# FICHE RÉFLEXE

## COMMENT SIGNALER UNE FUITE DE DONNÉES PATIENTS ?

Les établissements de santé manipulent des données hautement sensibles concernant les patients. Toute fuite de données peut avoir des conséquences graves, tant sur le plan juridique que sur la confiance des patients.

#1

### IDENTIFICATION DES TYPES DE FUITES DE DONNÉES PATIENTS

- Un envoi erroné d'informations sensibles (email mal adressé, dossier transmis à un mauvais destinataire)
- Une perte ou vol de matériel contenant des données patients (ordinateur, téléphone, clé USB non chiffrée...)
- Une attaque informatique (hameçonnage, rançongiciel, intrusion dans le système)
- Un accès non autorisé à des dossiers patients par une personne non habilitée
- Une divulgation accidentelle sur des supports numériques ou papiers accessible au public

#2

### DÈS QUE VOUS SUSPECTEZ OU CONSTATEZ UNE FUITE DE DONNÉES PATIENTS, VOUS DEVEZ

- Ne pas tenter de masquer ou de minimiser l'incident. Tout le monde peut faire une erreur ou être victime de vol (rappel des peines encourues)
- Documenter l'incident (date et heure, nature des données compromises, origine possible de la fuite)
- Prendre des captures d'écran ou conserver des preuves sans les partager publiquement
- Éviter toute communication externe avant validation par la direction
- Informer immédiatement le service informatique par mail ou par appel

#3

### ALERTE ET DÉROULEMENT SUITE À LA DÉCLARATION DE FUITE

- Dans un premier temps, une pré analyse sera effectué au sein du service informatique pour vérifier les différents éléments transmis.
- S'il s'avère que le constat aboutit bien sur une fuite de données, le DPO sera mis au courant de la situation.
- Des mesures de sécurité seront immédiatement mises en place : suspension immédiate de l'accès aux comptes compromis (si applicable), limitation de l'accès aux données concernées pour éviter une propagation de la fuite, ou une récidive, analyse approfondie de l'ampleur de l'incident (volume de données exposées, personnes affectées, durée d'exposition)
- Selon la gravité de la fuite, le DPO devra : notifier les autorités compétentes sous 72 heures si la fuite représente un risque confirmé pour les droits et libertés des patients. Ces derniers devront être informés de la compromission de leurs données.

### SIGNALEZ IMMÉDIATEMENT

- Se référer au #1

**Avertir le service informatique**
1017 ou 05 55 43 10 17

Ou nous contacter sur
informatique@ch-esquirol-limoges.fr