# Commission médicale d'établissement

Renforcement des contrôles des accès illégitimes aux données des patients : limitation de l'accès au mode « bris de glace »

2 février 2023



#### Limitation de l'accès au mode « bris de glace »



#### Rappel de l'historique :

- Contrôle CNIL sur Orbis à PSL en février 2020
- Injonctions CNIL en date d'avril 2021 en lien avec la confidentialité des données
- Échanges AP/CNIL entre 2021 et 2023 sur la finalisation / le bon avancement des chantiers
- Procédure encore en cours à ce stade (attente du retour CNIL)
- Risque réglementaire image et confiance des patients aspects éthiques
- Accès illégitime aux données de santé = violation de données personnelles = violation du secret médical
- Injonction n°5 de la CNIL sur le bris de glace :

« Mise en œuvre d'un système de surveillance du mode bris de glace, par exemple l'utilisation de ce mode pourrait déclencher une notification ou être tracée sur un tableau de bord dédié »



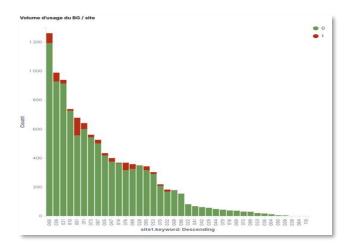
Contrôler et identifier les abus /
les accès illégitimes aux
données sensibles via le mode
BG



#### Limitation de l'accès au mode « bris de glace »

### Actions réalisées 2021 /2022 :

- ✓ Audit de l'état des lieux du BG
- ✓ But : diminuer le volume d'utilisation afin de pouvoir effectuer un système de surveillance cohérent et efficace
- Redéfinition des 12 motifs du menu déroulant, suppression du motif
   « accès transverse »
- ✓ Tutoriel sur le mode bris de glace et sur la demande d'avis
- ✓ Tableau de bord sur le volume / pic d'utilisation précis selon les sites, les rôles, etc. (= les abus et accès illégitimes potentiels)
- Conduite du changement (sensibilisation et communication) à mener par la communauté médicale sur le bon usage du mode BG et sur la fonctionnalité demande d'avis, à relayer en CMEL



## Sensibilisation et communication à renforcer / poursuivre en 2023 :

- Sur la fonctionnalité « demande d'avis »
- Sur le bon usage du mode BG, le caractère exceptionnel et les contrôles effectués
- Plus généralement : sur les règles d'accès au DPI, au BG et contrôles effectués



## Limitation de l'accès au mode « bris de glace »

# Processus de surveillance envisagé :

	Processus
Nature du contrôle	Outil de visualisation des pics /volumes (tableau de bord)
Identification des éventuels abus / accès illégitimes	Référent habilitation Orbis Siège puis sites
Fréquence du contrôle	Hebdomadaire
Quelles actions en cas de suspicion d'accès illégitime	Mail type 1, 2 / 3 à l'utilisateur, justifications <i>Puis</i> Présentation et débat des dossiers en 3cadp en cas d'accès illégitime, arbitrage
Qui qualifie l'abus in fine, qui initie la sanction	Convocation par RH (PNM) / DAM (PM)



#### Annexe - Limitation de l'accès au mode « bris de glace »

# Proposition de communication sur le bris de glace

« La fonctionnalité « bris de glace » et la fonctionnalité « Demande d'avis » ont fait l'objet d'une mise à jour.
L'usage du mode bris de glace doit demeurer exceptionnel et en aucun cas être utilisé « par défaut ». Le motif d'utilisation sélectionné dans le menu déroulant doit être pertinent et adapté à la situation qui justifie l'accès dérogatoire au dossier patient concerné via ce mode. Un système de surveillance est mis en place. Tout accès illégitime aux données de santé pourra faire l'objet de sanctions, disciplinaires et/ou pénales.

Pour plus d'informations sur l'utilisation de ce mode et sur la fonctionnalité « demande d'avis », pour pouvez consulter les tutoriels dédié <u>ici</u> ou sur la sur la plateforme Orbis & Moi »

# Proposition de communication sur les règles d'accès au DPI, contrôles et sanctions

« Pour rappel, voici les règles à respecter concernant l'accès au dossier patient :

- L'accès au dossier d'un patient n'est autorisé qu'aux professionnels faisant partie de l'équipe de soin ayant pris en charge ledit patient : tout autre accès peut être considéré comme illégitime et constitutif d'une violation du secret et d'une violation de données personnelles
- L'utilisateur ne doit pas tenter d'accéder à des dossiers pour lesquels il n'est pas habilité, et même s'il est habilité, il ne doit accéder qu'aux seuls dossiers strictement nécessaires à sa mission
- Toutes les actions des utilisateurs sur Orbis sont tracées et peuvent être auditées (audits ciblés à la demande d'un patient ou audits aléatoires)
- En cas de suspicion d'un accès illégitime, toute personne concernée peut demander les traces des connexions (accès et actions) effectuées sur ce dossier à l'adresse protection.donnees.dsi@aphp.fr. Les traces d'accès seront analysées dans le cadre d'une instance collégiale pluridisciplinaire dédiée (la 3CADP).
- Tout accès illégitime aux données de santé pourra faire l'objet de sanctions, disciplinaires et/ou pénales.



