swiss cancer screening

Protection des données

Guide pratique

Swiss Cancer Screening SCS

swiss cancer screening

Table des matières

1. Objectifs du présent document

Les programmes cantonaux de dépistage (ci-après: Programmes) mettent en œuvre l'offre de dépistage du cancer du sein et du côlon dans les cantons qui ont choisi de systématiquement le proposer[1]. Douze cantons proposent le dépistage du cancer du sein, tandis que quatre cantons, bientôt huit, proposent celui du côlon[2]. Dans un cas comme dans l'autre, la Confédération fixe les conditions du remboursement des prestations correspondantes par l'assurance-maladie de base[3]. En revanche, la législation fédérale sur le dépistage ne régit pas ses modalités pratiques.

Le dépistage implique la collecte, puis le traitement, d'une multitude de données personnelles auprès d'un large groupe de personnes. La Loi fédérale sur la protection des données (LPD[4]) encadre ces activités afin d'assurer les droits des personnes concernées, en particulier leurs droits en matière de protection des données. Si, dans un canton, le dépistage est une activité assumée directement par l'autorité publique cantonale, la réglementation cantonale en matière de protection des données s'applique en lieu et place de la LPD.[5]

L'*objectif* assigné à ce Guide est de récapituler les principes et de préciser les obligations en matière de protection des données que les Programmes sont tenus de respecter. Il doit servir d'outil d'orientation aux Programmes et aux membres de Swiss Cancer Screening (SCS). Il s'adresse avant tout au directeur médical et au directeur administratif de chaque Programme, même s'il constitue un outil précieux pour les autres collaborateurs. Le Guide définit notamment les modalités d'utilisation de l'outil informatique commun Multi-cancer Screening Information System (MC-SIS). Cet outil est conçu pour faciliter et gérer les processus administratifs, pour enregistrer les données récoltées, y compris les images, pour analyser et agréger les données en vue du monitorage.

La *structure* de ce Guide est autant que possible calquée sur l'itinéraire du participant. Elle débute avec l'acquisition des noms et adresses des personnes à qui le dépistage s'adresse et termine avec la destruction des données lorsque celles-ci cessent d'être utiles.

Les *annexes* au Guide contiennent un rappel des définitions (Annexe I), un aperçu des bases légales (Annexe II) ainsi qu'un survol des principes relatifs à la protection des données (Annexe III). L'annexe IV fournit des modèles de documents que les Programmes sont invités à reprendre. L'annexe V liste les indicateurs du monitorage national. L'annexe VI rappelle le

[1] Le dépistage est remboursé par les caisses-maladie dans l'assurance-maladie de base à condition qu'il satisfasse aux exigences de l'art. 12e al. 1 let.c OPAS (ordonnance du DFI sur les prestations dans l'assurance obligatoire des soins en cas de maladie). Par renvoi de cet article, la mammographie de dépistage doit satisfaire aux exigences de l'Ordonnance du Conseil fédéral sur la garantie de la qualité des programmes de dépistage du cancer du sein réalisé par mammographie du 23 juin 1999 (RS 732.102.4).

[2] Concernant le cancer du côlon, il existe actuellement un Programme organisé de dépistage dans les cantons d'Uri et Vaud, et une introduction est planifiée en 2019 dans les cantons de Bâle-Ville, Genève, Jura-Neuchâtel et des Grisons.

[3] Art. 26 de la Loi sur l'assurance maladie (LAMal, RS 832.10). L'article 12e de l'Ordonnance sur les prestations de l'assurance des soins (OPAS, RS 832.112.31) précise que la mammographie de dépistage ou le dépistage du cancer du côlon sont pris en charge par l'assurance obligatoire des soins pour les personnes de plus de 50 ans, uniquement dans le cadre d'un Programme organisé de dépistage. Pour la mammographie, les conditions sont fixées par l'Ordonnance du 23 juin 1999 sur la garantie de la qualité des Programmes de dépistage du cancer du sein par mammographie (RS 832.102.4, ci-après Ordonnance sur la garantie de la qualité).

[4] Loi fédérale sur la protection des données (RS 235.1; LPD) du 19 juin 1992; cette loi est actuellement en cours de révision devant le Parlement. La LPD s'applique à toutes les données personnelles, et non pas spécifiquement aux données personnelles médicales. A noter que le Règlement européen sur la protection des données (RGPD) est inapplicable ici car le traitement de données en cause ne relève pas du champ d'application du Règlement.

[5] La LPD ne s'applique pas à l'activité des autorités publiques cantonales, mais uniquement à l'activité des autorités publiques fédérales et des personnes privées.

contenu de la directive de protection des données. L'annexe VII liste les Standard Operating Procedures (SOP) que doit établir chaque Programme. Finalement, l'Annexe VIII fournit une liste des abréviations couramment utilisées.

Le présent Guide est conçu comme un document évolutif qui sera complété et actualisé au minimum tous les deux ans en fonction de l'évolution de la réglementation et des commentaires des Programmes.

2. Obligations des Programmes et du SCS en matière de dépistage

Le dépistage nécessite d'accéder puis de traiter des *données personnelles*, c'est-à-dire des données qui identifient directement la personne (p. ex. via son nom) ou qui permettent son identification par une combinaison ou un recoupement d'informations[6]. Lorsqu'une donnée est qualifiée de personnelle, la loi – qu'il s'agisse de la Constitution, de la loi fédérale sur la protection des données ou des lois cantonales – oblige celui qui la traite à prendre des mesures pour assurer sa confidentialité et pour garantir les droits accordés à l'individu concerné. Les données médicales sont de surcroît considérées comme des données personnelles particulièrement *sensibles* et appellent à ce titre une protection accrue[7].

Le respect des obligations qui découlent de la réglementation en matière de protection des données contribue de manière décisive à la *confiance* du public dans le dépistage. Or, sans confiance du public, le succès du dépistage est menacé. Il est donc essentiel que toutes les parties impliquées assurent le plus haut niveau de protection et de sécurité aux données dont elles ont la maîtrise.

Les étapes critiques au niveau de la protection des données sont :

- Dans une première étape, le Programme s'adresse à l'autorité cantonale (ou aux autorités cantonales/communales) qui maintient le registre des habitants, afin d'obtenir un extrait du registre pour le territoire concerné. Le Programme a besoin, au minimum, des noms, prénoms, adresses et dates de naissance du public-cible concerné (i.e., les personnes éligibles à participer au dépistage). Cette étape est expliquée dans le chapitre 2.1.
- Le public-cible reçoit une invitation pour l'informer de la possibilité de participer à un dépistage. Le chapitre 2.2 détaille les obligations du Programme à ce stade.
- Les personnes qui décident de participer sont incluses dans le programme. Les obligations afférentes à cette étape (consentement éclairé, collecte de données, etc.) sont décrites au chapitre 2.3.
- Les aspects relevant de la protection des données en lien avec l'évaluation des résultats sont examinés au chapitre 2.4.
- Les participants sont informés des résultats de l'examen. Les obligations afférentes à cette étape sont décrites au chapitre 2.5. Après notification d'un éventuel diagnostic de cancer, les interactions entre la personne concernée et l'équipe médicale qui la prend en charge ne sont plus du ressort du Programme.
- Le Programme conserve les données acquises lors des étapes précédentes. Les personnes doivent pouvoir être réinvitées régulièrement. Pour des raisons de contrôle qualité, le programme analyse régulièrement les données. SCS, sur la base des

[6] P. ex. en connaissant la date de naissance et l'adresse d'une personne, il est en général possible de retrouver son identité.
[7] Art. 3 let. c, art. 4 al. 5 et art. 11a al. 3, art. 12 al. 2 let. c, art. 14, art. 35 LPD.

données agrégées et anonymisées, émet également un rapport répertoriant les indicateurs-clés sur une période donnée (voir le chapitre 2.6).

- La loi exclut que des données personnelles soient conservées indéfiniment. Les Programmes doivent donc décider à quel moment les données ne sont plus pertinentes dans le cadre du dépistage et doivent être détruites. Le chapitre 2.7 clarifie les obligations à ce stade.

2.1. Acquisition des données auprès de l'autorité cantonale

Le Programme a besoin de savoir quelles personnes inviter à participer au dépistage, conformément aux conditions de participation définies généralement dans le mandat conféré par l'autorité publique cantonale[8]. Le Programme demande à l'autorité cantonale la liste, parmi le public-cible, de toutes les personnes décédées, des nouveaux arrivants et des personnes ayant déménagé, afin d'éviter d'adresser un rappel d'invitation à une personne inéligible. Dans certains cantons, ces informations ne sont pas centralisées et le Programme est amené à s'adresser à plusieurs instances régionales.

La législation n'autorise la transmission de données personnelles (noms, adresses, âges des personnes, décès) d'une autorité publique à un tiers, ici le Programme, qu'à des conditions strictes. Une disposition dans la loi cantonale[9] doit autoriser explicitement cette transmission ; en d'autres termes, une *base légale* doit autoriser l'autorité cantonale à transmettre les données personnelles et le Programme à les recevoir (principe de la légalité[10]).

Cette base légale peut résider dans une loi cantonale du Parlement ou dans une ordonnance de l'exécutif. Une directive du service administratif cantonal concerné ne suffit pas, à elle seule, à justifier la transmission. Elle peut préciser les modalités de transmission.

Si le droit cantonal ne contient aucune base légale, le Programme doit se renseigner auprès de l'autorité cantonale afin que soit déterminé ensemble le fondement d'une telle transmission. En cas de doute sur l'existence d'une base légale suffisante, le programme peut consulter le Préposé cantonal à la protection des données afin de mettre en place une solution appropriée.

Le Programme importe l'ensemble des informations acquises de l'autorité cantonale dans le logiciel MC-SIS. Il vérifie si possible leur exactitude, par exemple en écartant les dates de naissance invraisemblables (ex. personne née en 1812). Le Programme est invité à définir par écrit le type de vérifications systématiques auquel il procède.

L'importation des données dans MC-SIS constitue un *traitement* de données (au sens de la loi)[11]. Pour être licite, ce traitement doit – lui aussi – être justifié par une base légale qui se trouve dans la loi cantonale régissant le dépistage (voir Annexe II). En effet, en donnant

[8] Selon l'Ordonnance sur la garantie de la qualité, le dépistage doit être proposé par une organisation reconnue par le canton ou les cantons (art. 3 al. 1).
[9] Comme il s'agit d'une transmission par l'autorité publique cantonale, la LPD n'est pas applicable.
[10] Le principe de la légalité veut que l'action de l'Etat repose sur une base légale. Dans le contexte de la protection des données, un traitement de données, quel qu'il soit, doit être licite. La licéité d'un traitement de données peut découler du consentement libre et éclairé de la personne concernée ou d'une base légale autorisant ledit traitement; dans certains cas, un intérêt privé ou public prépondérant peut également justifier le traitement de données, et donc le rendre licite.
[11] En droit fédéral, le traitement de données est défini très largement comme "toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données" (art. 3 let. e LPD). Les lois cantonales ont également des définitions larges de cette notion.

mandat de mettre en place un dépistage, cette loi autorise le Programme correspondant à traiter les données nécessaires à cette fin.

Concrètement, le Programme doit vérifier puis consigner dans sa directive sur la protection des données la ou les bases légales cantonales autorisant son traitement des données personnelles.

2.2. Invitations adressées aux personnes concernées

Une fois que les personnes éligibles à participer au dépistage sont identifiées (public-cible), le Programme doit envoyer à chacune d'elle une invitation par poste[12]. Cette invitation contient une lettre personnalisée (i.e., mentionnant le nom de la personne), une brochure d'information[13], et selon les modalités[14], un formulaire alliant questionnaire de santé et consentement éclairé, et finalement, un coupon-réponse pour les personnes voulant signifier leur refus de participer.

Le Programme peut déléguer une partie de ces activités à un tiers. Un prestataire externe, par exemple un imprimeur, peut ainsi être chargé d'imprimer les invitations et d'assurer leur envoi. A cette occasion, le tiers peut prendre connaissance des données sensibles des personnes concernées. Il est donc crucial qu'il les traite de manière confidentielle (notamment qu'il ne les transmette pas à d'autres), de manière correcte (par ex. qu'il ne se trompe pas dans l'envoi, en transmettant à une personne une invitation destinée à une autre), et de manière sûre (c'est-à-dire qu'il protège ses locaux et ses systèmes de stockage d'un accès non-autorisé, par ex. par des pirates informatiques).

La transmission de données, par exemple le fichier des noms et adresses, par le Programme au tiers doit se faire via un canal sûr : un système d'e-mail crypté, la remise en mains propres d'une clé USB cryptée, un téléchargement sécurisé, etc. Le personnel du Programme doit être sensibilisé à cette particularité.

Parce que le Programme a délégué à ce tiers une tâche qui lui appartient, la loi l'oblige à superviser le tiers ainsi que son traitement de données[15]. En d'autres termes, le Programme ne peut pas simplement « faire confiance » au tiers, mais il doit prendre des mesures concrètes pour assurer le respect constant de la protection des données. A cet égard, pour que la transmission des données personnelles du Programme au tiers soit licite; **elle doit se fonder sur un contrat écrit de collaboration. Ce contrat doit énoncer précisément les tâches déléguées et les obligations du tiers en matière de sécurité et de protection des données.** Le contrat doit être tenu à jour, en fonction notamment des évolutions techniques. **Il est joint comme annexe à la Directive sur la protection des données propre à chaque Programme.** Par ailleurs, cette Directive indique les rôles et attributions en rapport avec cette collaboration externe (par ex. qui transmet le fichier au tiers et quand, qui vérifie l'envoi quand et comment, etc.).

---

[12] Voir art. 5 de l'Ordonnance sur la garantie de la qualité.
[13] Voir annexe IV.
[14] Certains Programmes utilisent un questionnaire électronique ; le consentement éclairé pour le dépistage du cancer colorectal se fait en présence d'un médecin de famille, d'un pharmacien ou par Internet.
[15] En droit fédéral, l'art. 10a LPD prévoit: "Le traitement de données personnelles peut être confié à un tiers pour autant qu'une convention ou la loi le prévoie et que les conditions suivantes soient remplies:
a. seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués;
b. aucune obligation légale ou contractuelle de garder le secret ne l'interdit.
[2] Le mandant doit en particulier s'assurer que le tiers garantit la sécurité des données."

2.3. Documents adressés aux personnes concernées, consentement et examen de dépistage

2.3.1. Invitation du public-cible

L'invitation adressée aux personnes concernées (public-cible) doit leur permettre de prendre une décision sur leur participation. Cette décision doit être libre et informée[16]. Chaque personne doit donc recevoir par écrit des informations précises sur les modalités, les avantages et les inconvénients du dépistage ; chaque personne doit ensuite pouvoir obtenir des réponses orales à ses (éventuelles) questions, elle peut notamment interroger le personnel d'accueil et le personnel de santé. Son choix doit se faire libre de toute influence. Même après avoir donné son consentement (en l'occurrence par écrit[17]), la personne reste libre de changer d'avis et donc de le révoquer[18] (à ce sujet, voir le chapitre 2.5.5). Elle n'a pas à justifier ou motiver son choix.

S'agissant des tâches incombant au Programme, celui-ci doit tout d'abord arrêter le contenu de la lettre d'invitation, de la brochure qui l'accompagne et du formulaire adressés par poste au public-cible. Les informations communiquées doivent être compréhensibles, complètes, et équilibrées dans leur contenu. En cas de doute sur le contenu ou la forme, le Programme peut contacter la commission cantonale (ou intercantonale) d'éthique en matière de recherche sur l'être humain, laquelle peut fournir des conseils en la matière[19]. Le programme peut également consulter le Préposé cantonal à la protection des données. SCS a mis au point des **modèles** multilingues pour la brochure d'information que les Programmes peuvent utiliser, éventuellement après les avoir adaptés.

Concrètement, le Programme doit faire figurer ces trois documents en annexe à sa Directive_PD.

2.3.2. Inclusion/Rendez-vous pour un examen

Les modalités d'inclusion varient en fonction du type de dépistage : l'invitation au dépistage du cancer du sein autorise les participantes à prendre rendez-vous auprès d'un institut de radiologie ; l'invitation au dépistage du cancer du côlon renvoie à une consultation avec un médecin de famille, un pharmacien ou via une plate-forme Internet. La personne qui inclut le participant entre les données personnelles dans MC-SIS.

Lorsque la personne se rend à l'institut de radiologie (mammographie pour le dépistage du cancer du sein) ou à l'institut/au cabinet de gastroentérologie (colonoscopie pour le dépistage du cancer du côlon) (ci-après: institut), elle est invitée à poser ses questions et reçoit les

[16] Selon la LPD, "Lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée." (art. 4 al. 5, 1ère phrase, LPD).
[17] Comme les données traitées sont sensibles, le consentement de la personne concernée doit être donné par écrit. Cf. art. 4 al. 5 in fine LPD.
[18] La partie "consentement" du formulaire indique "Nous attirons votre attention sur le fait que votre consentement peut être retiré en tout temps".
[19] Si le dépistage ne tombe pas sous la notion de recherche médicale au sens de la LRH (Loi sur la recherche sur l'être humain du 30 septembre 2011; RS 810.30), les commissions d'éthique de la recherche demeurent habilitées à fournir des conseils en dehors du champ d'application de la LRH. Cf. art. 51 al. 2 LRH. Elles jouissent d'une large expérience en matière de vérification des formulaires d'information et de consentement utilisés dans la recherche. Cette expérience peut être mise à profit également dans le contexte du dépistage.

réponses correspondantes. A moins qu'elle n'ait changé d'avis, elle remet le formulaire de consentement signé sur un support papier ou électronique (e-Quest).

Le personnel de l'institut vérifie ou complète les réponses sur son statut personnel[20], sur sa caisse-maladie[21] et son état de santé actuel et passé. Les données récoltées directement auprès d'elle à ce stade sont : les antécédents médicaux et familiaux et les symptômes éventuels[22]. La personne doit indiquer le nom et les coordonnées d'un médecin de son choix (médecin de référence) à qui le résultat du dépistage sera envoyé directement par le Programme[23]. La personne est invitée à apposer sa signature sur un formulaire pour marquer son consentement. Ce consentement autorise l'échange et l'évaluation des données nécessaires au bon déroulement du dépistage[24].

Le personnel de l'institut recense les anomalies cliniques et les difficultés techniques rencontrées lors de l'examen ; il les consigne dans MC-SIS. Ces données sont considérées comme pertinentes et proportionnées par rapport à l'objectif, c'est-à-dire qu'elles sont nécessaires pour assurer le meilleur dépistage possible dans l'intérêt de la santé individuelle et publique[25].

Si la personne refuse de donner son consentement, et notamment son consentement à l'utilisation des données et à la transmission au médecin de référence, elle ne peut pas participer au dépistage. Le questionnaire de santé doit attirer l'attention sur ce point. La personne peut en tout moment revenir sur sa décision (à ce sujet, voir le chapitre 2.5.5). A cet égard, elle peut indiquer si son refus doit être compris comme définitif, dans quel cas elle ne recevra plus les lettres d'invitation à participer au dépistage. Son refus est entré dans MC-SIS afin d'assurer le respect de sa volonté, ce qui signifie que cette donnée personnelle est conservée durablement.

La relation entre le Programme et l'institut ainsi que tous les prestataires de services œuvrant dans le cadre d'un Programme (radiologues, pathologistes, médecins de famille, pharmaciens, laboratoires qui analysent le test FIT) doit faire l'objet d'un contrat écrit. Ce contrat doit définir les obligations et droits de chaque partie. S'agissant des aspects afférents à la protection des données, **le contrat doit préciser comment le prestataire de services garantit la protection des données et les droits des personnes concernées. Il doit notamment inclure une clause de confidentialité, laquelle garantit que l'institut et ses collaborateurs maintiendront strictement confidentiels les données personnelles et autres informations acquises dans le cadre du dépistage. Ces contrats doivent être tenus à**

[20] A l'heure actuelle, la personne doit fournir son nom, prénom, nom de célibataire, date de naissance, adresse, téléphones, nationalité et numéro AVS.
[21] A l'heure actuelle, la personne doit en principe indiquer le nom de sa caisse-maladie de base et son numéro d'assuré.
[22] Plus précisément, la personne est invitée en principe à répondre aux questions suivantes: a-t-elle déjà effectué une mammographie, suit-elle un traitement hormonal pour la ménopause, y a-t-il eu des cas de cancer du sein dans la famille, souffre-t-elle ou a-t-elle souffert de problèmes au sein?
[23] Si la personne ne souhaite pas indiquer de médecin de référence, le responsable médical du programme peut exceptionnellement occuper cette fonction.
[24] Ainsi, la personne accepte que ses données personnelles soient envoyées par l'institut au centre de dépistage, au registre des tumeurs, au médecin de référence, au programme de dépistage du nouveau canton de domicile en cas de déménagement. Elle accepte également que ses données soient stockées et archivées. Elle accepte enfin que ses données soient anonymisées pour être ensuite analysées à des fins statistiques, de qualité et de formation. De plus, les données sont transmises aux caisses-maladie.
[25] En droit suisse, tout traitement de données doit être proportionné (principe de proportionnalité). Ce principe implique que le traitement doit se limiter au strict minimum, qu'il s'agisse de l'ampleur des données récoltées, du cercle des personnes auprès desquelles elles sont collectées, du cercle des personnes habilitées à les traiter, de l'ampleur des opérations effectuées sur ces données et de leur durée de conservation, tout en permettant d'atteindre le but recherché.

jour et être annexés à la Directive sur la protection des données propre à chaque programme.

2.3.3. Eventuelle collecte de données supplémentaires

La législation en matière de protection des données exige que seules les données strictement nécessaires à l'objectif attribué soient collectées et traitées[26]. Il arrive qu'un Programme souhaite récolter de manière systématique des données *supplémentaires*. Une telle récolte de données additionnelles doit se justifier par un besoin dûment établi par le Programme ; elle doit de surcroît être proportionnée. Le but du traitement des données doit aussi être reconnaissable pour la personne ayant consenti et il doit ensuite demeurer inchangé (principe dit de *finalité*)[27].

A noter qu'il n'est pas licite de collecter, dans ce contexte, des données supplémentaires *à des fins de recherche*, car ceci requiert un consentement spécifique du participant à la recherche (chapitre 2.5.9)[28]. En effet, lorsque le but visé est la recherche, le participant doit être informé au préalable que ses réponses seront analysées à cette fin et doit donner son accord libre, informé et écrit. Une autorisation de la commission d'éthique compétente en matière de recherche médicale doit alors être requise et obtenue[29]. La frontière entre la recherche et le contrôle-qualité n'est pas toujours nette[30]. Cependant, si au moment de la collecte, l'institut ou le Programme ne peut justifier que les données supplémentaires sont directement pertinentes à des fins de dépistage, mais qu'il entend encore tester ou évaluer la pertinence de cette collecte, la qualification de recherche s'impose.

Si le Programme entend récolter des données supplémentaires, il **doit rédiger une SOP** qui décrit comment les données sont collectées et comment ces informations supplémentaires seront ensuite traitées pour atteindre le but d'améliorer le dépistage (ci-après **SOP-1**). Ce document explique également comment et par qui ces données supplémentaires seront périodiquement évaluées. **Ce document est joint à la Directive_PD. Le Programme communique cette SOP-1 au SCS qui coordonne au besoin l'adjonction d'un champ à compléter dans le MC-SIS.**

2.4. Résultats médicaux

La présente section est divisée en six sous-chapitres. Tout d'abord, l'exactitude des données récoltées durant la visite à l'institut de la personne concernée doit être contrôlée[31]. Les

[26] En droit fédéral, tout traitement de données "doit être effectué conformément aux principes de la bonne foi et de la proportionnalité". Art. 4 al. 2 LPD.
[27] En droit fédéral, selon les alinéas 3 et 4 de l'art. 4 LPD, "Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.
La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée." En d'autres termes, la personne doit savoir que ses données sont collectées et doit être renseignée sur le but de la collecte. Ce but tel qu'il lui a été indiqué ne peut ensuite en principe plus être modifié.
[28] Une recherche dans le domaine médical est soumise à la LRH. Or, cette loi exige, à de rares exceptions près, que le participant à la recherche donne son consentement. Art. 7 LRH.
[29] Art. 45 LRH.
[30] Cf. SwissEthics (Commissions d'éthique suisses relatives à la recherche sur l'être humain), Groupe de travail n° 19 : Clarification des compétences. Sous www.swissethics.ch/doc/ab2014/Zustaendigkeit_f.pdf
[31] La législation fédérale en matière de protection des données pose un principe d'exactitude. Selon l'art. 5 al. 1 LPD, "Celui qui traite des données personnelles doit s'assurer qu'elles sont correctes. Il prend toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées." Les législations cantonales contiennent généralement une règle similaire.

données de mammographie sont examinées par deux, voire trois, radiologues[32]. Les résultats du dépistage du cancer colorectal sont évalués par le laboratoire (FIT) ou le gastroentérologue/pathologiste (colonoscopie). Enfin, les résultats sont transmis au participant et au médecin de référence indiqué. Si le participant n'a pas indiqué de médecin de référence, le directeur médical du programme fournit des conseils médicaux. Le médecin de référence ou d'autres médecins-traitants demandent parfois à recevoir certaines informations complémentaires. La transmission d'informations aux autorités cantonales et fédérales est abordée au chapitre 2.6 ci-dessous.

2.4.1. Contrôle des données

L'institut doit vérifier la plausibilité des données qu'il collecte directement.

De plus, le Programme contrôle les données saisies par l'institut dans MC-SIS, notamment pour leur cohérence interne. MC-SIS permet d'exporter des tableaux avec des données individuelles pour permettre aux Programmes d'effectuer leurs propres validations. De telles validations sont fortement recommandées.

Pour assurer la qualité de sa démarche, le Programme doit rédiger une SOP décrivant les étapes de sa vérification (notamment, qui vérifie quoi, comment, qui corrige quoi, comment, qui supervise quoi et comment) (SOP-2).

2.4.2. Échange de données entre partenaires internes

L'échange de données personnelles entre partenaires internes au dépistage – par exemple les collaborateurs du Programme, le personnel des laboratoires, les radiologues, les gastroentérologues ou les pathologistes– se fait en principe dans MC-SIS. Les individus concernés doivent être spécifiquement autorisés à échanger et à accéder aux données. Cette autorisation doit être décrite **dans la matrice des droits d'accès de chaque Programme et figurer dans une SOP**. Le type et le contenu de l'échange de données sont en principe dictés par MC-SIS. Ces échanges font l'objet des mesures de sécurité incorporées dans le logiciel et décrites dans le concept de sécurité de CDI.

Ces échanges de données sont licites car basés sur la législation cantonale régissant le dépistage, ce que chaque Programme doit cependant vérifier. Ces transferts sont également proportionnés au but poursuivi, à savoir offrir au public-cible un dépistage de qualité.

2.4.3. Analyse des données et diagnostic médical[33]

Les professionnels chargés d'établir le diagnostic ont accès à l'ensemble des données collectées (données démographiques, anamnèse, images, tests de laboratoire) et saisissent le diagnostic dans MC-SIS.

Concrètement, le Programme doit s'assurer avoir conclu des contrats écrits non seulement avec l'institut (chapitre 2.3.2)**, mais aussi avec les prestataires de services externes chargés d'effectuer des tests (par ex. laboratoires, pathologistes, médecins de famille, pharmaciens) ou d'analyser des données (par ex. radiologues,**

[32] Voir l'art. 4 de l'Ordonnance sur la garantie de la qualité.
[33] Il s'agit généralement d'une analyse de risque qui conclut à une suspicion de cancer, le diagnostic définitif étant effectué lors des examens complémentaires après biopsie et examens de pathologie.

gastroentérologues). Ces contrats (ou cahiers des charges) doivent décrire précisément les tâches attendues. Ils doivent inclure une clause de confidentialité, laquelle garantit que les partenaires externes et leurs collaborateurs maintiendront strictement confidentielles les données personnelles et autres informations acquises dans le cadre du dépistage. Ces contrats sont tenus à jour et **sont inclus en annexe à la Directive sur la protection des données propre à chaque programme.**

Cet échange de données du Programme avec les personnes chargées du diagnostic via MC-SIS est licite, car fondée sur la loi cantonale régissant le dépistage. Le consentement éclairé de la personne concernée couvre également cet échange de données, qui est nécessaire et proportionné au but recherché.

L'échange de données personnelles qui s'opère par d'autres canaux que MC-SIS est à éviter. Par exemple, l'envoi par téléphone, e-mail, par le biais de clés USB ou de CD_ROM ne présente pas les mêmes garanties de sécurité que l'échange par MC-SIS. Dans pareils cas, le Programme doit assurer le même niveau de protection que celui de MC-SIS (par ex. avec un e-mail crypté). Sa Directive_PD doit expliciter comment ce niveau de protection est garanti.

2.4.4. Transmission des résultats à la personne concernée

Le directeur médical du Programme est responsable de communiquer par courrier à la personne concernée ou à son médecin référent les résultats du dépistage (résultat FIT avec colonoscopie, colonoscopie, mammographie). Ce résultat est transmis en principe dans les 8 jours après la visite de la personne[34]. Souvent, le résultat positif (suspicion de cancer) est transmis 24 heures à l'avance au médecin de référence que la personne concernée a mentionné sur le formulaire de consentement. Cette transmission anticipée permet au médecin de prendre contact avec la personne afin de répondre à ses questions éventuelles.

Si le résultat est positif, le courrier invite la personne concernée à contacter le ou les médecins de son choix[35]. La suite de son traitement est décidée d'entente entre la personne et son équipe médicale, sans que le Programme ou l'institut ne soient impliqués.

Lorsque le résultat est négatif (pas de suspicion de cancer), la personne concernée et son médecin sont informés. Elle est invitée à continuer à participer régulièrement au dépistage.

Si l'impression et/ou l'envoi sont délégués à un prestataire externe, les explications figurant au chapitre 2.2 doivent être respectées (notamment en ce qui concerne le contrat écrit).

2.4.5. Echange ultérieur d'informations

La personne concernée ou ses médecins-traitants communiquent parfois spontanément au Programme ou à l'institut des informations sur le suivi médical ultérieur. Ces informations peuvent être entrées dans le système MC-SIS. Elles sont considérées licites, la démarche active de la personne ou de ses médecins (agissant avec l'accord présumé de la personne) valant consentement au traitement des données.

Il arrive aussi qu'un professionnel de la santé autre que le médecin de référence, notamment un oncologue chargé du suivi de la personne, contacte directement un Programme en

[34] Voir l'art. 9 al. 1 de l'Ordonnance sur la garantie de la qualité.
[35] Voir l'art. 9 al. 2 de l'Ordonnance sur la garantie de la qualité.

demandant à recevoir des données relatives à son ou sa patiente. Le Programme ne peut répondre à cette demande que s'il reçoit une **autorisation explicite** de la personne concernée (en principe, une autorisation écrite et signée de la personne justifiant de son identité par une copie de son passeport ou de sa carte d'identité). Le Programme ne peut *pas spontanément renseigner* le professionnel de la santé, même si celui-ci se dit dûment habilité par son ou sa patiente. S'il détient l'autorisation du patient ou de la patiente, le Programme utilise alors un canal sûr pour transmettre l'information requise au professionnel de la santé (p. ex. e-mail crypté, clé USB cryptée, réseau HIN (« Health Info Net »), carte CPS de la FMH[36]). Le Programme doit au moins s'assurer que l'adresse électronique indiquée est bien celle du professionnel en question.

2.4.6. Communication à l'étranger

Ni les Programmes, ni le SCS ne transmettent en principe de données personnelles à l'étranger.

La personne concernée peut toutefois demander explicitement au Programme que ses propres données lui soient envoyées à l'étranger ou soient communiquées à son mandataire, généralement un médecin, à l'étranger. Cette situation peut survenir notamment lorsque la personne déménage et que son traitement médical se poursuit à l'étranger.

Dans ces situations rares en pratique, la communication a lieu conformément aux instructions de la personne et est licite sur la base de son consentement. En général, un CD-ROM contenant ses données est gravé et lui est remis. Le Programme doit aussi vérifier que les instructions émanent bien de la personne dont les données personnelles sont en cause ou de son mandataire dûment habilité. Au besoin, le Programme peut souhaiter attirer l'attention de la personne sur les risques d'une transmission à l'étranger.

2.5. Stockage des données, mesures de sécurité et droit d'accès, monitorage

Le présent chapitre traite des étapes qui suivent le retour des résultats à la personne concernée. Il est scindé en neuf parties. La première concerne les mesures visant à garantir la sécurité des données récoltées et traitées par les Programmes, elle aborde également le thème des droits d'accès par leurs collaborateurs. La deuxième partie envisage la désignation d'un conseiller à la protection des données au sein du Programme. La troisième clarifie l'accès aux données personnelles par SCS.

La quatrième partie rappelle que les personnes concernées ayant participé au dépistage ont le droit d'accéder à leurs propres données. Sont traitées à la suite (cinquième partie) les questions liées à la révocation du consentement et aux demandes d'effacement de données formulées par ces personnes.

Les parties six à neuf visent la communication à des tiers ; sont notamment abordés l'annonce du fichier au Préposé à la protection des données et la communication des données à d'autres autorités, en particulier les registres cantonaux des tumeurs et l'OFSP.

[36] FMH, Bases juridiques pour le quotidien du médecin, Un guide pratique, p. 105.

2.5.1. Sécurité et accès par les collaborateurs des Programmes

Les données collectées par le Programme et ses partenaires sont conservées dans le système MC-SIS. Le Programme peut en tout temps accéder aux données qu'il a entrées. Il ne peut pas accéder aux données personnelles d'un autre Programme.

Tant pour des raisons légales qu'éthiques, il est capital que ces données soient maintenues strictement sûres et confidentielles[37]. De plus, ces données ne doivent être utilisées que dans le cadre strictement nécessaire au but annoncé aux personnes participantes (principes dits de proportionnalité et de finalité)[38].

Dans la pratique du dépistage, les deux principales catégories de risques identifiés sont les défaillances techniques (pannes informatiques et autres dysfonctionnements provoquant des erreurs ou des pertes de données) et les actes malintentionnés ou négligents (manipulation des données, mauvais usage, vol, perte de formulaires).

Concrètement, le Programme doit adopter une Directive_PD complétée par une matrice des droits d'accès et une SOP. Conjointement, ces documents précisent qui est habilité à accéder à quelles données (notamment sur MC-SIS), quand, comment et à quelles fins. La matrice des droits d'accès énonce le nom de chaque collaborateur ayant un droit d'accès à des données personnelles et l'étendue de ce droit. Seules les personnes ayant réellement besoin, pour l'accomplissement de leurs tâches, d'accéder à des données personnelles doivent recevoir cette autorisation d'accès; leur nombre doit être aussi réduit que possible. Chaque accès informatique doit être individuel (c'est-à-dire propre à l'employé concerné et sans partage possible) et traçable[39]. **Chaque collaborateur du Programme, même s'il n'a pas de droit d'accès attribué par la matrice, doit signer un engagement écrit de confidentialité.**

Toujours dans le but d'empêcher des personnes externes au Programme d'accéder aux données personnelles, la Directive_PD et la matrice des droits d'accès doivent également décrire la politique d'accès aux locaux et différentes pièces des Programmes, la politique de gestion des documents écrits (notamment les formulaires papier remplis par les participants), la politique de gestion des imprimantes et l'accès des visiteurs aux locaux. **Le Programme doit définir des mesures de sécurité et d'identification, de sorte que les personnes non autorisées n'entrent pas dans les bâtiments ou parties de bâtiments (notamment les sites où se trouvent les terminaux d'accès au MC-SIS).** En principe, les visiteurs doivent être pré-annoncés, approuvés et contrôlés. Ils doivent être accompagnés dans les locaux.

La matrice des droits d'accès doit être régulièrement tenue à jour, notamment concernant les modifications des droits d'accès liées à l'arrivée et au départ de collaborateurs. La SOP correspondante décrit la procédure de mise à jour des droits d'accès (qui accorde le droit d'accès, sur la base de quel processus, qui effectue les contrôles, **SOP-3**).

Une tâche essentielle attribuée au responsable de Programme est la sensibilisation de ses collaborateurs. L'expérience montre que la majorité des cas de divulgation illicite ("security breach") de données est le fait de collaborateurs, généralement en raison d'une négligence, elle-même attribuable à un manque de formation. Le Programme doit donc former ses collaborateurs aux enjeux de la protection des données. La formation suit la prise de

[37] En droit fédéral, selon l'art. 7 al. 1 LPD, "[l] es données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées." Les mesures de sécurité sont également explicitées aux art. 8 à 11 OLPD.
[38] Voir l'art. 4 LPD déjà cité.
[39] Art. 9 OLPD.

fonction et est réitérée à intervalles réguliers tant que dure la relation entre le collaborateur et le Programme ou les différents prestataires de services. La formation doit préciser l'étendue du secret et de l'obligation de confidentialité, les mesures concrètes à adopter et à éviter, les risques les plus courants, les sanctions en cas de violation.

Enfin, il incombe au directeur médical ou au directeur administratif du Programme de vérifier ou de faire vérifier régulièrement le respect de la Directive_PD, de la matrice des droits d'accès et de la SOP-3, ainsi que des obligations qu'elles énoncent. Il vérifie notamment que seules les personnes autorisées à accéder aux données personnelles y ont accédé.

2.5.2. Conseiller à la protection des données

Les Programmes peuvent vouloir désigner un conseiller indépendant à la protection des données[40] ayant pour tâche de vérifier le respect de la législation ainsi que des politiques et procédures internes en matière de protection des données. Ce conseiller peut être un mandataire externe au Programme ou un collaborateur interne du Programme, à la condition que ce dernier jouisse de l'indépendance nécessaire. Si un conseiller à la protection des données est désigné, ses tâches sont clairement définies par écrit.

2.5.3. Accès aux données par SCS

SCS n'accède pas aux données personnelles des Programmes, il n'accède tout particulièrement pas aux données des personnes ayant été invitées ou ayant participé au dépistage. Les Programmes sont d'ailleurs priés de ne pas envoyer de telles données personnelles à SCS. Si un tel échange s'avère inévitable, les données doivent être anonymisées.

SCS doit recevoir des programmes des données agrégées et/ou pseudonymisées. SCS peut ainsi émettre périodiquement un rapport de monitorage qui présente les résultats du dépistage en fonction d'indicateurs statistiques[41]. A cette fin, SCS peut mandater des experts externes qui analysent lesdites données. La collaboration entre SCS et ces experts est réglée par un contrat écrit qui inclut une clause de confidentialité, étant précisé que les experts n'accèdent pas à des données personnelles, mais uniquement pseudonymisées. Le rapport qui en résulte est public.

Par ailleurs, SCS est chargé de veiller à la sécurité technique des données via MC-SIS. A cette fin, SCS a mandaté CDI pour élaborer un **concept** de sécurité décrivant les mesures techniques de sécurité mises en place dans MC-SIS. Le Préposé à la protection des données bernois a validé ce document. Ce dernier est mis à disposition des préposés cantonaux à la protection des données qui le requièrent. **Ce concept de sécurité de CDI décrit les méthodes (organisationnelles et techniques) de sécurité (journalisation, sauvegarde régulière, prévention du hacking) en lien avec l'accès et le traitement des données.**

[40] Art. 11a al. 5 let. e LPD re art. 12a et 12b OLPD.
[41] Voir par exemple SCS, Rapport de monitorage 2012 des programmes suisses de dépistage du cancer du sein, un bref bilan.

2.5.4. Droits d'accès des personnes concernées

La loi accorde à chaque personne le droit de demander si des données la concernant sont traitées et si oui, quelles données exactement[42]. Ce droit bénéficie à toute personne, donc y compris celles n'ayant pas participé au dépistage. La personne doit adresser sa demande d'accès directement au Programme. Si elle adresse sa demande à l'institut, celui-ci la transmet au Programme.

La personne peut exiger une copie (écrite) de son dossier, c'est-à-dire de *toutes* les données la concernant en main du responsable du fichier (aussi appelé « maître du fichier »). Ce droit n'est donc pas limité aux données que la personne a elle-même fournies, mais s'étend également aux données obtenues de tiers (par exemple des médecins experts)[43]. L'origine de telles données doit être indiquée[44]. Le Programme doit également préciser à la personne requérante le but du fichier[45].

Si la personne concernée constate des erreurs dans ses données, elle peut les signaler et exiger leur correction[46]. De nouveau, la personne doit s'adresser au Programme. Si elle s'adresse à l'institut, celui-ci la renvoie au Programme.

Concrètement, le Programme cantonal doit établir une SOP (SOP-4) qui décrit comment il traite les demandes d'accès et les demandes de correction. Celle-ci aborde notamment la manière de formuler la demande et d'établir l'identité de la personne requérante (en principe carte d'identité ou passeport[47]), détermine qui traite la demande, comment l'information est ensuite transmise à la personne, sous quelle forme et dans quel délai (maximum 30 jours à compter de la demande[48]).

Les données sont en principe transmises gratuitement[49]. Si la remise n'a pas lieu en mains propres, elle se fait via un support sûr, par exemple un e-mail crypté, en ayant dûment vérifié

[42] En droit fédéral, ce droit d'accès découle de l'art. 8 LPD et est explicité aux art. 1 et 2 OLPD. Selon l'art. 8 alinéa 1 LPD, "[t]oute personne peut demander au maître d'un fichier si des données la concernant sont traitées." L'alinéa 2 décrit les données que le maître du fichier doit fournir en réponse à une telle requête. L'alinéa 3 autorise la transmission de données médicales par l'intermédiaire d'un médecin, plutôt que directement à la personne concernée si celle-ci le souhaite. L'alinéa 4 règle la situation lorsque le maître du fichier a sous-traité certaines activités à un tiers. Les informations fournies en réponse à une demande d'accès doivent l'être en principe gratuitement, selon l'alinéa 5. Finalement, l'alinéa 6 précise qu'il s'agit là d'un droit inaliénable de la personne. Les cas de figure où le maître du fichier peut refuser de faire droit à une demande d'accès sont décrits à l'art. 9; cependant, dans le cas du dépistage, aucune exception n'entre en principe en considération.

[43] En revanche, le Programme n'a pas à requérir auprès de tiers des données qu'il ne détient pas lui-même, quand bien même la personne concernée en fait la demande.

[44] En droit fédéral, l'art. 8 al. 2 let. a LPD prévoit: " Le maître du fichier doit lui communiquer: a. toutes les données la concernant qui sont contenues dans le fichier, y compris les informations disponibles sur l'origine des données."

[45] En droit fédéral, voir l'art. 8 al. 2 let. b LPD. Le programme est tenu de communiquer toutes les données concernant la personne qui sont contenues dans le fichier, y compris les informations sur l'origine des données ; le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, les participants au fichier et les destinataires des données (personnes et organes auxquelles les données sont communiquées). Préposé fédéral à la protection des données et à la transparence (PFPDT), Droits de la personne concernée en matière de traitement des données personnelles, p. 7.

[46] En droit fédéral, l'art. 5 al. 2 LPD prévoit que "[t]oute personne concernée peut requérir la rectification des données inexactes."

[47] La demande doit en principe être faite par écrit (cf. en droit fédéral art. 1 al. 1 OLPD). Il faut, pour des raisons de preuve, la copie d'une pièce d'identité annexée à la demande et l'envoi de la demande par pli recommandé. La demande d'accès et la communication des renseignements demandés peuvent être faites par voie électronique (art. 1 al. 2 OLPD), pour autant que le Programme le prévoie expressément et qu'il prenne des mesures adéquates afin d'assurer l'identification de la personne concernée et de protéger les données de la personne concernée de tout accès de tiers non autorisés lors de la communication des renseignements (art. 1 al. 2 OLPD). La personne peut également venir au secrétariat du centre de dépistage munie d'une pièce d'identité. Une situation particulière vise les demandes faites par des membres de la famille de la personne concernée, lorsque celle-ci est décédée (à ce sujet art. 1 al. 7 OLPD).

[48] Art. 1 al. 4 OLPD.

[49] Les renseignements sont, en règle générale, fournis gratuitement et par écrit, sous forme d'imprimé ou de photocopie (art. 1 OLPD et exception à l'art. 2 OLPD). Les données médicales et les images de mammographie

l'exactitude de l'adresse e-mail. En principe, le Programme ne peut refuser ou limiter la demande portant sur l'existence de données personnelles, la demande d'accès à ces données ou encore la demande de correction des données.

2.5.5. Révocation du consentement

La personne concernée qui a consenti à prendre part au dépistage peut en tout temps révoquer son consentement. Elle communique sa décision en principe au Programme ; si elle a communiqué sa décision à l'institut, par exemple sur place lors de la visite, celui-ci la transmet au Programme. Le Programme doit s'assurer que la manifestation de volonté reçue a bien été émise par la personne habilitée à le faire (p. ex. vérification de l'identité).

Si le test et l'analyse ont déjà eu lieu et les résultats ont été transmis, la révocation du consentement n'a toutefois que des effets limités. Aucun traitement ultérieur n'a lieu. Le Programme doit légalement conserver et archiver le dossier complet. Il ne peut donc pas effacer entièrement les données, même si la personne le lui demande.

Si l'analyse des données, notamment des images, n'a pas encore eu lieu au moment de la réception de la révocation, le Programme interrompt le traitement des données. Celles-ci ne sont pas transmises aux médecins spécialistes ni à d'autres tiers. Elles sont uniquement conservées à des fins d'archivage.

Si, au moment de la déclaration de révocation, l'analyse a déjà eu lieu mais que le résultat n'a pas encore été communiqué, le résultat n'est pas communiqué. Le Programme peut s'assurer auprès de la personne qu'elle a pris à cet égard une décision informée. Il doit cependant veiller à respecter son droit de ne pas savoir. Il ne peut donc pas lui imposer une information qu'elle ne souhaite pas recevoir, quand bien même le résultat du dépistage serait positif.

La personne peut aussi décider qu'elle ne souhaite plus être invitée à participer au dépistage. Dans ce cas, le Programme prend note et respecte sa décision. Une mention correspondante est entrée dans MC-SIS.

La personne peut également révoquer sa révocation, c'est-à-dire consentir à nouveau au traitement de ses données. Dans ce cas, la procédure reprend son cours. Par exemple, si les données n'ont pas été soumises aux médecins experts pour analyse, elles le sont dès que la personne consent à nouveau. Est réservé le cas où les données sont alors trop anciennes pour être utilement analysées.

2.5.6. Communication aux Préposés cantonaux à la protection des données

Certaines lois cantonales exigent que la collecte de données personnelles, tout particulièrement de données médicales sensibles, soit annoncée. Cela concerne également les programmes de dépistage. Le Programme doit se renseigner si le canton ou le Préposé ont introduit des exigences et des procédures particulières.[50]. **Le document par lequel le**

peuvent être fournies sur CD-ROM. Une participation aux frais (maximum CHF 300.-, art. 2 al. 2 OLPD) peut être demandée exceptionnellement par le Programme (art. 2 al. 1 OLPD) lorsque la personne a déjà obtenu les renseignements demandés dans les douze derniers mois (sauf si elle a un intérêt légitime à refaire une demande d'accès), et lorsque la communication des renseignements occasionne un volume de travail considérable (par exemple si les données ont déjà été rendues partiellement anonymes ou nécessitent de longues recherches).

[50] Typiquement, l'annonce au Préposé cantonal contient les éléments suivants : les nom et adresse du maître du fichier, le nom et la dénomination complète du fichier, la personne ou l'organe auprès duquel peut être exercé le

programme annonce sa collecte de données au Préposé cantonal doit être consigné par écrit et annexé à sa Directive_PD.

Pour les programmes qui sont organisés sous la forme d'une entité de droit privé (par opposition à une autorité publique) et qui ne sont pas tenus par le droit cantonal d'annoncer leur fichier au Préposé cantonal, il convient de vérifier si une annonce du fichier au Préposé fédéral à la protection des données est requise[51]. **Les Programmes concernés prennent contact avec le Préposé cantonal pour clarifier leurs obligations.**

En principe, aucune donnée personnelle, c'est-à-dire au sujet des personnes concernées (participants), n'est communiquée au Préposé (fédéral ou cantonal).

2.5.7. Communication au registre cantonal des tumeurs

Chaque registre cantonal des tumeurs est habilité par la loi cantonale qui l'institue à recevoir les informations sur les cancers diagnostiqués sur le territoire cantonal. Ces informations lui sont nécessaires pour analyser l'efficacité sur le long terme du dépistage cantonal. En effet, le diagnostic définitif et/ou les informations définitives relatives à la survenue des cancers d'intervalle sont enregistrés uniquement dans ce registre. C'est ainsi qu'il répertorie tous les cas de cancers diagnostiqués sur le territoire cantonal (dans le cadre ou hors du dépistage) et qu'il mène un suivi épidémiologique de ces patients ainsi diagnostiqués.

La transmission audit registre est assurée par le Programme. Le cas échéant, le registre cantonal adresse une confirmation du diagnostic au Programme.

La communication au registre cantonal des tumeurs est licite parce que fondée sur la loi cantonale régissant le dépistage et/ou la loi cantonale instituant le registre cantonal des tumeurs. Cette communication est également proportionnée à l'objectif poursuivi, à savoir assurer la qualité et l'efficacité du dépistage. Ce procédé d'annonce est consigné dans la Directive_PD du programme, cas échéant dans ses annexes.

2.5.8. Monitorage interne du Programme et communication aux autorités

Chaque Programme doit établir un rapport annuel d'activités[52] basé sur des indicateurs de qualité qu'il définit. De plus, SCS a défini un ensemble minimum d'indicateurs qui sont calculés au niveau national [Annexe V]. Ces rapports ne contiennent aucune donnée personnelle, même s'ils sont élaborés à partir des données personnelles auxquelles le Programme accède via MC-SIS.

---

droit d'accès, la base juridique et le but du fichier, les catégories de données traitées (sont indiquées dans cette rubrique les sortes de données contenues dans le fichier, par exemple les nom, adresse, profession, date de naissance), le cercle des personnes concernées et leur nombre approximatif, les catégories de destinataires des données, les catégories de participants au fichier. Le Préposé cantonal peut exiger des éléments ou des informations supplémentaires.

[51] Selon l'art. 11a al. 3 LPD, "Les personnes privées sont tenues de déclarer leurs fichiers dans les cas suivants: a. elles traitent régulièrement des données sensibles ou des profils de la personnalité". Toutefois, l'alinéa 5 de ce même article énonce plusieurs exceptions à l'obligation de déclarer. En droit fédéral, les art. 3 à 4 OLPD précisent le contenu de la déclaration et les exceptions à l'obligation de déclarer.

[52] Cf. art. 10 al. 1 de l'Ordonnance sur la garantie de la qualité.

Les Programmes peuvent mandater un expert externe pour analyser les données personnelles issues de MC-SIS. **Dans ce cas, la collaboration avec cet expert doit être réglée par un contrat écrit, incluant une clause de protection des données.**

Ces rapports peuvent être soumis à d'autres autorités, cantonales ou fédérales. Le Programme vérifie quelles sont ses obligations de transmission et ses modalités (notamment : qui transmet quoi comment et quand) et consigne l'information dans sa Directive_PD.

2.5.9. Communication à des chercheurs tiers

Chaque programme qui entend collaborer, même partiellement, avec des tiers à des projets de recherche est tenu de respecter la législation en matière de recherche (le plus souvent la Loi fédérale sur la recherche sur l'être humain (LRH) et ses ordonnances). La récolte systématique de données supplémentaires à des fins de recherche doit faire l'objet d'une SOP-1 (chapitre 2.3.3).

2.6. Effacement des données

Avec l'écoulement du temps, la conservation des données peut se révéler disproportionnée, et donc cesser d'être justifiée et licite[53]. La loi exige alors l'effacement de ces données ; en d'autres termes, celles-ci doivent être rendues totalement et définitivement inaccessibles[54]. Selon les cas, un effacement partiel peut se justifier (par ex. effacement des données plus anciennes et maintien des données plus récentes).

Aujourd'hui, aucune loi ne règle la durée (minimale ou maximale) de conservation des données issues du dépistage. Des lois cantonales fixent parfois la durée de conservation des données de santé en général. En l'absence de délai spécifique, le délai de prescription des actions (contractuelles ou délictuelles) en responsabilité est souvent pris comme point de référence. En d'autres termes, tant qu'un Programme ou un institut peut être attaqué en responsabilité par l'individu concerné, il doit conserver les données nécessaires à sa défense. Aujourd'hui, le délai de prescription absolu est en principe de 10 ans à compter du fait dommageable (ici l'acte médical ayant causé le dommage). Le 1er janvier 2020, le délai absolu passera à 20 ans, toujours à compter du fait dommageable[55]. Dès lors, le dossier *complet* ne devrait pas être détruit avant l'écoulement d'un délai de 20 ans à compter du dernier acte. C'est ainsi que, par exemple, l'analyse d'images anciennes peut aider à expliquer pourquoi certains examens ont été faits ou n'ont pas été faits d'une certaine manière.

La préservation des données jusqu'à l'échéance du délai de prescription est autorisée et obligatoire, quand bien même l'individu concerné demande l'effacement anticipé (voir aussi chapitre 2.5.5).

[53] Pour rappel, tout traitement des données doit être licite et proportionné (art. 4 al 1 et 2 LPD). La conservation des données personnelles constitue un traitement de données. Dès lors, le maître du fichier doit se demander à partir de quel moment la conservation de données cesse d'être nécessaire pour atteindre le but poursuivi et devient donc disproportionnée. A partir de ce moment, le traitement doit cesser ou être limité dans son ampleur.
[54] Destruction de données : http://www.thinkdata.ch/fr/glossaire.
[55] Selon l'art. 60 al.1bis, "En cas de mort d'homme ou de lésions corporelles, elle se prescrit par trois ans à compter du jour où la partie lésée a eu connaissance du dommage ainsi que de la personne tenue à réparation et, dans tous les cas, par vingt ans à compter du jour où le fait dommageable s'est produit ou a cessé.". Selon l'art. 128a, "En cas de mort d'homme ou de lésions corporelles résultant d'une faute contractuelle, l'action en dommages-intérêts ou en paiement d'une somme d'argent à titre de réparation morale se prescrit par trois ans à compter du jour où la partie lésée a eu connaissance du dommage et, dans tous les cas, par vingt ans à compter du jour où le fait dommageable s'est produit ou a cessé.".

Concrètement, la Directive_PD du Programme doit décrire comment l'effacement des données est effectué, notamment qui décide et comment, qui effectue l'effacement et qui vérifie le caractère complet de l'effacement. En principe, la responsabilité de l'effacement incombe au directeur médical de chaque Programme. MC-SIS envoie une alerte au Programme lorsque des données personnelles sont stockées depuis plus de 20 ans.

3. Conclusions

Pour que le dépistage atteigne ses objectifs, la confiance de la population est indispensable. Pour maintenir cette confiance, les données que confient les personnes doivent être traitées dans la plus grande confidentialité. Toujours à cette fin, il importe également que les droits des personnes en matière de protection des données, notamment le droit de consentir et le droit d'accès, soient respectés.

Pour assurer cet objectif, chaque Programme doit définir ses procédures internes et en assurer le respect. Il doit fournir une information complète et fiable aux participants au dépistage, de nature à permettre un consentement libre et éclairé. Il sensibilise régulièrement son personnel et ses partenaires externes et veille à un usage aussi restreint que possible des données non-anonymisées. Il s'assure que les données sont correctes et à jour. Enfin, il conclut les contrats garantissant la confidentialité des données personnelles.

En résumé, les directeurs de Programmes sont responsables de la protection des données. Chaque Programme doit se doter d'une Directive_PD qui tient compte de la législation fédérale et cantonale spécifique et des activités concrètes menées par le Programme. Autant que possible, le Programme doit impliquer dans la rédaction de cette Directive le Préposé cantonal à la protection des données. Au besoin, il annonce le fichier au Préposé cantonal ou fédéral.

La protection des données est une tâche exigeante qui implique une vigilance constante, car nul n'est jamais totalement à l'abri d'une brèche de confidentialité. Des procédures internes solides bien connues de l'ensemble des collaborateurs constituent dès lors un outil-clé pour assurer le niveau de protection le plus élevé.

swiss cancer screening

ANNEXES

Liste :

Annexe I **Définitions**

Annexe II **Bases légales**

Annexe III **Principes fondamentaux de la protection des données et droits des personnes**

Annexe IV **Modèles destinés aux participants**

Annexe V **Concept de monitoring national**

Annexe VI **Eléments constituant la Directive PD (et ses annexes)**

Annexe VII **Récapitulatif des SOP à établir par les Programmes**

Annexe VIII **Abréviations courantes**

Annexe I : Définitions

En Suisse, les lois opèrent des distinctions fondamentales entre les données personnelles et les données anonymes. Seul le traitement de données personnelles est soumis à la loi, tandis que le traitement de données anonymes ne l'est en principe pas. En pratique, d'autres termes sont parfois utilisés; les données sensibles sont une sous-catégorie des données personnelles qui demandent une protection particulière.

Données personnelles : les données personnelles sont toutes les informations relatives à une personne identifiée ou identifiable (art. 3 a LPD). Par informations, on comprend tout type de renseignements, quel que soit le moyen de transmission et le support. Les données traitées dans le cadre de la santé sont, en principe, des données à caractère personnel, puisqu'elles concernent des personnes physiques identifiées ou identifiables[56]. Les données identifiantes permettent d'identifier sans équivoque un individu. En principe, un individu peut être identifié de manière univoque par une combinaison de plusieurs des données suivantes : prénom, nom, date de naissance, photo, signature, taille, sexe et origine. Dans le domaine médical, les numéros d'identification caractéristiques comme le numéro de dossier ou le numéro AVS entrent aussi dans la catégorie des données identifiantes.

Données anonymes : les données anonymisées ne sont plus du tout corrélables avec les personnes concernées, ou alors au prix d'efforts démesurés. Elles ne sont plus considérées comme données personnelles. Si les données sont anonymisées, alors les lois sur la protection des données ne s'appliquent plus. Pour anonymiser les données personnelles liées à la santé, toutes les informations qui, en elles-mêmes ou combinées les unes aux autres, permettent de rétablir l'identité de la personne sans efforts disproportionnés doivent être rendues définitivement méconnaissables ou être détruites. Cela inclut le nom, les numéros d'identification caractéristiques (numéro AVS, numéro de cas), la date de naissance (le maximum autorisé étant mois et année), la date exacte du décès (le maximum autorisé est également le mois et l'année) et l'adresse exacte (le maximum autorisé est le numéro de commune OFS). Il faut toutefois garder à l'esprit que les informations médicales ne sont jamais entièrement anonymes, car chaque cas est unique et même avec des données « anonymisées », il est souvent possible de remonter au patient.

Données sensibles : les données personnelles sur la santé (selon une interprétation large) sont considérées comme des données sensibles (art. 3 c LPD).

Traitement de données personnelles : toute opération relative à des données personnelles – quels que soient les moyens utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données (art. 3 e LPD).

Communication de données personnelles : est considérée comme communication le fait de rendre des données accessibles (art. 3 f LPD), notamment d'autoriser leur consultation, de les transmettre, de les publier.

En particulier, dans le contexte de la recherche, le terme de données pseudonymisées est couramment utilisé, car la recherche sur de telles données est soumise à des règles moins strictes que sur des données identifiantes.

[56] European Data Protection Supervisor, Avis 1/2015, La santé mobile : concilier innovation techologique et protection des données, p.6

Données pseudonymisées ou codées : la pseudonymisation (ou déidentification) est le procédé de séparation des données identifiantes du reste des données personnelles. La corrélation des deux ensembles de données ainsi créés a lieu au moyen d'un pseudonyme ou d'un code (un identificateur non parlant), devant être présent aussi bien dans les données identifiantes (souvent sous forme d'une table de correspondance) que dans les données restantes (dites pseudonymisées). La réunion des deux ensembles de données (dépseudonymisation / réidentification) est ainsi rendue possible aux seules personnes autorisées, c'est-à-dire uniquement celles qui ont accès à la table de correspondance. Les données pseudonymisées demeurent des données à caractère personnel dans la mesure où elles peuvent être réidentifiées non seulement par le responsable du traitement, mais aussi par des tiers qui les combinent avec des informations externes émanant d'autres sources

Annexe II : Bases légales

Ce chapitre énonce les bases légales, au niveau international, fédéral et cantonal. Il est également fait référence aux règles non-contraignantes (dites « soft law ») applicables en matière de dépistage.

A. Conventions internationales ratifiées par la Suisse

Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n°108) signée à Strasbourg le 28.01.1981 : elle est entrée en vigueur pour la Suisse le 1er février 1998. Les parties signataires s'engagent à appliquer les règles fixées par la convention aux fichiers et aux traitements automatisés de données à caractère personnel tant dans les secteurs publics que privés. Ses normes ne sont toutefois pas directement applicables (*self-executing*) et les individus ne peuvent donc pas en tirer directement des droits. **La mise à jour de cette Convention** et la modernisation des principes énoncés figurent dans la directive européenne de 1995 sur la protection des données, sous la forme du règlement général sur la protection des données (RGPD). En tant que réglementation européenne, le RGPD est obligatoirement applicable à l'ensemble de l'Union européenne. Il ne s'applique pas aux programmes de dépistage du cancer en Suisse.

B. Bases légales fédérales

Cette section énumère et décrit brièvement l'ensemble des lois fédérales qui traitent, d'une manière ou d'une autre, des données médicales. Il est toutefois précisé que la LPD demeure le principal texte applicable, notamment car il sert généralement de modèle aux cantons élaborant leur législation en matière de protection des données par des autorités cantonales.

Constitution fédérale (art. 13), RS 101 : la Constitution fédérale accorde à toute personne le droit fondamental « d'être protégée contre l'emploi abusif des données qui la concernent » (art. 13 al. 2 Cst). Elle garantit ainsi le droit à l'autodétermination en matière d'information, ce qui signifie que tout individu a fondamentalement le droit de déterminer lui-même quand et à qui il entend révéler des faits personnels le concernant[57]. Les Constitutions cantonales contiennent des dispositions similaires (art. 21 constitution genevoise, art. 12 constitution fribourgeoise, art. 15 constitution vaudoise, art. 18 constitution bernoise… etc).

Loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1 et Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD), RS 235.11 : la loi fédérale sur la protection des données s'applique à l'ensemble des traitements de données personnelles effectués par l'administration fédérale ou par les personnes privées. Elle ne concerne donc a priori pas les programmes cantonaux, qui sont soumis aux lois cantonales sur la protection des données. Les données concernant la santé – notes sur le déroulement d'un traitement, descriptions de symptômes, diagnostics, résultats d'analyses ou radiographies – sont des données sensibles dont le traitement nécessite une protection spéciale. Ce document se base principalement sur la LPD.

Loi sur l'enregistrement des maladies oncologiques (LEMO), **RS 818.33**, et son ordonnance (OEMO), RS 818.331: les données figurant dans les registres cantonaux des tumeurs seront transmises à un organe national d'enregistrement du cancer financé par la Confédération, qui sera chargé de les regrouper, de les évaluer et de les publier. A l'avenir, un ensemble minimal de données, comprenant notamment le diagnostic précis, la date à laquelle

[57] Kiener/Kälin, Grundrechte, Berne 2007, p.158.

il a été posé et celle à laquelle le traitement a débuté, sera collecté pour chaque cas. Le patient dispose des droits suivants quant à la protection des données : droit à l'information (art. 5), droit d'opposition (art. 6), droit d'obtenir un soutien et d'accéder aux données (art. 7).

Loi sur la radioprotection (LRaP), RS 814.50 : cette loi prévoit que le médecin chargé d'effectuer un examen communique à l'autorité de surveillance les données nécessaires à la surveillance médicale et à l'établissement de statistiques (art. 14 LRaP).

Loi sur dossier électronique du patient (LDEP), RS 816.1 et autres lois à venir dans le domaine eHealth : cette loi rappelle le principe du consentement libre et éclairé du patient quant au traitement de ses données (art. 3) ainsi que le droit d'accès du patient aux données le concernant (art. 4). Des normes cantonales et fédérales dans le domaine de l'eHealth vont encore voir le jour, avec des effets probables dans le domaine de la protection des données. Il faut suivre les développements dans ce domaine avec attention. Le délai de mise en œuvre échoit en avril 2020 pour les hôpitaux. Les médecins en cabinet privé ne sont pas obligés d'offrir à leurs patient un dossier électronique.

Loi fédérale relative à la recherche sur l'être humain (LRH), RS 810.30 et art. 321 Code pénal suisse RS 311.0 : cette loi contient des dispositions sur la transparence et la protection des données. La question est de savoir si la loi sur la recherche a des effets dans le domaine du dépistage[58] ? La recherche est définie à l'art. 3 comme étant la recherche méthodologique visant à obtenir des connaissances généralisables, pratiquée notamment sur les données personnelles liées à la santé. Dans ce sens, le dépistage peut être considéré comme de la recherche[59]. De même, les données qui ont été obtenues dans le cadre du programme et qui sont utilisées pour obtenir de nouvelles connaissances constitueraient également de la recherche et les dispositions de la loi sur la recherche seraient alors applicables[60].

Loi fédérale sur l'assurance maladie (LAMal), RS 832.10 : les assureurs doivent prendre les mesures techniques et organisationnelles nécessaires pour garantir la protection des données (art. 84b) et avoir des règlements de traitement des données conformes à la LPD.

Code pénal art 321. Les données de patients ne peuvent être communiquées à des tiers que si le patient libère le médecin de son devoir de discrétion ou que la loi le permet. L'obligation de garder le secret en vertu du code pénal (art. 321 CP) ne vaut que pour les professions mentionnées dans celui-ci, c'est-à-dire les médecins et leurs auxiliaires. Les infirmiers et assistants médicaux peuvent être considérés comme des auxiliaires. Une violation de l'obligation de garder le secret peut entraîner une poursuite pénale, sur plainte du lésé.

Ordonnance sur la garantie de la qualité des programmes de dépistage du cancer du sein réalisé par mammographie, RS 832.102.4 : cette ordonnance fixe les conditions minimales que doivent remplir les Programmes mais ne contient pas d'article spécifique en matière de protection des données.

C. Bases légales cantonales

Lois cantonales sur la protection des données : presque chaque canton dispose d'une loi cantonale sur la protection des données. Les lois cantonales sur la protection des données réglementent le traitement des données par des autorités cantonales, dont font partie entre autres les programmes de dépistage. Ces bases légales s'appliquent à l'ensemble des autorités cantonales, et ne sont donc pas spécialement conçues pour le traitement de données

[58] Bericht Datenschutz, Brustkrebs-Früherkennungsprogramme in der Schweiz, p.5
[59] Bericht Datenschutz, Brustkrebs-Früherkennungsprogramme in der Schweiz, p.5
[60] Bericht Datenschutz, Brustkrebs-Früherkennungsprogramme in der Schweiz, p.5

médicales. Elles énoncent des grands principes de protection des données ainsi que des droits aux individus dont les données sont traitées par les autorités. Il est du devoir des Programmes, en collaboration avec le Préposé cantonal à la protection des données, d'assurer la protection des données et le respect de la réglementation au niveau cantonal.
Les différentes lois cantonales :
http://www.privatim.ch/de/internaldatenschutzgesetzgebung-kantone/

Lois et ordonnances cantonales sur la santé : les lois cantonales sur la santé et leurs ordonnances peuvent contenir des dispositions sur le dépistage du cancer et sur la protection des données, notamment sur le dossier médical du patient. Il existe parfois une ordonnance spécifique concernant le programme cantonal de dépistage (par exemple à Fribourg).

D. Soft law

Il s'agit des directives, des bonnes pratiques ou des normes de qualité qui sont applicables en Suisse sans toutefois avoir force légale.

Normes de qualité pour le dépistage organisé du cancer du sein en Suisse (2014) : ces normes de la Ligue suisse contre le cancer contiennent des dispositions sur la conservation et l'archivage des mammographies (p.6 §d), l'accès aux données démographiques pour les Programmes (p.7 §o et §s), l'applicabilité de la loi sur la protection des données (p.7 §r), l'échange de données (p.8 §t), le contrôle de la qualité des données (p.10 §k et p.11 §c).

European guidelines for quality assurance in breast cancer dépistage and diagnosis Fourth Edition : le document rappelle que selon la directive 95/46/EC pour le contrôle de la collecte de données, la protection des données personnelles est un droit fondamental de tout citoyen de l'UE[61]. Les lignes directrices européennes précisent que la lettre d'invitation au Programme doit contenir des informations sur la protection des données et la confidentialité[62]. Le document insiste sur l'attention qui doit être portée aux règles de protection des données lors de l'implémentation d'un Programme (p.398), lors de la collecte, l'enregistrement, la gestion et l'évaluation des données (p.399) et dans le cadre du monitorage (p.399).

European guidelines for quality assurance in colorectal cancer dépistage and diagnosis First Edition : le document demande une protection adéquate de toute donnée personnelle traitée dans le cadre du Programme, ainsi que le respect des directives européennes concernant la protection des données et des législations nationales (p.56). L'accès aux registres de population requiert une base légale (p.42).

[61] European guidelines for quality assurance in breast cancer screening and diagnosis Fourth edition, p.18
[62] European guidelines for quality assurance in breast cancer screening and diagnosis Fourth edition, p.388

Annexe III : Principes fondamentaux et droits des personnes

En Suisse, la protection contre le traitement abusif des données personnelles est ancrée dans la Constitution fédérale et est ensuite précisée dans une multitude de textes légaux et de recommandations.

Elle a pris une grande importance dans le domaine de la santé car « *plus les services électroniques de santé sont développés, plus les données doivent être sécurisées et disponibles rapidement. (…) Le traitement de données médicales implique une intervention dans les droits fondamentaux et les droits de la personnalité des personnes concernées (p. ex. les patients). Pour que l'intervention soit légitime, des mesures légales, organisationnelles et techniques doivent être prises. La qualité de ces mesures a une forte influence sur la confiance que l'on accorde aux services électroniques de santé.* »
La présente section est divisée en deux parties. La première récapitule les principes qui sont énoncés ou découlent de la législation suisse. La seconde résume les principaux droits des personnes concernées.

Principes fondamentaux

Principe de licité de la collecte (art. 4 al. 1 LPD) : tout traitement de données doit être licite. Lorsque le traitement est effectué par une autorité publique, il est licite s'il est permis par une loi (base légale) ou s'il est autorisé par le consentement explicite de la personne concernée. Dans de plus rares cas, une troisième justification envisageable peut tenir à un intérêt public ou privé prépondérant.

Principe de proportionnalité (art. 4 al. 2 LPD) : même si le traitement repose sur une base légale ou sur le consentement de la personne[63], il doit être effectué conformément aux principes de la proportionnalité et de la bonne foi. Seules peuvent être collectées les données personnelles utiles et nécessaires à atteindre un but déterminé. Le principe de proportionnalité entre notamment en compte dans le choix et l'ampleur des variables collectées.

Principe de finalité (art. 4 al. 3 LPD) : les données personnelles ne doivent être traitées que dans le but spécifiquement indiqué aux personnes qui les fournissent au stade de leur collecte. En d'autres termes, les personnes concernées doivent savoir dans quel but des questions leur sont posées et à quoi vont servir les réponses alors fournies. Dans des cas plus rares, il est également possible de traiter des données dans le but requis ou permis par une loi[64].

Principe d'exactitude (art. 5 al. 1 LPD) : celui qui traite des données personnelles doit s'assurer qu'elles sont correctes. Il prend toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées.

Droits des personnes

Droit d'accès « La LPD accorde à toute personne le droit de savoir si des données, et le cas échéant, quelles données la concernant sont traitées. Ainsi, la personne est mise en position d'exercer un certain contrôle sur son droit au respect de sa vie privée et de son

[63] Art. 4 al. 1 LPD (disposition révisée, en vigueur depuis janvier 2008). Amédéo Wermelinger / Daniel Schweri, «Teilrevision des Eidegnössischen Datenschutrechts – Es nützt nicht viel, schadetes etwas?» in Jusletter 3, mars 2008, ch. 10

[64] FMH, Bases juridiques pour le quotidien du médecin, Un guide pratique, p. 104.

autodétermination informationnelle. Sa demande n'a pas besoin d'être motivée. Elle est adressée au maître du fichier. Elle peut l'être par voie postale, par voie électronique ou en personne, pour autant que le maître puisse vérifier correctement l'identité de la personne. En principe, le maître du fichier doit répondre dans les 30 jours et doit fournir gratuitement les données requises. Exceptionnellement, si le maître du fichier refuse, il doit motiver sa décision.

https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/generalites/le-droit-d_acces.html

Droit de révocation du consentement Chaque personne qui a été amenée à consentir au traitement de ses données peut révoquer son consentement audit traitement. Cette révocation peut être communiquée en tout temps. Elle peut intervenir par écrit ou par oral. Le maître du fichier doit s'assurer qu'elle émane bien de la personne dont les données sont traitées. Il doit vérifier que la personne exprime réellement sa volonté libre et éclairée. La révocation du consentement signifie que le maître du fichier ne peut plus, à partir de ce moment, invoquer le consentement comme motif justifiant la licéité du traitement. Les traitements effectués avant la révocation restent conformes au droit. Le maître du fichier qui entend continuer à traiter les données (y compris les stocker) après la révocation doit pouvoir invoquer un autre motif justificatif (p. ex. une base légale, un intérêt privé prépondérant).

Droit de rectifier les données incorrectes Chaque personne dont les données personnelles sont traitées peut demander à ce que « ses » données incorrectes soient corrigées. Ce droit couvre aussi les données considérées incomplètes. La personne concernée adresse sa demande au maître du fichier. Si les données sont inexactes, le maître du fichier est tenu de les corriger pour qu'elles soient dorénavant correctes. Si les données sont incomplètes et donc susceptibles d'induire en erreur, le maître du fichier est tenu de les compléter. La correction ou le complément doit intervenir sans frais pour la personne concernée en principe dans les 30 jours. De nouveau, l'identité de la personne demandant la rectification doit être correctement vérifiée.

Annexe IV : Modèles destinés aux participants

Brochures d'information et flyers :

Cancer du sein: https://www.swisscancerscreening.ch/krebs-frueherkennung/brust/broschueren-und-flyer

Cancer du côlon: https://www.swisscancerscreening.ch/?id=278

Annexe V : Monitorage national

Indicateurs de participation : Couverture par invitation [%], Taux de participation à un an [%], Taux de participation en première invitation à 12 mois [%], Taux de fidélisation [%].

Indicateurs de performances : Taux de détection du cancer [1/1000], Taux des rappels [1/1000], Taux de faux positifs [1/1000], Valeur prédictive positive [%].

Indicateur de pronostic : Taux de cancer invasif [%], Taux de DCIS [%], Stades précoces [%], Cancers Stades avancés [%]

Annexe VI : Table des matières pour les Directives de protection des données propres à chaque programme

1. Résumé
2. Bases légales cantonales autorisant le traitement de données personnelles
3. Workflow du Programme
4. Identification des étapes avec un risque de brèche de sécurité/risque accru pour la protection des données (particulièrement si les données sont envoyées par d'autres biais que MC-SIS)
5. SOP-1-4, ainsi que la politique de mise à jour
6. Politique d'accès aux locaux, politique de gestion des documents écrits (notamment les formulaires papier remplis par les participants), politique de gestion des imprimantes et accès des visiteurs aux locaux.
7. Politique de sensibilisation des collaborateurs
8. Politique d'échange des données, entre autres avec le registre des tumeurs ou par le biais d'autres canaux que MC-SIS (p. ex. clé USB, etc)
9. Durée de conservation des données et procédure d'effacement
10. Annonce du fichier au Préposé à la protection des données

Annexes

11. Contrats avec des tiers (instituts, prestataires externes)
12. Modèle de lettre d'invitation
13. Modèle du formulaire de consentement
14. Brochure d'information

swiss cancer screening

Annexe VII : Set minimal de Standard Operating Procedures (SOP) et annexes en lien avec la protection des données.

SOP-1 : Procédure en cas d'acquisition systématique de données supplémentaires

SOP-2 : Procédure de vérification des données collectées

SOP-3 : Description des procédés d'actualisation et de contrôle de la matrice des droits d'accès

Matrice des droits Matrice des droits d'accès au système MC-SIS et aux locaux comprenant une liste nominative du personnel et de ses tâches

SOP-4 : Procédure réglant le traitement des demandes d'accès des personnes concernées.

Annexe VIII : Abréviations courantes

CDI	Conseils et développements informatiques SA
Cst	Constitution fédérale de la Confédération suisse
Directive_PD	Document où le Programme consigne sa politique liée à la protection des données
Test FIT	Fecal immunochemical test
FMH	Fédération des médecins suisses
Institut	Institut de radiologie ou de gastroentérologie qui collabore avec les Programmes
LAMal	Loi fédérale sur l'assurance maladie (RS 832.10)
LEMO	Loi fédérale sur l'enregistrement des maladies oncologiques (RS 818.33)
LPD	Loi fédérale sur la protection des données (RS 235.1)
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales (RS 830.1)
LRH	Loi fédérale relative à la recherche sur l'être humain (RS 810.30)
MC-SIS	Multi-Cancer Dépistage Information-System
OEMO	Ordonnance sur l'enregistrement des maladies oncologiques (RS 818.331)
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OPAS	Ordonnance sur les prestations de l'assurance des soins (RS 832.112.31)
PFPDT	Préposé fédéral à la protection des données et à la transparence
RGDP	Règlement général sur la protection des données. En tant que réglementation européenne, le RGPD est obligatoirement applicable à l'ensemble de l'Union européenne. Il ne s'applique pas aux Programmes de dépistage du cancer en Suisse.
SCS	Swiss Cancer Screening
SOP	Standard operating procedures