PROCEDURE DE GESTION DES INCIDENTS DE SECURITE ET VIOLATIONS DE DONNEES DANS LE DOSSIER COMMUNICANT DE CANCEROLOGIE (DCC) BRETAGNE

Version N°1 - Décembre 2024

Table des matières

i. Sigles cités dans la procédure

Identifiants	Intitulé
PGSSI	**Politique de Gouvernance de la Sécurité du Système d'Information**
RSSI	**Responsable de la Sécurité du Système d'Information**
DPO	**Délégué à la protection des données** (aussi nommé DPD)
DCP	**Données à Caractère Personnel**
DCC	**Dossier de Communicant de Cancérologie**
PSSI	**Politique de Sécurité du Système d'Information**
CR RCP	**Compte Rendu RCP**
RCP	**Réunion de Concertation Pluridisciplinaire**
SMSI	**Système de Management de la Sécurité de l'Information**
RSMSI	**Responsable du SMSI**
ANS	**Agence du Numérique en Santé**
CNIL	**Commission Nationale de l'Informatique et des Libertés**
RGPD	**Règlement Général sur la Protection des Données**

ii. Termes spécifiques à la procédure

Identifiants	Intitulé
Donnée à caractère personnel (DCP)	Une donnée à caractère personnel concerne toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement (nom, prénom, photo, empreinte, adresse postale, mail, numéro de téléphone, adresse IP, matricule interne, enregistrement vocal, …). Peu importe que ces informations soient confidentielles ou publiques. Attention : s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.
Responsable de traitement	Le responsable de traitement est le responsable de l'établissement/de la structure ou toute personne déléguée dûment inscrite au Registre Légal des Délégations
Le sous-traitant	Le sous-traitant est un prestataire qui effectue un traitement de données pour le compte du responsable de traitement (ex : administration des profils)

1. CHAMP D'APPLICATION

Cette procédure décrit les conditions d'application de l'obligation de notification aux autorités en cas d'incident de sécurité dans le Dossier Communicant de Cancérologie de Bretagne ayant pour conséquence ou non une violation de données à caractère personnel conformément à la réglementation en vigueur.

*« L'OMS définit la **cyber santé** comme "l'utilisation sécurisée et économiquement avantageuse de technologies de l'information et de la communication en appui à la santé et au domaine sanitaire". La cyber santé est aujourd'hui menacée par les cyber-attaques. Attaque par rançongiciel, destruction ou exfiltration de données sensibles telles que les données de santé à caractère personnel, accès illégitimes aux données, peuvent mettre en péril la sécurité des patients et l'activité des établissements » (source : site de l'ANS).*

Les incidents de sécurité au sein d'un établissement de santé peuvent avoir des conséquences graves à la fois sur la prise en charge des patients mais aussi sur la violation des données et sur l'organisation interne et externe de l'établissement. Les conséquences éventuelles sont une baisse significative d'activité de soins, des pertes financières et un impact sur la confiance du système de soins.

Un constat récent indique que les menaces liées à la cybercriminalité sont en augmentation pour le secteur de la santé. (*observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé- Rapport public 2021- MSS/ANS).*

En ce qui concerne les situations d'incidents de sécurité entrainant une violation des données (perte de disponibilité, d'intégrité ou la confidentialité), une récente publication des lignes directrices du Comité Européen de la Protection des Données (CEPD) recense 18 cas pratiques parmi lesquels on peut citer :

- **Rançongiciel :**
  - Sans exfiltration de données et avec sauvegarde ;
  - Sans sauvegarde ;
  - Dans un hôpital (avec sauvegarde et sans exfiltration) ;
  - Avec exfiltration et sans sauvegarde.
- **Attaques d'exfiltration de données :**
  - Exfiltration de données de candidature à des offres d'emploi ;
  - Exfiltration de mots de passe hachés ;
  - Bourrage d'identifiants sur un site bancaire (credential stuffing)
- **Source interne de risque humain :**
  - Exfiltration de données d'entreprise par un employé ;
  - Transmission accidentelle à un tiers.
- **Appareils ou documents papier perdus ou volés :**

- Matériel volé stockant des données personnelles chiffrées ;
- Matériel volé stockant des données personnelles non chiffrées ;
- Documents papier volé contenant des données sensibles.

- **Erreur d'envoi :**
  - Erreur d'envoi mail ou postal de compte-rendu médical ;
  - Données personnelles hautement confidentielle envoyées par courriel par erreur ;
  - Données personnelles envoyées par courriel par erreur ;
- **Ingénierie sociale :**
  - Vol d'identité ;
  - Exfiltration de courriels

2. REFERENCES

2.1. Contexte réglementaire

VIOLATION DE DONNEES

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - **RGPD**).

- Article 4 -12 RGPD – Définition d'une violation de données
- Article 33 RGPD - Notification à l'autorité de contrôle d'une violation de données à caractère personnel
- Article 34 RGPD - Communication à la personne concernée d'une violation de données à caractère personnel

Lignes directrices du G29

INCIDENT DE SECURITE

- CNIL- Délibération no 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et décret d'application n°2019-536 du 29 mai 2019.
- Violation de données : le CEPD publie des lignes directrices à partir de cas pratiques | CNIL
- PGSSI-S - Article L1110-4-1 de la Loi de Santé
- CSP- Article L. 1111-8-2 – Déclaration des incidents graves de sécurité

- CSP - Article D1111-16-2 à D1111-16-4 (avril 2022) – Catégories d'incidents, conditions et modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'informations
- CSP - 2010 – GIP – Agence du Numérique en Santé (ANS)
- CSP - Décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information
- CSP- Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique
- CSP - Décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information
- CSP - L'article L.1111-8, hébergement de données de santé chez un hébergeur agréé HDS. LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (dites HPST) - Droits de la personne
- Code de la défense Article L1332-6-2 – Délai de déclaration d'incident
- Code pénal (CP) – Art 323-1 à 3 – Infraction au système de traitement automatique de données
- Code pénal (CP) – Art 323-1 à 3 – Infraction en bande organisée
- Arrêté du 13 juin 2018 fixant les modalités des déclarations des systèmes d'information et des incidents de sécurité des opérateurs de services essentiels, et des incidents de sécurité des fournisseurs de service numérique.
- Arrêté du 1er août 2018 relatif au coût d'un contrôle effectué par l'Agence nationale de la sécurité des systèmes d'information Arrêté du 14 septembre 2018 fixant les règles de sécurité relatif à la sécurité des réseaux et systèmes d'informations des opérateurs de services essentiels ;

SITES INTERNET DE REFERENCE

- Site de l'ANSSI : Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Site de l'Agence du Numérique en Santé : https://esante.gouv.fr/lagence
- Site du CERT Santé (Computer Emergency Response Team Santé) : Cyber veille Santé | Accompagnement Cyber sécurité des Structures de Santé (cyberveille-sante.gouv.fr)
- Site de la Commission National et Liberté (CNIL) : Professionnel | CNIL
- Plateforme d'assistance et prévention du risque numérique au service publics - GIP ACYMA Actions Contre la Cyber malveillance : Assistance aux victimes de cyber malveillance
- Notifier une violation de données en ligne : Notification (cnil.fr)

- Déclarer un incident de sécurité en ligne : https://signalement.social-sante.gouv.fr
- Déclarer un incident de sécurité hors heures ouvrées : ssi@sg.social.gouv.fr

2.2. Document de référence

Liste des documents de référence à appliquer :

DOCUMENTS INTERNES RATTACHES	
Référence	**Intitulé**
Sur le site internet OB	Politique de protection des données
A réaliser	Plan de Continuité d'activité (PCA - procédure dégradée)
A réaliser	Plan de Reprise d'activité (PRA)
Annexe 1	Fiche de déclaration de violation de données dans le cadre de l'utilisation du dossier communicant de cancérologie de Bretagne
Modèle	Fiche de suivi d'une violation de données à caractère personnelle
Existant	Registre de violation de DCP
Modèle	Autoévaluation de la gravité de la violation
Modèle	Courrier type de notification aux personnes concernées

DOCUMENTS EXTERNES RATTACHES	
Instance	**Intitulé**
Cyberveille santé	Fiches pratiques : Fiches pratiques | Accompagnement Cyber sécurité des Structures de Santé (cyberveille-sante.gouv.fr)
ANSSI	Formulaire de déclaration d'incident de sécurité OSE : formulaire-incidents-ose_anssi.pdf
CNIL	Formulaire de notification de violations de données à caractère personnel (audentia-gestion.fr)
MSS/ANS	Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé- Rapport public 2021

3. PERSONNES CONCERNEES ET RESPONSABILITES

3.1. Les responsables de traitement

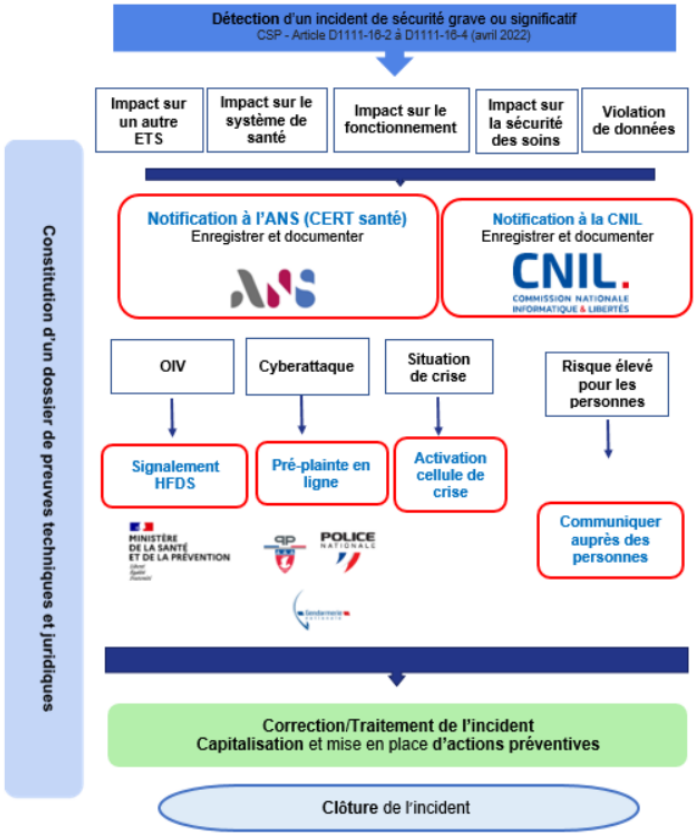
Traitements/ Base légale	Responsable de traitement	Sous-traitants
Gestion du dossier du patient sur le DCC RGPD Art 6.1 f) 9,2 h)	**Etablissements de santé autorisés en cancérologie et Centres de Radiothérapie** Les Professionnels de santé libéraux (CGU)	- GR e-santé Bretagne/ DEDALUS/Cloud Temple - Secrétariat de RCP (3C/PRC)
Gestion de l'administration régionale du DCC RGPD Art 6.1 f) 9,2 h)	**DSRC ONCOBRETAGNE**	- GR e-santé Bretagne / DEDALUS/SIB - Centres de Coordination en Cancérologie (3C) - Pôle Régional de Cancérologie (PRC)
Gestion de la base de données du DCC RGPD Art 6.1 f) 9,2 j)	**DSRC ONCOBRETAGNE** + **CADDOC** (Commission d'Accès aux Données du DCC)	- GR e-santé Bretagne / DEDALUS/SIB - Centres de Coordination en Cancérologie (3C) - Pôle Régional de Cancérologie (PRC)

Traitements/ Base légale	Finalités
Gestion du dossier du patient sur le DCC *Intérêt légitime Art 6.1 f) nécessaire à la prise en charge sanitaire 9,2 h) RGPD*	- **Constitution du dossier du patient** *(créer un patient, ajouter des correspondants, saisir, modifier et supprimer des données, envoyer des documents)* - **Passage en RCP** du dossier *(dérouler, tracer, valider le CR-RCP, envoyer)* - **Echange d'information** avec l'équipe médicale *(partage des documents nécessaires au suivi dont PPS et PPAC)*
Gestion de l'administration régionale du DCC *Intérêt légitime Art 6.1 f) nécessaire à la prise en charge sanitaire 9,2 h) RGPD*	- **Fourniture du service** *(paramétrage, installation, hébergement, maintenance, assistance, accès ENRS)* - **Gestion des annuaires professionnels, gestion des profils et droits, identito-vigilance, traçabilité**
Gestion de la base de données du DCC *Intérêt légitime Art 6.1 f) à des fins statistique et de recherche 9,2 j) RGPD*	- **Gestion des bases de données WebDCR (DCC actuel) et Alfalima (ancien DCC) et de l'interface infocentre** : extractions anonymisées et pseudonymisées, fichiers de correspondance *(Analyse de l'activité des RCP des patients et des professionnels)* - **Gestion des demandes dans le cadre d'études scientifiques** ayant un objectif de santé publique *(extractions, envois sécurisés, déclaration MR004)*

3.2. Les acteurs

- **Le président d'Oncobretagne et le directeur de l'établissement autorisé :** prennent les décisions nécessaires au traitement de l'incident et effectue les déclarations aux autorités compétentes. Ils sont responsables de traitement.
- **Chef de projet Maitre d'Ouvrage :** GR-esante assure le suivi des actions en lien avec l'éditeur.
- **Chef de projet Oncobretagne :** assure le suivi des actions en lien avec les utilisateurs du DCC
- **Le Délégué à la protection des données (DPO Oncobretagne et établissement)** : En cas de violation de données à caractère personnel, lors de la déclaration à la CNIL, le responsable de traitement communique le nom et les coordonnées du DPO ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues.
- **Le service de communication (Oncobretagne) :** communique avec tous les groupes de parties prenantes de manière appropriée. Répondre immédiatement aux questions des usagers, de leurs proches et de la presse.
- **L'éditeur (Dedalus) :** Fait remonter les incidents au plus tôt. Respecte la garantie de temps de rétablissement contractualisée.

4. PRESENTATION GENERALE DU PROCESSUS GENERAL



QUI	QUOI	COMMENT
Utilisateurs DCC/ patients	**SUSPICION D'UNE VIOLATION DE DONNEES PAR L'UTILISATEUR DU DCC/PATIENT** **PERTE D'INTEGRITE** **Modification/Erreur** Exemples : - Enregistrement d'un CR RCP dans un mauvais dossier - Saisie d'une mauvaise information dans un dossier ou une fiche RCP - Information manquante lors de l'enregistrement d'un document, etc… **PERTE DE DISPONIBILITE** **Indisponibilité du DCC > 7 jours** Exemples : - Coupure internet prolongée - Cyber-attaque avec chiffrement et vol de données, etc… **PERTE DE CONFIDENTIALITE** **Accès illicite volontaire ou non** Exemples : - Envoi d'un CR RCP à un mauvais correspondant ou au patient - Erreur d'habilitation avec accès illicite au dossier du patient - Vol ou prêt d'un identifiant/mot de passe, etc…	Ticket en cas d'incident de sécurité
DPO et Chef de projet OB	Déclaration d'un incident avec suspicion de la violation de données auprès **du réseau Oncobretagne** par **mail** via les adresses suivantes : **dpo@oncobretagne.fr** et **secretariat@oncobretagne.fr** **(possibilité d'utiliser le formulaire de déclaration de violation de données en annexe)**	Formulaire de déclaration de violation de données Doublon /collision (procédure)
DPO OB et DPO ETS et DIM/ Utilisateurs médicaux (médecin référent/secrétaire médicale) / Administrateurs locaux / Référent identito-vigilance	Enregistrement de l'incident et création d'un ticket via l'outil Dédalus si nécessaire	Enregistrement « fiche de suivi » partagée Registre de violation de DCP
	Collecte des preuves liées à l'incident de sécurité afin de qualifier la violation de données	Dossier patient DCC Journaux
Direction d'ETS et OB	Propositions et mise en œuvre d'actions de remédiation	Fiche de suivi de la violation Echange par Mail ou plateforme sécurisée
	Evaluation de l'impact sur la vie privée des personnes concernées par la violation de données	
Direction d'ETS et président OB	Information du/des DPO des établissements concernés et décision conjointe de notification CERT Santé et CNIL, si nécessaire	Formulaire en ligne CNIL (modèle OB pour les ETS)
	Information des personnes concernées si nécessaire	
DPO OB et ETS	**Clôture de la demande et enregistrement au registre des traitements**	LAR - AR Registre des violations OB (modèle) et ETS concernés

5. DETECTION ET SIGNALEMENTS

Il existe différents moyens de détection d'incidents :

- Toute personne qui a connaissance d'un fait ou d'une menace dans le DCC (par exemple la saisie d'une mauvaise information dans un dossier ou une fiche RCP, coupure internet prolongée),
- Un administrateur lorsqu'il est informé par un dispositif de supervision ou lorsqu'il constate une anomalie,

5.1. Les incidents ayant des conséquences sur la confidentialité ou l'intégrité des données de santé

L'incident de sécurité touche un traitement de données à caractère personnel et entraine une violation de données à caractère personnel :

- **Perte de la disponibilité**
    - Indisponibilité permanente

En cas de perte ou de destruction permanente, la perte de disponibilité est TOUJOURS considérée comme une violation de DCP

    - Indisponibilité temporaire

Il y a violation de données pour cause de perte de disponibilité (temporaire) en cas de PERTURBATION MAJEURE DU SERVICE NORMAL =

La durée d'interruption maximale acceptable est définie à 7 jours

A noter : une indisponibilité dans le cadre d'un entretien planifié du système n'est pas considérée comme une violation de données.

- **Perte de l'intégrité**

Les données sont modifiées en des données invalides, qui ne seront pas utilisées de manière correcte, le traitement pouvant engendrer des erreurs, des dysfonctionnements, ou modifiées en d'autres données valides, de telle sorte que les traitements soient détournés (ex : enregistrement d'un compte rendu RCP dans un mauvais dossier, saisie d'une mauvaise information dans un dossier ou une fiche RCP, envoi d'un CR RCP erroné vers le DPI d'un patient...).

- **Perte de la confidentialité**

Les données sont diffusées plus que nécessaire, elles sont exploitées à d'autres fins que celles prévues et/ou de manière injuste. Accès illicite volontaire ou non (ex : envoi d'un CR RCP à un mauvais correspondant ou au patient, erreur d'habilitation avec accès illicite au dossier de patient, vol ou prêt d'un identifiant/mot de passe…)

5.2. Les incidents portant atteinte au fonctionnement normal d'un établissement

EX : intégration d'un compte rendu RCP erroné dans le DPI d'un établissement autorisé

5.3. Les incidents ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé

LES EFFETS PAR RICOCHET SUR LES SYSTEMES DE L'ETAT

Plateforme de données en cancérologie :

https://www.e-cancer.fr/Expertises-et-publications/La-plateforme-de-donnees-en-cancerologie

6. DECLARATION D'UN INCIDENT DE SECURITE/ VIOLATION DE DONNEES AU DSRC ONCOBRETAGNE

- La déclaration est effectuée par un utilisateur du DCC aux adresses suivantes : **dpo@oncobretagne.fr, r.ngandjeu-sonnang@gmail.com**

  → Demande via le Formulaire de déclaration de violation de données dans le cadre de l'utilisation du dossier communicant de cancérologie de Bretagne (cf. annexe)

- Si un incident de sécurité est associé, Oncobretagne fera une notification par ticket à l'éditeur (Dedalus)

7. CONSTITUTION D'UN DOSSIER DE PREUVES TECHNIQUES ET JURIDIQUES

7.1. La collecte des preuves liés à l'incident de sécurité

Il convient en effet de documenter la correction de la faille, notamment en cas d'attaque d'un tiers malveillant.

L'élément technique qui a permis de collecter la preuve ne peut être recevable légalement qui si et seulement si elle a été portée à connaissance du CSE et des agents (*ex : traçabilité figurant dans la charte SI annexée au règlement intérieur*) (L1121-1, L1222-4, L2323-32 du code du travail) - Cours d'appel de Paris 25/11/2020 n°17-09.132.

Il est nécessaire de décrire les faits et les mesures prises et de les tracer (jours, heures, minutes, secondes)

Les DPO (OB, GR, ETS) et le RSSI d'établissement sont impliqués dans la démarche. Les directions sont tenues informées de l'évolution de l'instruction.

7.1.1. PRECAUTIONS PRISES

Dans le cadre d'un incident qui pourrait donner lieu à une action juridique ou dans le cadre d'une analyse a posteriori, un certain nombre de données sont collectées afin d'avoir une base de travail suffisamment conséquente.

Pour éviter de modifier les traces lors des investigations, l'actif analysé est au préalable sauvegardé et protégé en intégrité. Il sera par exemple déconnecté du réseau pour ne pas altérer les éléments de preuves qui serviront pour l'analyse de l'incident.

Pour pallier au cas de figure où la copie complète n'est pas réalisable (baie de stockage SAN par exemple), une sauvegarde des journaux de connexion est réalisée et conservée chiffrée. Cette sauvegarde est copiée sur un site distant ; copie également stockée de manière chiffrée.

7.1.2. TRAÇABILITE DES ACTIONS

La collecte de preuves se fait conjointement entre le DPO d'Oncobretagne, le DPO établissement, et l'administrateur local. Elle doit être fiable : valide, authentique, force probante.

En fonction des enjeux, il pourra être utile de réaliser ces actes en présence d'un huissier de justice et il est possible aussi d'être accompagné par un prestataire de réponse à incident dans la mesure ou l'incident demande un niveau d'expertise plus important.

Cette collecte ne se fait pas pour les incidents non critiques, qui n'impactent pas un tiers ou les faux-positifs.

Chaque personne intervenant sur la collecte trace ses actions qui seront regroupées dans un formulaire « collecte de preuves », en précisant :

- La personne effectuant l'action ;
- La date et heure (min, secondes) de l'action ;
- La description détaillée de l'action menée.

Le cas échéant, la personne à l'origine de l'action renseigne l'élément de preuve trouvé, à savoir :

- Le type de preuve collectée ;
- L'empreinte numérique ;
- La description de l'élément ;
- La source de collecte.

Le travail d'investigation est fait ensuite sur des copies de sauvegardes à partir d'un poste de travail dédié à cette tâche. Celui-ci contient un certain nombre d'outils permettant une investigation très poussé dans la recherche de compromission. Les données originales sont protégées et conservées dans des conditions de sécurité spécifiques.

Une empreinte numérique (hash MD5, SHA1, etc…) de la donnée originale et de sa copie permet d'en confirmer l'authenticité.

7.1.3. SECURISATION DES PREUVES

Les preuves ainsi collectées sont envoyées au DPO d'Oncobretagne qui les transfère et les stocke dans un dossier accès restreint. Pour se prémunir contre la perte de disponibilité et la perte d'intégrité, le répertoire est sauvegardé et dupliqué sur un site distant.

Les preuves sont sauvegardées 1 an sauf si une action juridique a découlé de l'incident, auquel cas la rétention sera portée à 6 ans (Art code pénal – L133-3)

Le CERT Santé peut accompagner l'établissement dans la résolution de l'incident et analyser les traces récoltées. Il peut dépêcher un expert sur place si nécessaire.

7.2. Concernant la violation de données

7.2.1. COLLECTE DE PREUVE

Il convient en effet de documenter la violation de données tout au long de l'investigation

Analyser la violation et évaluer le risque pour les personnes

- Identifier le type de violation (accès illicite, modification, disparition/indisponibilité)
- Les catégories de données et nombre approximatif
- Sensibilité des données
- La nature identifiable des données concernées = la probabilité d'exploitation des données impactées (facilité d'identification) ;
- Le nombre de personnes concernées
- Le caractère préjudiciable de la violation pour la personne concernée (Niveau de gravité de l'impact Impact)
- Fréquence de la violation

La fiche suivi la violation sera enrichie au cours des phases suivantes du traitement de l'incident

7.2.2. EVALUATION DE L'IMPACT SUR LA VIE PRIVEE AUPRES DES PERSONNES CONCERNEES

L'évaluation du risque s'effectue par la combinaison de deux critères :

- La probabilité d'exploitation des données impactées (facilité d'identification) ;
- La gravité (impact) sur les individus concernés d'une exploitation de données.

La CNIL dispose d'un délai de 2 mois pour vérifier le caractère approprié ou non de ces mesures techniques. En l'absence de retour de la CNIL dans ce délai, vous devrez considérer que les mesures ne sont pas appropriées et vous devrez immédiatement informer les personnes de la violation.

OUTILS :

- **FICHE DE SUIVI DE VIOLATION DE DONNEES (modèle OB) Annexe 2**
- **REGISTRE DE VIOLATION DES DCP OB**
- **OUTIL DE QUOTATION (modèle) Annexe 3**

8. SUITES TECHNIQUES DONNEES A L'INCIDENT

8.1. Correction de l'incident

Les chefs de projet OB et GR e-santé et l'éditeur (Dedalus) identifient les raisons techniques et fonctionnelles de l'incident de sécurité.

En cas de violation les utilisateurs identifient et recueillent les preuves.

Les acteurs en lien avec le DPO proposent des mesures adéquates pour y remédier.

Un plan d'action est établi, puis mis en œuvre sur ordre du Responsable de Traitement (président OB et directeur établissement).

Le DPO complète le registre des incidents en indiquant les mesures de remédiation définies.

Une fois l'incident analysé, le DPO OB communique l'ensemble des informations aux DPO des établissements concernés et à leur direction/copie président et coordinatrice OB.

Les DPO et les chefs de projets OB et GR e-santé s'assurent de la mise en œuvre et de l'efficacité des mesures avant de clore l'incident dans le registre de violations de données.

Le DPO Oncobretagne en lien avec les DPO d'établissement émettent un avis quant à la notification CNIL et l'information des personnes.

Le président OB et les directeurs décident des suites à donner.

En cas d'incident de sécurité (se reporter à la procédure gestion de crise en cours de rédaction)

8.2. Capitalisation de l'expérience acquise

Suite à la clôture de l'incident de sécurité, le président ou coordinateur d'Oncobretagne organise une revue avec Dedalus, DPO OB, et les sous-traitants concernés le cas échéant afin de :

- Mener un bilan sur la détection et la correction de l'incident qui a mené à la violation des données personnelles,
- Mieux comprendre les vulnérabilités organisationnelles et techniques qui existent,
- Émettre des recommandations et identifier les mesures permettant d'éviter que ce genre de violation ne se reproduise.

A l'issue de cette revue, un plan d'action est défini. Sa mise en œuvre est suivie par le RSSI/DPO accompagné de toutes personnes utiles.

9. SIGNALEMENT A D'AUTRES AUTORITES ADMINISTRATIVES

9.1. Oncobretagne effectue une déclaration auprès de l'ANS: Cert santé

Vous avez identifié un incident significatif ou grave de sécurité des systèmes d'information les événements générateurs d'une situation exceptionnelle au sein d'un établissement, organisme ou service, vous déclarez sans délai auprès de **l'Agence du Numérique en Santé (ANS)**

- https://signalement.social-sante.gouv.fr
- (Hors période ouvrées) ssi@sg.social.gouv.fr

Le document récapitulatif de votre signalement permet de répondre à l'obligation de documentation interne.

9.2. Dépôt de plainte

Le président d'Oncobretagne veillera à ce qu'en cas d'acte cyber-malveillant, ou suspicion d'un tiers responsable, **une plainte soit déposée sans délais auprès du commissariat** ou de la gendarmerie.

Pré-plainte en ligne (pre-plainte-en-ligne.gouv.fr)

9.3. Oncobretagne effectue une déclaration auprès de la CNIL

Vous avez identifié **une violation** de données à caractère personnel

- Vous avez mis en œuvre un traitement de données personnelles.
- Ces données ont fait l'objet d'une violation (perte de **disponibilité**, **d'intégrité** ou de **confidentialité** de données personnelles, de manière **accidentelle** ou **illicite**

➢ **L'enregistrement** de la violation de données dans un **registre spécifique** est obligatoire

➢ **La notification à la CNIL**

Cette violation engendre **un risque*** pour la vie privée des personnes dans ce cas vous notifiez auprès de la CNIL : **Notification (cnil.fr)**

***Si la violation n'engendre pas d'impact sur la vie privée des personnes : la violation est à inscrire au registre uniquement**

La notification initiale doit être établie dans les meilleurs délais à la suite de la constatation de la violation (sous **24 heures idéalement**)

Puis, une notification complémentaire dans le délai de **72 heures si possible** après la notification initiale.

Dès lors que de nouveaux éléments sont découverts, l'établissement les fait parvenir à la CNIL.

Si l'établissement ne peut pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, il convient de procéder à une notification en deux

Si le délai de 72 heures est dépassé, il conviendra d'expliquer, lors de votre notification, les motifs du retard.

Informations à transmettre à la CNIL

- La nature de la violation de données à caractère personnel y compris, si possible, des catégories et du nombre approximatif de personnes concernées par la violation et des catégories et du nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Le nom et des coordonnées du délégué à la protection des données (DPO OB), ou de tout contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Les conséquences probables de la violation de données à caractère personnel ;

- Les mesures prises ou proposées par le responsable du traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Le document récapitulatif de votre notification à la CNIL permet de répondre à l'obligation de documentation interne.

10.AUTRES DECLARATION

10.1. Assurance

Oncobretagne doit procéder aux déclarations de sinistres en faisant attention à :

- La tenue des délais : généralement 48 heures pour le vol, 5 jours ouvrés au maximum dans la plupart des autres cas,
- Ne rien « toucher » avant la venue de l'expert en assurances sauf nécessité.

En cas d'urgence, on peut remplacer le matériel et mettre le matériel endommagé de côté (cette mesure ne peut être prise qu'en cas d'urgence, afin d'éviter l'arrêt de l'exploitation).

Si le sinistre est important, des photos peuvent ne pas suffire, il faut procéder à un constat par huissier et faire mettre toutes les preuves sous scellés.

11.COMMUNICATION A LA (AUX) PERSONNE(S) CONCERNEE(S)

Par ailleurs, en cas de risque élever pour les personnes concernées, le responsable de traitement doit également informer, en des termes clairs et simples, les utilisateurs touchés par l'incident, sauf si le responsable a pris préalablement ou postérieurement à la violation des mesures techniques ou organisationnelles appropriées.

La communication à la personne concernée doit être claire et simple, et contenir les informations suivantes :

- Le nom et des coordonnées du délégué à la protection des données (DPO), ou de tout contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Les conséquences probables de la violation de données à caractère personnel ;
- Les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Cette communication peut être faite par envoi de mail, communiqué de presse.

Il existe certaines dérogations à la notification des violations de données personnelles aux personnes concernées lorsque :

- Le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux DCP affectées par ladite violation, en particulier les mesures qui rendent les DCP incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

- Le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser (exemple : suite au vol des mots de passe des comptes d'accès au DCC, tous les mots de passe d'accès au compte ont été réinitialisés et un mail a été envoyé aux personnes atteintes pour accéder à leur compte) ;
- Elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

La CNIL peut, si elle l'estime nécessaire, demander au responsable de traitement ne l'ayant pas fait, d'effectuer cette communication.

ANNEXES

ANNEXE 1 : FORMULAIRE – DECLARATION DE VIOLATION DE DONNEES dans le cadre de l'utilisation du dossier communicant de cancérologie de Bretagne

VOUS SOUHAITEZ DECLARER UN INCIDENT DE SECURITE AVEC VIOLATIONS DE DONNEES DANS LE DCC ?

Merci de remplir ce formulaire !!

Ce formulaire doit être envoyé : dpo@oncobretagne.fr et r.ngandjeu-sonnang@oncobretagne.fr

Nom Prénom du déclarant	
Coordonnées de contact (téléphone/mail)	
Date de la déclaration de violation	
Date de l'événement	
Type de violation	☐ Violation de la confidentialité (Accès illicite) ☐ Violation de la disponibilité (erreur) ☐ Violation de l'intégrité (usurpation d'identité, erreur de saisie ..)
Description de la violation et impact sur les perosnnes	
Catégorie de personnes concernées et nombre	
Catégorie de données impliquées / nombre approximatif	
Mesures de sécurité mises en place	

ANNEXE 2 : FICHE SUIVI VIOLATION DE DONNEES PERSONNELLES

I. INFORMATIONS GENERALES

1. Date de la violation
2. Identifiant de la violation
3. Entité juridique concernée
4. Commentaire

II. DESCRIPTION DE LA VIOLATION

1. Nature de la violation
2. Bref descriptif de la violation
3. Source
4. Composants du SI concerné
5. Traitements concernés
6. Catégorie des personnes concernées
7. Le Nombre de personnes concernées
8. Sensibilité des données concernées

III. IMPACTS & RISQUES

1. Disponibilité
2. Intégrité
3. Confidentialité
4. Risques identifiés pour les personnes concernées
5. Niveau de gravité

IV. MESURES PRISES

1. Actions de limitation des impacts
2. Actions de remédiation
3. Actions préventives (Capitalisation)

V. NOTIFICATION CNIL

1. Notification nécessaire
2. Justification (obligatoire en cas de non notification)
3. Date de la première notification
4. Date de la notification complémentaire (si nécessaire)

5. Identifiant de la notification
6. Formulaire CNIL

VI. Notification de l'ARS

1. Justification de la notification
2. Date de la notification
3. Identifiant de la notification

VII. INFORMATION DES PERSONNES CONCERNEES

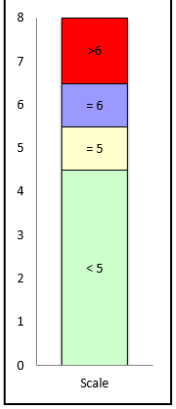
1. Information nécessaire
2. Justification (obligatoire en cas de non-information)
3. Date de la mesure d'information

ANNEXE 3 : QUOTATION DE VIOLATION DE DCP (Modèle)

Caractère identifiant des données ayant fait l'objet de la violation	
Valeur *Les données ayant fait l'objet de la violation permettent-elles d'identifier les personnes concernées ? Apprécier le caractère identifiant des données en choisissant l'une des 4 valeurs suivantes : 1 = négligeable, 2 = limité, 3 = important, 4 = maximal.*	1
Description de chaque valeur	1. Négligeable : il semble quasiment impossible d'identifier les personnes à l'aide des données les concernant (ex. : identifier quelqu'un au sein de la population française en ne connaissant que son prénom)

Caractère préjudiciable de la violation sur les personnes concernées	
Conséquences potentielles de la violation *Quelle est la conséquence potentielle de la violation la plus vraisemblable ? Choisir parmi les sept scenarios proposés.*	Perte de confidentialité : les données ont été ou pourraient être diffusées plus que nécessaire et ont été ou pourraient avoir échappé à la maîtrise des personnes concernées (ex. :diffusion non désirée d'une photo sur Internet, perte de contrôle d'informations publiées dans un réseau social...).
Valeur *Apprécier le caractère préjudiciable de la violation en choisissant l'une des valeurs suivantes : 1 = négligeable, 2 = limité, 3 = important, 4 = maximal.*	3
Description de chaque valeur	3. Important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourraient surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, affection physique ou psychologique grave...)

Gravité
4



Caractère préjudiciable (CP)	
Valeur	**Description des préjudices potentiels**
1	1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, simple contrariété...)
2	2. Limité : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, affection physique ou psychologique mineure...)
3	3. Important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourraient surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, affection physique ou psychologique grave...)
4	4. Maximal : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée ou permanente, décès...)

Conséquences potentielles	
Type	**Libellé**
Perte de confidentialité	Perte de confidentialité : les données ont été ou pourraient être diffusées plus que nécessaire et ont été ou pourraient avoir échappé à la maîtrise des personnes concernées (ex. :diffusion non désirée d'une photo sur Internet, perte de contrôle d'informations publiées dans un réseau social...).
Perte de confidentialité	Perte de confidentialité : les données ont été ou pourraient être corrélées avec d'autres informations relatives aux personnes concernées (ex. : corrélation d'adresses de résidence et de données de géolocalisation en temps réel...).
Perte de confidentialité	Perte de confidentialité: les données ont été ou pourraient être exploitées à d'autres fins que celles prévues et/ou de manière injuste (ex. : fins commerciales, usurpation d'identité, utilisation à l'encontre des personnes concernées...).
Perte d'intégrité	Perte d'intégrité: les données ont été ou pourraient être modifiées en des données invalides, qui ne seront pas utilisées de manière correcte, le traitement pouvant engendrer des erreurs, des dysfonctionnements, ou ne plus fournir le service attendu (ex. : altération du bon déroulement de démarches importantes...).
Perte d'intégrité	Perte d'intégrité : les données ont été ou pourraient être modifiées en d'autres données valides, de telle sorte que les traitements ont été ou pourraient être détournés (ex. : exploitation pour usurper des identités en changeant la relation entre l'identité des personnes et les données biométriques d'autres personnes...).
Perte de disponibilité	Perte de disponibilité : les données ont été ou pourraient être manquantes à des traitements qui ne peuvent plus du tout fournir le service attendu (ex. : ralentissement ou blocage de processus administratifs ou commerciaux, impossibilité de fournir des soins du fait de la disparition de dossiers médicaux, impossibilité pour des personnes concernées d'exercer leurs droits...).
Perte de disponibilité	Perte de disponibilité : les données ont été ou pourraient être manquantes à des traitements et générer des erreurs, des dysfonctionnements, ou fournir un service différent de celui attendu (ex. : certaines allergies ne sont plus signalées dans un dossier médical, certaines informations figurant dans des déclarations de revenus ont disparu, ce qui empêche le calcul du montant des impôts...).

Gravité	
Valeur	**Libellé**
<5	Négligeable
=5	Limité
=6	Important
>6	Maximal