la campagne. Cette disposition s'applique en cas de perte ou de vol d'un appareil, de violation avérée des conditions générales, d'incident de sécurité grave ou de clôture d'une campagne. Lorsque la gestion complète des appareils mobiles n'est pas mise en œuvre, la politique doit préciser clairement que l'effacement à distance ne s'applique qu'aux données de la campagne et non au contenu personnel du collaborateur.

3.5 Gestion des incidents liés à la perte, au partage ou à la compromission d'appareils

Les PNLP doivent mettre en place une procédure simple de signalement des incidents et d'intervention avant le début de la mise en œuvre. Cette procédure devrait couvrir :

- les appareils perdus ou volés ;
- les tentatives de connexion infructueuses ou les suspicions d'utilisation abusive du compte ;
- le partage accidentel de données ;
- le remplacement de l'appareil pendant la campagne ;
- le dysfonctionnement de l'application affectant l'intégrité des données ;
- la suspicion de fuite de données ou d'accès non autorisé.

Enquête sur la pénétration et l'utilisation des téléphones portables.

© Togo CDM 2014





Tous les utilisateurs sont tenus de signaler tout incident de sécurité, notamment la perte ou le vol d'appareils, les soupçons de violation de données ou tout accès non autorisé, à leur responsable direct ou au service d'assistance informatique désigné, dans un délai défini, et doivent coopérer pleinement aux procédures d'intervention en cas d'incident.

L'accès à la campagne doit, au minimum, être désactivé sans délai lorsque cela s'avère néces-

saire, les appareils de remplacement doivent faire l'objet d'une nouvelle vérification avant leur utilisation, et tous les incidents doivent être consignés et examinés.

Lorsque le partage d'appareils est courant, les programmes doivent déterminer si le modèle BYOD est adapté à ce type de personnel ou si des mesures de protection supplémentaires ou d'autres dispositions sont nécessaires.

4. MISE EN ŒUVRE DU BYOD

Cette partie décrit les étapes pratiques à suivre pour mettre en œuvre le BYOD dans le cadre d'une campagne de MII. Avant la mise en œuvre, les PNLP doivent s'assurer que la plateforme soit adaptée, que la politique soit en

place, que l'état de préparation des appareils a été évalué et que le budget nécessaire a été approuvé. Les étapes décrites au point 1.2 doivent être menées à bien avant le début de la mise en œuvre.

4.1 Dispositions de secours

Le BYOD ne devrait jamais être la seule solution opérationnelle. Des solutions de secours (alternatives) doivent être élaborées dans le cadre de la planification de la numérisation de la campagne lors de la macroplanification, et non pas après coup.

La solution de secours doit être activée lorsque :

- un appareil ne passe pas la vérification, ou bien a été perdu, volé ou endommagé ;
- l'application ne fonctionne pas de manière fiable, ou lorsque les problèmes de connexion empêchent son utilisation opérationnelle ;

- l'utilisateur choisit de ne pas participer au programme BYOD.

Les solutions de secours peuvent inclure :

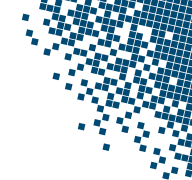
- les appareils prêtés ou appartenant au programme ;
- la réaffectation de l'utilisateur à un rôle non BYOD ;
- la collecte provisoire sur support papier, suivi d'une saisie ultérieure des données ;
- l'envoi des données avec l'aide d'un superviseur, le cas échéant.

4.2 Formation

Veillez à ce que tous les propriétaires d'appareils assistent aux sessions de formation avec leurs appareils enregistrés. La formation doit être axée sur la pratique et adaptée à chaque fonction. La formation devrait aborder à la fois l'utilisation de l'application et les règles de fonctionnement relatives au BYOD.

Les utilisateurs doivent au minimum suivre une formation sur :

- Comment se connecter et accéder aux bons formulaires ?
- Comment travailler hors ligne et quand synchroniser ?



- Comment protéger les données relatives aux appareils et aux campagnes ?
- Que faire et qui contacter en cas de dysfonctionnement de l'application, de perte de l'appareil ou de problème de synchronisation ?
- Qui contacter pour obtenir une assistance technique ?
- Quelles sont les procédures opérationnelles standard (SOP) de campagne ?

Les responsables devraient bénéficier d'une formation complémentaire sur la vérification des appareils, le suivi de la synchronisation, la remontée des problèmes et l'activation des solutions de secours.

Outre les procédures opérationnelles standard (SOP) de la campagne, la formation des agents de terrain doit porter sur :

- la présentation de la politique BYOD : ce à quoi les collaborateurs s'engagent, ce qui leur sera fourni dans le cadre du programme et quels sont leurs droits, y compris le droit de se retirer du programme ;
- la procédure de retour à la normale : qui contacter en fonction du problème, numéros de téléphone du service d'assistance, etc. ;
- l'exercice pratique sur le protocole de consentement : jeu de rôle au cours duquel les collaborateurs s'entraînent à expliquer aux ménages pourquoi des données sont collectées, en utilisant leurs propres mots.

4.3 Accompagnement et surveillance pendant la mise en œuvre

Le modèle BYOD nécessite un accompagnement actif lors de sa mise en œuvre, en particulier lorsque les appareils présentent des différences en termes d'âge, de qualité et de spécifications. Les PNLP devraient mettre en place une structure de soutien à plusieurs niveaux couvrant les échelons local, régional et national, comme :

- une assistance sur site pour la configuration, la connexion et le dépannage de base ;
- une assistance au niveau du district pour les problèmes liés aux comptes, à la synchronisation et aux applications ;

- une assistance au niveau national ou au niveau des partenaires en cas de pannes de la plateforme, de problèmes liés aux données et d'incidents de sécurité.

Les responsables doivent contrôler régulièrement :

- si les utilisateurs inscrits sont actifs ;
- si les appareils se synchronisent à l'heure prévue ;
- si les problèmes liés à la qualité des données sont en augmentation ;
- si certains utilisateurs doivent recourir à des solutions de secours.

4.4 Contrôles opérationnels quotidiens

Au cours de la mise en œuvre, les contrôles opérationnels suivants doivent être appliqués, en fonction du type de personnel, des responsabilités et du niveau d'accès aux systèmes et aux données de la campagne :

- les utilisateurs doivent effectuer la synchronisation selon le calendrier défini ;

- les responsables doivent vérifier chaque jour les utilisateurs dont les données ne se synchronisent pas ;
- il convient de surveiller les contrôles de doublons et les rapports d'exception ;



- il convient de vérifier que les données relatives aux stocks, à la distribution et à la surveillance soient complètes ;
 - les problèmes techniques non résolus doivent être signalés rapidement.
- Les programmes doivent veiller à ce que ces contrôles restent simples et s'inscrivent dans le cadre des processus existants de gestion des campagnes.

4.5 Désactivation du matériel après la campagne

À la fin de la campagne, les programmes doivent veiller à ce que l'accès BYOD soit correctement désactivé. La désactivation des appareils doit être systématique et consignée, comme indiqué au tableau 7.

Tableau 7 : Processus de désactivation du matériel après la campagne

Étape	Action	Vérification
Déconnexion à distance	Le responsable informatique déconnecte à distance tous les comptes enregistrés par le biais de la console d'administration de la plateforme.	La console d'administration de la plateforme indique que tous les comptes sont déconnectés.
Confirmation de la suppression de l'application	Le responsable vérifie que l'application a bien été désinstallée de l'appareil lors de la dernière visite sur le terrain ou par appel vidéo.	Le responsable procède à la mise hors service du dispositif relatif à l'appareil.
Vérification de la suppression des données	Le collaborateur confirme qu'aucune donnée relative à la campagne ne figure plus dans aucune application, aucun fichier ni aucune sauvegarde dans le cloud sur son appareil.	Confirmation signée sur la liste de contrôle et de clôture.
Contrôle aléatoire après la campagne	Le responsable informatique sélectionne 10 % des collaborateurs pour un contrôle aléatoire supplémentaire dans un délai de quatorze jours.	Registre des contrôles ponctuels tenu à jour.
Clôture de l'inventaire des appareils	Les appareils prêtés doivent être restitués après chaque campagne, enregistrés dans l'inventaire, stockés en toute sécurité et entretenus en vue de leur réutilisation lors de futures campagnes ou d'autres activités du programme, dans le cadre d'une gestion permanente des stocks.	Inventaire final signé par le responsable informatique du district.

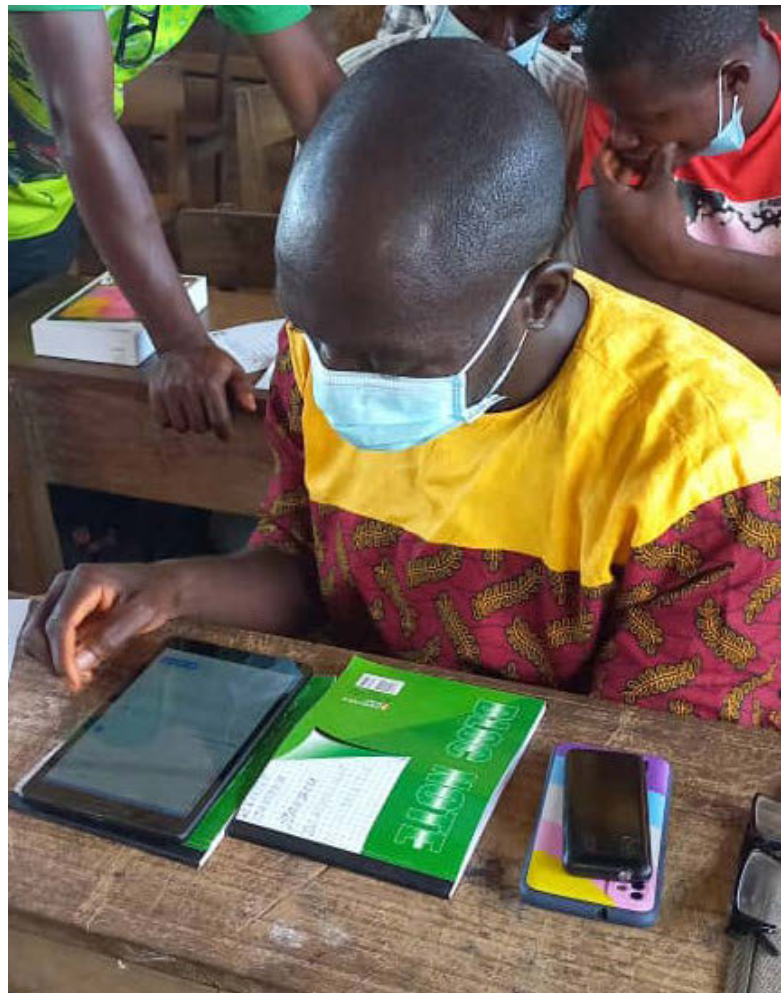
5. CONCLUSION

Les programmes qui envisagent de mettre en place ou de développer le BYOD dans le cadre de la numérisation de la campagne de MII devraient adopter une approche réfléchie et progressive. Le BYOD ne devrait être utilisé que lorsque les conditions minimales en matière de politique, de technique, d'exploitation et d'équité sont réunies. Il ne devrait pas être adopté comme solution par défaut ni être généralisé uniquement pour des raisons de commodité.

Le BYOD peut offrir des avantages opérationnels et financiers importants pour la numérisation des campagnes de MII, mais uniquement s'il est mis en place dans le cadre d'une politique claire, d'une évaluation réaliste de l'état de préparation, de mesures de protection adaptées et d'un suivi actif. Une approche structurée et fondée sur des données probantes aidera les PNLP à recourir au BYOD lorsque cela apporte une plus-value, tout en protégeant les données, en accompagnant les collaborateurs et en garantissant la qualité de la mise en œuvre.

Références

Doargajudhur, M. S., & Dell, P. (2020). The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation. *Journal of Computer Information Systems*, 60(6), pp. 518-529. <https://doi.org/10.1080/08874417.2018.1543001>



Campagne en Guinée 2022

ANNEXE 1 : Liste de contrôle pour l'évaluation de l'état de préparation au BYOD

(également disponible sous forme d'outil adaptable dans MS Word)

Remplissez cette liste de contrôle lors de la conception de la campagne, avant de choisir la plateforme et d'établir le budget.

N°	Question	Réponse	Remarques/ commentaires
Aspects juridiques, politiques et protection des données			
1	La législation nationale ou l'autorité chargée de la protection des données autorise-t-elle le traitement des catégories de données concernées sur des appareils personnels ?	☐ Oui ☐ Non ☐ En cours	
2	Une analyse d'impact relative à la protection des données a-t-elle été réalisée lorsque des données présentant un risque plus élevé sont concernées ?	☐ Oui ☐ Non ☐ En cours	
3	La politique BYOD a-t-elle été rédigée, soumise à un examen juridique et approuvée par le PNLP et les partenaires de mise en œuvre ?	☐ Oui ☐ Non ☐ En cours	
4	Cette politique a-t-elle été traduite dans les principales langues de la campagne ?	☐ Oui ☐ Non ☐ En cours	
Panorama des appareils et exigences			
5	Un inventaire des appareils a-t-il été réalisé auprès d'au moins 80 % des collaborateurs ciblés par la campagne ?	☐ Oui ☐ Non ☐ En cours	
6	Au moins 85 % des appareils inventoriés répondent-ils aux spécifications minimales ?	☐ Oui ☐ Non ☐ En cours	
7	L'application a-t-elle été testée sur au moins trois modèles d'appareils d'entrée de gamme représentatifs ?	☐ Oui ☐ Non ☐ En cours	

N°	Question	Réponse	Remarques/ commentaires
Équité, inclusion et option de retrait			
8	Les compétences numériques des agents de la campagne ciblés ont-elles été évaluées ?	☐ Oui ☐ Non ☐ En cours	
9	L'état de préparation a-t-il fait l'objet d'une évaluation ventilée par sexe, âge, catégorie professionnelle et zone géographique ?	☐ Oui ☐ Non ☐ En cours	
10	Un parc de matériel de prêt représentant au moins 5 % des effectifs participant au programme BYOD est-il prévu au budget ?	☐ Oui ☐ Non ☐ En cours	
11	Les possibilités de refus sont-elles consignées par écrit et portées à la connaissance de tous les acteurs ?	☐ Oui ☐ Non ☐ En cours	
Connectivité, sécurité et plateforme			
12	L'application fonctionne-t-elle entièrement hors ligne pour tous les processus essentiels, avec une capacité de stockage local de 2 à 3 jours ?	☐ Oui ☐ Non ☐ En cours	
13	Les contrôles au niveau des applications sont-ils confirmés : chiffrement, authentification, accès basé sur les fonctions et délai d'expiration des sessions ?	☐ Oui ☐ Non ☐ En cours	
14	Est-il possible de confirmer que la déconnexion à distance/la désauthentification est possible pour tous les types d'appareils enregistrés ?	☐ Oui ☐ Non ☐ En cours	
Coûts et rétribution			
15	Une comparaison complète des coûts entre le modèle BYOD et celui des appareils appartenant au programme a-t-elle été réalisée ?	☐ Oui ☐ Non ☐ En cours	
16	Un modèle de remboursement ou de rétribution a-t-il été défini et communiqué avant le lancement de la campagne ?	☐ Oui ☐ Non ☐ En cours	

N°	Question	Réponse	Remarques/ commentaires
Risques et état de préparation à la mise en œuvre			
17	Les risques liés au BYOD ont-ils été évalués, et les risques résiduels élevés ou critiques ont-ils été résolus ou officiellement acceptés ?	☐ Oui ☐ Non ☐ En cours	
18	Le programme BYOD fera-t-il l'objet d'un projet pilote assorti de critères de généralisation bien définis avant sa mise en œuvre à grande échelle ?	☐ Oui ☐ Non ☐ En cours	

Résumé	
Commentaires	
Indice de préparation	☐ Prêt ☐ Prêt, mais avec des lacunes ☐ Pas prêt
Lacunes importantes à combler avant de poursuivre	
Réalisé par	
Date	
Examiné par (PNLP ou point focal du partenaire de mise en œuvre)	

ANNEXE 2 : Inscription au programme BYOD, vérification des appareils et formulaire de consentement

(également disponible sous forme d'outil adaptable dans Excel)

Remplissez un formulaire par utilisateur inscrit. À récupérer lors de la formation avant l'installation de l'application ou, si possible, avant le début de la formation. Conservez les exemplaires signés auprès du coordinateur de district et du responsable de la numérisation du PNLP.

Section 1 – Informations sur les collaborateurs			
Nom complet			
Sexe	☐ Femme ☐ Homme ☐ Autre		
Fonction dans la campagne de distribution de MII			
Organisation (le cas échéant)			
Circonscription/établissement/collectivité	District	Établissement	Collectivité
Numéro de téléphone (principal)			
Adresse électronique (le cas échéant)			
Section 2 – Identification de l'appareil et vérification des caractéristiques techniques (à remplir par le responsable ou par le responsable informatique)			
Appareil	Détails enregistrés	Conditions minimales requises	Résultat
Type d'appareil		Smartphone ou tablette	☐ Admis ☐ Echec
Marque et modèle		Fiche de stock	—
Système d'exploitation et version		Android 8.0 ou version ultérieure (API 26 ou version ultérieure) ou iOS 13 ou version ultérieure	☐ Admis ☐ Echec

RAM		2 Go au minimum	☐ Admis ☐ Echec
Espace de stockage interne gratuit		2 Go avant l'installation de l'application	☐ Admis ☐ Echec
Batterie (journée de travail complète)		6 à 8 heures au minimum ; évaluez l'état réel de la batterie	☐ Admis ☐ Cond. ☐ Echec
Taille de l'écran		5 pouces au minimum	☐ Admis ☐ Echec
Réseau mobile		2G au minimum, 3G de préférence	☐ Admis ☐ Echec
GPS/services de localisation		Fonctionnalité permettant à l'application de détecter la position	☐ Admis ☐ N/A
Appareil photo		Fonctionnalité permettant à l'application de scanner un code QR ou un code-barres	☐ Admis ☐ N/A
IMEI/numéro de série		Facultatif	—

Inscrivez les données réelles dans la colonne du milieu et indiquez le résultat. Pour être homologué, un dispositif doit satisfaire à tous les critères applicables.

Section 3 – Sécurité, exclusion et contrôles fonctionnels (à remplir par le responsable ou par le responsable informatique)

Vérification	Exigence	Résultat
Verrouillage de l'écran activé	Code PIN, mot de passe, séquence ou données biométriques confirmés comme étant actifs	☐ Admis ☐ Echec
Appareil NON débridé	Aucun signe indiquant la présence de SuperSU, Magisk ou d'un débrideur. Critère d'exclusion absolu.	☐ Admis ☐ Echec
Mise à jour du système d'exploitation	Dernière version disponible, dans la mesure du possible	☐ Yes ☐ No
Chiffrement activé	Chiffrement complet du disque ou au niveau des applications confirmé	☐ Admis ☐ Echec
Installation et exécution de l'application dans le cadre de la campagne	L'application ouvre le formulaire approprié et effectue l'envoi du test	☐ Admis ☐ Echec
Désauthentification à distance confirmée	Un responsable informatique confirme que la déconnexion à distance fonctionne pour ce compte	☐ Admis ☐ Echec

Un appareil débridé constitue un critère d'exclusion absolu et ne peut pas être enregistré, quels que soient les autres résultats.

Section 4 – Déclaration et consentement du collaborateur (à remplir par ce dernier)

L'appareil décrit ci-dessus m'appartient ou est sous mon contrôle.	☐ Confirmé
J'ai lu et compris la politique BYOD et les conditions d'utilisation (annexe 4), et j'accepte de m'y conformer.	☐ Confirmé
Je comprends que les applications et les données liées à la campagne peuvent être désactivées ou supprimées à distance par le programme.	☐ Confirmé
Je signalerai immédiatement toute perte, tout vol ou toute utilisation abusive présumée de mon appareil ou des données de ma campagne.	☐ Confirmé
Je comprends que la participation au programme BYOD est facultative et que le fait de ne pas y participer n'aura aucune incidence sur le déroulement de ma campagne ni sur ma rétribution.	☐ Confirmé
En signant ci-dessous, je confirme les déclarations ci-dessus. Par ma signature, je confirme également avoir pris connaissance de la politique BYOD et des conditions d'utilisation.	
Signature du collaborateur	Date

Section 5 – Approbation du programme et décision d'admission (à usage interne uniquement)

L'appareil répond aux exigences techniques et de sécurité minimales	☐ Oui ☐ Non – Motif :
Inscrit par (nom du responsable informatique ou du représentant du programme)	
Date d'inscription	
Identifiant utilisateur/ identifiant d'appareil BYOD attribué dans le système	
Signature du responsable de l'approbation	

ANNEXE 3 : Modèle d'inventaire des appareils

(également disponible sous forme d'outil adaptable dans Excel)

Conservez ce document sous forme de feuille de calcul partagée, accessible aux responsables informatiques du district et au responsable de la numérisation du PNLP. Mise à jour en temps réel tout au long de la campagne.

Identifiant utilisateur BYOD	Nom complet	Fonction	District	Marque et modèle de l'appareil	Système d'exploitation et version	Conforme aux spécifications minimales	Date d'inscription	Date de désinscription	Remarques
BYOD-0001	Nom d'exemple	Agents de dénombrement	[District]	Samsung A10	Android 11	Oui	JJ-MM-AAAA		
BYOD-0002									
BYOD-0003									

ANNEXE 4 : Exemple de politique BYOD et de conditions d'utilisation pour les campagnes de MII

(également disponible sous forme d'outil adaptable dans MS Word)

Avant utilisation, remplacez tout le texte figurant entre [crochets] par des informations spécifiques au pays ou au programme. Un examen juridique

est obligatoire avant la finalisation et la diffusion de cette politique. Traduire dans toutes les langues utilisées dans la zone de la campagne.

1. Objectif

La présente politique relative à l'utilisation des appareils personnels (BYOD) définit les conditions dans lesquelles les appareils mobiles personnels peuvent être utilisés dans le cadre de la campagne de MII [Pays] en [Année], coordonnée par le [ministère de la Santé/programme national de lutte contre le paludisme] (« le pro-

gramme »). L'objectif est de permettre une utilisation sûre et efficace des appareils personnels dans le cadre d'activités de campagne approuvées, tout en protégeant les données du programme, les collaborateurs et les bénéficiaires des MII.

2. Cadre

La présente politique s'applique à :

- L'ensemble du personnel, des bénévoles et des prestataires (« utilisateurs ») participant à la campagne de MII [Pays] en [Année] et utilisant leurs appareils personnels dans le cadre de cette campagne
- Tous les smartphones, tablettes ou ordinateurs portables personnels enregistrés pour accéder aux applications ou aux données de la campagne

La présente politique ne s'applique pas aux serveurs *back-end*, à l'infrastructure d'hébergement ni aux appareils appartenant au programme, qui sont régis par des politiques distinctes en matière de technologies de l'information et de la communication (TIC) et de protection des données.

3. Définitions

Terme	Définition
BYOD	L'utilisation d'appareils personnels dans le cadre d'activités de campagne autorisées en vertu de la présente politique.
Appareil personnel	Un smartphone, une tablette ou un ordinateur portable appartenant à l'utilisateur, et non au programme.
Application de campagne	Un outil numérique agréé utilisé dans le cadre des activités de campagne, telles que l'enregistrement des ménages, le suivi des distributions, la surveillance ou la situation des stocks.
Appareil appartenant au programme	Un équipement acheté et géré par le programme ou par un partenaire chargé de la mise en œuvre.

4. Conditions d'admissibilité

Un utilisateur ne peut participer au programme BYOD que si toutes les conditions suivantes sont remplies :

- l'utilisateur participe officiellement à la campagne ;
- l'appareil répond aux exigences techniques et de sécurité minimales énoncées à l'[annexe 2](#) ;
- l'utilisateur a suivi la formation ou la séance d'orientation obligatoire sur le BYOD, comme l'atteste le test de fin de formation en ligne ;

- L'utilisateur a signé la présente politique ainsi que le formulaire d'inscription et de consentement au programme BYOD figurant à l'[annexe 2](#).

La participation au programme BYOD est facultative. Les collaborateurs qui refusent d'utiliser un appareil personnel ne doivent pas être pénalisés et doivent pouvoir bénéficier d'une solution de remplacement. Le programme se réserve le droit de refuser, de suspendre ou de révoquer à tout moment la participation au programme BYOD pour des raisons de sécurité, juridiques ou opérationnelles.

5. Conditions d'utilisation

Les utilisateurs ne peuvent utiliser leurs appareils personnels que pour les tâches liées à la campagne qui ont été approuvées. Il s'agit notamment (par exemple) :

- de l'enregistrement des ménages ;
- de l'enregistrement de la distribution des MII ;
- des listes de contrôle pour la surveillance et l'assurance qualité ;
- des mises à jour concernant les stocks et la logistique ;
- des supports de formation et de référence approuvés.

Les utilisateurs peuvent également recourir aux canaux de communication approuvés pour coordonner les campagnes avec leurs responsables et leurs collègues.

Les utilisateurs ne doivent pas utiliser les appareils personnels enregistrés dans le cadre du programme BYOD pour :

- partager des données de campagne par le biais d'applications ou des canaux non approuvés ;

- copier, exporter ou stocker des données de campagne en dehors des applications autorisées ;
- faire des captures d'écran des listes de destinataires, des données relatives aux ménages ou de toute information contenant des identifiants personnels ;
- permettre à des personnes non autorisées d'accéder aux applications ou aux données de campagne ;
- harceler, maltraiter ou faire preuve de discrimination à l'égard des bénéficiaires, des collègues ou des membres de la communauté ;
- accéder à des contenus illégaux, préjudiciables ou inappropriés, en utilisant les données financées par le programme.

L'utilisation des réseaux sociaux, des services de *streaming* et d'autres services non professionnels pendant les activités de campagne doit être restreinte lorsque des données financées par le programme sont fournies.

6. Exigences en matière de sécurité

Les utilisateurs doivent s'assurer que :

- l'appareil est protégé par un code PIN, un mot de passe, un schéma ou un système de verrouillage biométrique ;
- l'appareil se verrouille automatiquement après cinq minutes d'inactivité au maximum ;

- le système d'exploitation et les applications de campagne sont régulièrement mis à jour ;
- l'appareil n'est pas débridé ;
- seules les applications approuvées sont retenues pour les missions de campagne ;
- les données relatives aux campagnes ne sont ni copiées ni exportées ni partagées en dehors des canaux autorisés.

Dans la mesure du possible, le programme peut recourir à des contrôles techniques, tels que des paramètres de sécurité au niveau des

applications, des profils professionnels ou des outils de gestion des appareils mobiles.

7. Protection des données et vie privée

Les utilisateurs ne doivent collecter et traiter que les données nécessaires aux activités de la campagne, conformément aux procédures du programme et à la législation applicable en matière de protection des données en [Pays].

Les utilisateurs ne doivent pas stocker les données relatives aux campagnes dans un espace de stockage cloud personnel, dans leur messagerie électronique personnelle, dans des applications de messagerie instantanée personnelles ou sur tout autre emplacement non autorisé.

Le programme s'engage à :

- d'appliquer les principes de minimisation des données et de ne collecter que les

données nécessaires au bon déroulement des campagnes ;

- d'utiliser les mesures techniques les moins intrusives possibles pour protéger les données de campagne ;
- d'éviter d'accéder au contenu personnel stocké sur l'appareil, sauf lorsque la loi l'autorise et que cela est strictement nécessaire pour enquêter sur un incident de sécurité grave.

Les agents disposeront d'un modèle de consentement oral approuvé pour expliquer aux ménages quelles données sont collectées, pourquoi elles sont nécessaires et qui y aura accès.

8. Aide, remboursement et matériel

Ce programme permettra :

- d'assurer la formation et de fournir une assistance technique de base pour les applications de campagne approuvées ;
- de fournir des données, un crédit de communication ou une allocation définie, pour une utilisation raisonnable liée à la campagne, conformément aux procédures de campagne ;
- de gérer un stock limité d'appareils de prêt appartenant au programme, destinés aux uti-

lisateur ne disposant pas d'appareils personnels adaptés ou à titre de solution de secours.

En fonction des décisions stratégiques, le remplacement intégral d'un appareil personnel perdu, volé ou endommagé n'est pas garanti. Toute aide apportée dépendra des règles du programme, des ressources disponibles et des circonstances de l'incident telles qu'elles ont été constatées.

9. Responsabilités de l'utilisateur

En participant au programme BYOD, les utilisateurs s'engagent à :

- respecter la présente politique et les procédures associées au programme ;
- veiller à ce que leur appareil soit sécurisé, à jour et en bon état de fonctionnement ;
- signaler immédiatement la perte ou le vol d'appareils, les violations présumées de données et les infractions aux règles ;
- autoriser le programme à supprimer les applications et les données liées à la campagne à la fin de celle-ci ou de l'engagement ;

- autoriser le programme à bloquer l'accès aux données de campagne ou à les supprimer à distance en cas de perte, de vol ou d'incident de sécurité grave.

Les utilisateurs ne doivent pas permettre à des personnes non autorisées d'utiliser leur appareil pour accéder aux applications ou aux données de la campagne.

10. Responsabilités liées au programme

Ce programme permettra :

- de communiquer clairement les règles, les risques et les responsabilités liés au BYOD, dans un langage compréhensible pour les collaborateurs ;
- de fournir des supports de formation et les coordonnées des personnes à contacter avant le lancement de la campagne ;
- d'appliquer cette politique de manière cohérente et équitable à l'ensemble des utilisateurs et des cadres ;
- de prendre des mesures raisonnables pour protéger à la fois les données de la campagne et la confidentialité du contenu des appareils personnels des collaborateurs.

11. Non-conformité

Le non-respect de cette politique peut entraîner :

- la suspension ou la suppression de l'accès BYOD ;
- la désactivation des comptes liés aux applications de la campagne ;
- des mesures disciplinaires conformes aux procédures applicables au personnel ou aux bénévoles ;
- la transmission du dossier aux autorités compétentes lorsque la loi l'exige.

12. Accusé de réception de l'utilisateur

Ce formulaire doit être signé avant que l'enregistrement de l'appareil ne soit finalisé et avant que l'accès aux applications de la campagne ne soit accordé.

Champ	Réponse
Je soussigné(e), [Nom], certifie avoir lu et compris la politique BYOD ainsi que les conditions d'utilisation de la campagne de MII du/de la [Pays] en [Année]. J'accepte de me conformer à ces exigences et je comprends les responsabilités liées à l'utilisation de mon appareil personnel dans le cadre de la campagne.	
Nom complet	
Fonction	
Organisation (le cas échéant)	
Numéro de téléphone	
Marque et modèle de l'appareil	

Champ	Réponse
IMEI/numéro de série (facultatif)	
Signature	
Date	



CONTACTS APP

Pour participer à la conférence téléphonique hebdomadaire de l'AMP chaque mercredi à 10h00, heure de l'Est (16h00 CET), veuillez utiliser la ligne de réunion Zoom suivante :

<https://us06web.zoom.us/j/88935481892?pwd=h3cuJ3x5LOsR58YXcEaub8ULqu5LMj.1>

Vous pouvez trouver votre numéro local pour rejoindre l'appel hebdomadaire :

<https://zoom.us/j/acyOjklJj4>

Pour être ajouté à la liste de distribution de l'AMP, veuillez visiter :

<https://allianceformalariaprevention.com/join-us>

Pour contacter AMP ou rejoindre un groupe de travail AMP, veuillez envoyer un courriel électronique à :

info@allianceformalariaprevention.com

Pour plus d'informations, veuillez consulter le site de l'AMP :

<https://allianceformalariaprevention.com>



Alliance pour la
Prévention du Paludisme
Elargir la possession et l'utilisation de moustiquaires