swiss cancer screening

Datenschutz

Ein Leitfaden für die Praxis

Swiss Cancer Screening (SCS)

swiss cancer screening

1 Zweck dieses Dokuments

Kantonale Früherkennungsprogramme (nachfolgend: Programme) organisieren das Angebot für Brust- und Darmkrebsfrüherkennung in denjenigen Kantonen, die sich für eine systematisches Angebot entscheiden[1]. Zwölf Kantone bieten ein Brustkrebs-Screening an, während vier Kantone (bald acht) ein Darmkrebs-Screening anbieten[2]. Der Bund legt die Bedingungen für die Erstattung der entsprechenden Leistungen durch die Grundversicherung sowohl für Brust- wie auch Darmkrebs-Screeningprogramme fest[3]. Die Bundesgesetzgebung regelt aber nicht die praktischen Modalitäten der Früherkennung.

Die Früherkennung beinhaltet die Erhebung und Weiterverarbeitung einer Vielzahl von Personendaten einer grossen Gruppe von Personen. Das Bundesgesetz über den Datenschutz (DSG[4]) regelt diese Aktivitäten, um die Rechte der Betroffenen, insbesondere ihre Rechte im Bereich Datenschutz, zu gewährleisten. Falls in einem Kanton die Kantonsbehörden die Früherkennung selbst übernehmen, gelten anstelle des DSG die kantonalen Datenschutzbestimmungen[5].

Ziel dieses Leitfadens ist es, die Grundsätze zusammenzufassen und die Datenschutzverpflichtungen, die die Programme erfüllen müssen, zu präzisieren. Er soll den Programmen resp. Mitgliedern von Swiss Cancer Screening (SCS), als Orientierungshilfe dienen. Er richtet sich in erster Linie an den medizinischen und administrativen Leiter der einzelnen Programme, stellt jedoch auch für die anderen Mitarbeiter ein wertvolles Arbeitsmittel dar. Der Leitfaden legt insbesondere die Nutzungsmodalitäten des gemeinsamen IT-Tools Multi-Cancer Screening Information System (MC-SIS) fest. Dieses Tool wurde zur Vereinfachung und Verwaltung der administrativen Abläufe, zur Speicherung der erfassten Daten (einschliesslich Bilddateien) und zur Analyse und Aggregierung von Daten für das Monitoring entwickelt.

Die *Struktur* dieses Leitfadens orientiert sich weitestgehend an den vom Teilnehmer durchlaufenen Stationen. Er beginnt mit der Erfassung von Namen und Adressen der Personen, an die sich die Früherkennung richtet, und endet mit der Vernichtung der Daten, sobald diese nicht mehr von Nutzen sind.

Die *Anhänge* zum Leitfaden enthalten eine Übersicht über die Definitionen (Anhang I) und über die gesetzlichen Grundlagen (Anhang II); Anhang III beleuchtet die Grundsätze des Datenschutzes. Anhang IV bietet Vorlagen, zu deren Verwendung die Programme aufgefordert werden. Anhang V führt Kennzahlen des landesweiten Monitorings an. Anhang VI vergegenwärtigt

[1] Die Früherkennung wird von den Krankenkassen im Rahmen der Grundversicherung erstattet, sofern sie den Anforderungen von Art. 12e Abs. 1 Buchst. c KLV (Verordnung des EDI über Leistungen in der obligatorischen Krankenpflegeversicherung) entspricht. Unter Verweis auf diesen Artikel, muss das Mammografie-Screening den Anforderungen der Verordnung über die Qualitätssicherung bei Programmen zur Früherkennung von Brustkrebs durch Mammographie vom 23. Juni 1999 (SR 732.102.4) entsprechen.

[2] Für Darmkrebs gibt es derzeit ein organisiertes Screening-Programm in den Kantonen Uri und Waadt, für das Jahr 2019 ist die Einführung in den Kantonen Basel-Stadt, Genf, Jura-Neuenburg und Graubünden geplant.

[3] Art. 26 Krankenversicherungsgesetz (KVG, SR 832.10). Artikel 12e der Krankenpflege-Leistungsverordnung (KLV, SR 832.112.31) besagt, dass die Früherkennungs-Mammographie und die Darmkrebs-Früherkennung von der obligatorischen Krankenpflegeversicherung für Personen über 50 Jahre nur im Rahmen eines organisierten Screening-Programms abgedeckt sind. Für die Mammographie sind die Bedingungen in der Verordnung vom 23. Juni 1999 über die Qualitätssicherung bei Programmen zur Früherkennung von Brustkrebs durch Mammographie (SR 832.102.4, nachstehend Qualitätssicherungsverordnung genannt) festgelegt.

[4] Bundesgesetz über den Datenschutz (SR 235.1; DSG) vom 19. Juni 1992; dieses Gesetz wird derzeit vom Parlament überarbeitet. Das DSG gilt für alle Personendaten, nicht speziell für medizinische Personendaten. Es sei darauf hingewiesen, dass die europäische Datenschutz-Grundverordnung (DSGVO) hier keine Anwendung findet, da die Verarbeitung der betreffenden Daten nicht in den Anwendungsbereich der Verordnung fällt.

[5] Das DSG gilt nicht für die Tätigkeit der kantonalen Behörden, sondern nur für die Tätigkeit der Bundesbehörden und von Privatpersonen.

den Inhalt der Datenschutzrichtlinie. Anhang VII listet die Standard Operating Procedures (SOP) auf, die jedes Programm zu erfüllen hat. Anhang VIII listet schliesslich häufig verwendete Abkürzungen auf.

Der vorliegende Leitfaden ist als dynamisches Dokument konzipiert, das bei Änderungen der Vorschriften und gemäss den Kommentaren durch die Programme laufend vervollständigt aber mindestens alle 2 Jahre aktualisiert wird.

2 Verpflichtungen von SCS und Programmen im Bereich Früherkennung

Zur Früherkennung müssen *Personendaten* erhoben und verarbeitet werden, d. h. Daten, die eine Person (z. B. über ihren Namen) direkt identifizieren, oder die ihre Identifizierung durch Kombination oder Abgleich von Daten ermöglichen[6]. Bei personenbezogenen Daten verpflichtet das Gesetz – sei es die Verfassung, das Bundesgesetz über den Datenschutz oder die kantonalen Gesetze – den Datennutzer dazu, Massnahmen zur Wahrung der Vertraulichkeit und zur Gewährleistung der Rechte der betroffenen Person zu ergreifen. Medizinische Daten werden darüber hinaus als *besonders schützenswerte* Personendaten betrachtet und bedürfen daher eines erhöhten Schutzes[7].

Die Einhaltung der datenschutzrechtlichen Verpflichtungen ist ein Schlüsselfaktor, um das *Vertrauen* der Öffentlichkeit in die Früherkennung zu gewährleisten. Ohne das Vertrauen der Öffentlichkeit wiederum wäre der Erfolg der Früherkennung gefährdet. Daher ist es unerlässlich, dass alle beteiligten Parteien ein Höchstmass an Schutz und Sicherheit der Daten gewährleisten, die ihnen anvertraut werden.

Die aus Sicht des Datenschutzes kritischen Schritte sind:

- In einer ersten Phase wendet sich das Programm an die Kantonsbehörde (oder an die kantonalen/kommunalen Behörden), die das Einwohnerregister führt, um für das betreffende Gebiet einen Auszug daraus zu erhalten. Das Programm benötigt mindestens Namen und Vornamen, Adressen und Geburtsdaten der betroffenen Zielgruppe (d. h. für die Personen, die für die Teilnahme an der Untersuchung in Frage kommen) (s. Abschnitt 2.1).
- Die Zielbevölkerung wird mit einer Einladung über die Möglichkeit einer Teilnahme an der Früherkennung informiert. Abschnitt 2.2 führt die Verpflichtungen des Programms in dieser Phase näher aus.
- Personen, die teilnehmen möchten, werden ins Programm eingeschlossen. Die mit diesem Schritt verbundenen Verpflichtungen (informierte Zustimmung, Erfassen von Daten, etc.) werden in Abschnitt 2.3 beschrieben.
- Die Datenschutzrelevanten Aspekte im Zusammenhang mit der Auswertung der Resultate wird in Abschnitt 2.4 erörtert.
- Teilnehmende werden über das Untersuchungsergebnis informiert. Die mit diesem Schritt verbundenen Verpflichtungen werden in Abschnitt 2.5 beschrieben. Nach Mitteilung einer allfälligen Krebsdiagnose fallen die Interaktionen zwischen der betroffenen Person und dem medizinischen Team, das sie betreut, nicht mehr in die Zuständigkeit des Programms.

[6] So ist es bspw. in der Regel möglich, eine Person über die Kenntnis von Geburtsdatum und Adresse zu identifizieren.
[7] Art. 3 Buchst. c, Art. 4 Abs. 5 und Art. 11a Abs. 3, Art. 12 Abs. 2 Buchst. c, Art. 14, Art. 35 DSG.

- Das Programm speichert die in den vorherigen Schritten erfassten Daten. Die Personen müssen regelmässig wieder eingeladen werden können. Aus Gründen der Qualitätskontrolle analysiert das Programm zudem die Daten regelmässig. SCS erstellt auf der Grundlage aggregierter, anonymisierter Daten ebenfalls einen Bericht, in dem die Schlüsselindikatoren für einen gegebenen Zeitraum aufgeführt sind (siehe Abschnitt 2.6).
- Das Gesetz schliesst die unbefristete Speicherung von Personendaten aus. Die Programme müssen daher entscheiden, wann Daten für den Zweck der Früherkennung nicht mehr relevant sind und vernichtet werden. Abschnitt 2.7 präzisiert die Verpflichtungen in dieser Phase.

2.1 Beschaffung der Daten bei den Kantonsbehörden

Das Programm muss wissen, welche Personen zur Teilnahme an der Früherkennung eingeladen werden sollen. Die Einladung erfolgt gemäss den Teilnahmebedingungen, die im Allgemeinen in dem von der Kantonsbehörde erteilten Auftrag festgelegt[8] werden. Das Programm fordert von der Kantonsbehörde eine Liste aller Todesfälle, neuen Niederlassungen und Umzüge in der entsprechenden Zielgruppe und dem betreffenden Gebiet an, um zu vermeiden, dass wiederholte Einladungen an unberechtigte Personen gesendet werden. In einigen Kantonen werden diese Informationen nicht zentral gesammelt und das Programm muss sich an mehrere, regionale Stellen wenden.

Die Gesetzgebung erlaubt die Übermittlung von Personendaten (Namen, Adressen, Alter der Personen, Todesfälle) von einer öffentlichen Behörde an einen Dritten, in diesem Falle das Programm, nur unter strengen Bedingungen. Eine Bestimmung im kantonalen Recht[9] muss diese Übermittlung ausdrücklich erlauben, d. h., die Kantonsbehörde muss *auf einer rechtlichen Grundlage* zur Übermittlung der Personendaten (bzw. das Programm zu deren Erhalt) ermächtigt sein (Legalitätsprinzip[10]).

Diese Rechtsgrundlage kann in Form eines kantonalen Gesetzes des Parlaments oder einer Verordnung der Exekutive vorliegen. Eine Richtlinie der zuständigen Kantonsverwaltung allein reicht nicht aus, um die Übermittlung zu rechtfertigen. Sie kann aber die Modalitäten der Übermittlung festlegen.

Enthält das kantonale Recht keine Rechtsgrundlage, muss sich das Programm an die Kantonsbehörden wenden, um gemeinsam die Grundlagen für eine solche Übermittlung festzulegen. Im Zweifel darüber, ob eine ausreichende Rechtsgrundlage vorhanden ist, kann das Programm den kantonalen Datenschutzbeauftragten konsultieren, um eine geeignete Lösung zu finden.

Das Programm importiert alle von der kantonalen Behörde erhaltenen Informationen in MC-SIS ein. Wenn möglich, überprüft dieses deren Richtigkeit, z. B. indem es unwahrscheinliche

[8] Gemäss der Qualitätssicherungsverordnung muss das Screening von einer vom Kanton oder den Kantonen anerkannten Organisation angeboten werden (Art. 3 Abs. 1).
[9] Da es sich um eine Übermittlung durch die kantonale Behörde handelt, ist das DSG nicht anwendbar.
[10] Das Legalitätsprinzip verlangt, dass das Handeln des Staates auf einer Rechtsgrundlage beruht. Im Kontext des Datenschutzes muss jedwede Datenverarbeitung rechtmässig sein. Die Rechtmässigkeit eines Datenverarbeitungsvorgangs kann sich aus der freien und informierten Einwilligung der betroffenen Person oder aus einer Rechtsgrundlage ergeben, die eine solche Verarbeitung zulässt; in bestimmten Fällen kann auch ein übergeordnetes privates oder öffentliches Interesse die Verarbeitung von Daten rechtfertigen und damit zulässig machen.

Geburtsdaten verwirft (etwa eine im Jahre 1812 geborene Person). Das Programm sollte die Art der durchgeführten systematischen Überprüfungen schriftlich festlegen.

Der Import von Daten in MC-SIS stellt eine *Datenverarbeitung* (im Sinne des Gesetzes)[11] dar. Um zulässig zu sein, muss auch diese Verarbeitung auf einer Rechtsgrundlage gründen. Diese Rechtsgrundlage findet sich im kantonalen Gesetz zur Früherkennung (siehe Anhang II). Durch die Erteilung eines Mandats zur Durchführung eines Screenings, ermächtigt dieses Gesetz das entsprechende Programm, die zu diesem Zweck erforderlichen Daten zu verarbeiten.

Konkret muss das Programm die kantonale(n) Rechtsgrundlage(n), die die Verarbeitung von Personendaten erlaubt/erlauben, überprüfen und in seiner Datenschutzrichtlinie festhalten.

2.2. Einladungen an die betroffenen Personen

Sobald die Personen, die für die Teilnahme an der Früherkennung in Frage kommen, ordnungsgemäss identifiziert wurden (Zielgruppe), muss das Programm jeder von ihnen per Post eine Einladung zukommen lassen[12]. Diese Einladung enthält einen personalisierten Brief (d. h. unter Nennung des Namens der Person), eine Informationsbroschüre[13] und ggf. ein Formular[14], das eine Kombination aus Gesundheitsfragebogen und Einverständniserklärung darstellt, und schliesslich einen Antwortschein für Personen, die ihre Ablehnung der Teilnahme mitteilen möchten.

Das Programm kann einige dieser Tätigkeiten an einen Dritten übertragen. Ein anderer externer Dienstleister wie z.B. eine Druckerei kann mit dem Druck und Versand der Einladungen beauftragt werden. In diesem Rahmen kann der Dritte Kenntnis schützenswerter Daten der betroffenen Personen erhalten. Daher ist es von entscheidender Bedeutung, dass er sie vertraulich (d. h. keine Weitergabe an andere), korrekt (d. h. keine Fehler beim Versand, indem Einladungen fälschlich an andere Personen gesendet werden) und sicher (d. h. Schutz seiner Räumlichkeiten und Speichersysteme vor unbefugtem Zugriff, z. B. durch Hacker) behandelt.

Die Übermittlung von Daten, z. B. der Namens- und Adressdatei durch das Programm an Dritte, muss über einen sicheren Kanal erfolgen, z. B. über ein verschlüsseltes E-Mail-System, die persönliche Übergabe eines verschlüsselten USB-Sticks oder durch geschützte Downloads. Die Mitarbeiter des Programms müssen diesbezüglich sensibilisiert werden.

Da das Programm diesem Dritten eine ihm obliegende Aufgabe übertragen hat, ist es gesetzlich verpflichtet, den Dritten und seine Datenverarbeitung zu kontrollieren[15]. Mit anderen Worten, das Programm kann dem Dritten nicht einfach "vertrauen", sondern muss konkrete Massnahmen ergreifen, um sicherzustellen, dass der Datenschutz durchgehend eingehalten wird.

---

[11] Im Bundesrecht ist die Datenverarbeitung im weitesten Sinne definiert als „jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten" (Art. 3 Buchst. e DSG). Auch die kantonalen Gesetze definieren diesen Begriff im weitesten Sinne.

[12] Vgl. Art. 5 der Qualitätssicherungsverordnung.

[13] Siehe Anhang IV.

[14] Einige Programme verwenden einen elektronischen Fragebogen; die informierte Einwilligung in die Früherkennung eines kolorektalen Karzinoms wird in Anwesenheit eines Hausarztes, eines Apothekers oder über das Internet eingeholt.

[15] Im Bundesgesetz sieht Art. 10a DSG vor: „Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:

a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und
b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

[2] Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet."

Damit die Übermittlung der Personendaten des Programms an Dritte rechtmässig ist, **muss diese auf einem schriftlichen Kooperationsvertrag beruhen. In diesem Vertrag müssen die übertragenen Aufgaben und Pflichten des Dritten in Bezug auf Sicherheit und Datenschutz genau festgelegt werden.** Der Vertrag muss insbesondere im Hinblick auf den technischen Fortschritt auf dem neuesten Stand gehalten werden. **Er ist als Anhang zur programmeigenen Datenschutzrichtlinie beigefügt.** Darüber hinaus legt diese Richtlinie die Rollen und Verantwortlichkeiten im Zusammenhang mit dieser externen Zusammenarbeit fest (z. B. wer die Datei wann an den Dritten übermittelt, wer die Versendung wann und wie überprüft usw.).

2.3 An die betroffenen Personen gesendete Dokumente, Einwilligung und Früherkennungsuntersuchung

2.3.1 Einladung der Zielgruppe

Die an die betroffenen Personen (Zielgruppe) gerichtete Einladung sollte es diesen ermöglichen, eine Entscheidung über ihre Teilnahme zu treffen. Diese Entscheidung muss frei und informiert erfolgen[16]. Jede Person muss daher detaillierte schriftliche Informationen über die Modalitäten und die Vor- und Nachteile des Screenings erhalten. Jede Person muss sodann mündliche Antworten auf ihre (möglichen) Fragen erhalten können. Insbesondere kann sie das Empfangs- und Gesundheitspersonal befragen. Ihre Entscheidung muss frei und unabhängig erfolgen. Selbst nach der (im vorliegenden Fall schriftlichen[17]) Erteilung der Einwilligung, steht es der Person frei, ihre Meinung zu ändern und die Einwilligung daher zu widerrufen[18] (siehe dazu Abschnitt 2.5.5). Sie muss ihre Wahl nicht rechtfertigen oder begründen.

Im Hinblick auf die dem Programm obliegenden Aufgaben, muss dieses zunächst den Inhalt des Einladungsschreibens, der Informationsbroschüre und des Formulars festlegen, das per Post an die Zielgruppe geschickt wird. Die bereitgestellten Informationen müssen verständlich, vollständig und inhaltlich ausgewogen sein. Bei inhaltlichen oder formalen Zweifeln, kann sich das Programm an die kantonale (oder interkantonale) Ethikkommission zur Forschung am Menschen wenden, die zu diesem Thema beraten kann[19]. Das Programm kann auch den kantonalen Datenschutzbeauftragten konsultieren. Für die Informationsbroschüre hat SCS mehrsprachige **Vorlagen** entwickelt, die die Programme (ggf. nach vorheriger Anpassung) verwenden können.

Konkret muss das Programm diese drei Dokumente als Anhang zu seiner DS-Richtlinie aufnehmen.

[16] Nach dem DSG: „Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt." (Art. 4 Abs. 5, Satz [1], DSG).
[17] Da es sich bei den verarbeiteten Daten um schützenswerte Daten handelt, muss die Zustimmung der betroffenen Person schriftlich erteilt werden. Vgl. Art. 4 Abs. 5 in fine DSG.
[18] Im Abschnitt „Einwilligung" des Formulars steht: „Wir weisen Sie darauf hin, dass Ihre Einwilligung jederzeit widerrufen werden kann".
[19] Fällt das Screening nicht unter den Begriff der medizinischen Forschung im Sinne des HFG (Bundesgesetz über die Forschung am Menschen vom 30. September 2011; SR 810.30), sind die Ethikkommissionen für die Forschung weiterhin befugt, ausserhalb des Anwendungsbereichs des HFG zu beraten. Vgl. Art. 51 Abs. 2 HFG. Sie verfügen über umfangreiche Erfahrungen bei der Überprüfung der in der Forschung verwendeten Informations- und Einwilligungsformulare. Diese Erfahrung kann auch im Kontext des Screenings genutzt werden.

2.3.2 Einschluss/Termin für eine Untersuchung

Die Modalitäten zum Einschluss unterscheiden sich je nach Art des Screenings: Die Einladung zur Brustkrebsfrüherkennung ermöglicht es den Teilnehmerinnen, einen Termin an einem Institut für Radiologie wahrzunehmen; die Einladung zur Darmkrebsvorsorge bezieht sich auf eine Beratung bei einem Allgemeinmediziner, bei einem Apotheker oder über eine Internetplattform. Die den Teilnehmer einschliessende Person gibt die Personendaten in MC-SIS ein.

Wenn die Person zum Institut für Radiologie (Mammographie bei Brustkrebsfrüherkennung) oder zum Institut / zur Praxis für Gastroenterologie (Koloskopie bei Darmkrebsvorsorge) (nachfolgend: Institut) geht, bekommt sie die Gelegenheit Fragen zu stellen und die entsprechenden Antworten zu erhalten. Sofern sie ihre Meinung nicht ändert, reicht die Person die unterschriebene Einverständniserklärung in Papier- oder elektronischer Form (e-Quest) ein.

Die Mitarbeiter des Instituts überprüfen oder vervollständigen die Antworten zu ihrem persönlichen Status[20], der Krankenversicherung[21] sowie ihrem aktuellen und vergangenen Gesundheitszustand. Die in diesem Stadium direkt von der Person erhobenen Daten sind die medizinische und familiäre Vorgeschichte und mögliche Symptome[22]. Die Person muss den Namen und die Kontaktinformationen eines Arztes ihrer Wahl (Referenzarzt) angeben[23], an den das Programm das Screening-Ergebnis direkt senden kann. Die Person wird aufgefordert, ein Formular zu unterzeichnen, um ihre Einwilligung zu erteilen; diese Einwilligung berechtigt zum Austausch und Auswertung der Daten, die für die korrekte Durchführung des Screenings erforderlich sind[24].

Die Mitarbeitenden des Instituts erfassen klinische Auffälligkeiten und allfällige technische Schwierigkeiten während der Untersuchung in MC-SIS. Diese Daten gelten als relevant und dem Zweck angemessen, d. h. sie sind notwendig, um die Früherkennung im Interesse der individuellen und öffentlichen Gesundheit in bestmöglicher Weise zu gewährleisten[25].

Verweigert die Person ihre Einwilligung, und insbesondere die Zustimmung zur Verwendung der Daten und der Übermittlung an den Referenzarzt[24], kann sie nicht an der Früherkennung teilnehmen. Der Gesundheitsfragebogen sollte auf diesen Punkt hinweisen. Die Person kann ihre Entscheidung jederzeit überdenken (dazu Abschnitt 2.5.5). In diesem Zusammenhang kann sie angeben, ob ihre Ablehnung als endgültig zu verstehen ist. In diesem Fall erhält sie keine Einladungsschreiben mehr zur Teilnahme an der Früherkennung. Ihre Ablehnung wird im MC-SIS eingetragen, um die Einhaltung ihres Wunsches zu gewährleisten; diese persönlichen Daten werden daher dauerhaft gespeichert.

---

[20] Derzeit muss die Person im Normalfall Angaben zu ihrem Nachnamen, Vornamen, Ledignamen, Geburtsdatum, ihrer Adresse, Telefonnummer, Nationalität und AHV-Nummer machen.

[21] Derzeit muss die Person im Normalfall den Namen ihrer Grundversicherung und ihre Versicherungsnummer angeben.

[22] Wird die Person also gebeten, folgende Fragen zu beantworten: Hat sie sich jemals einer Mammographie unterzogen, unterzieht sie sich einer Hormonbehandlung in den Wechseljahren, gab es eine Familiengeschichte von Brustkrebs, leidet oder litt sie schon einmal an Problemen an der Brust?

[23] Falls die Person keinen Referenzarzt angeben möchte, kann in Ausnahmefälle der medizinische Leiter des Programms diese Funktion übernehmen.

[24] Damit akzeptiert die Person, dass ihre Personendaten vom Institut im Falle eines Umzugs an das Zentrum für Früherkennung, das Krebsregister, den Referenzarzt und das Screening-Programm des neuen Wohnkantons übermittelt werden können. Sie akzeptiert auch, dass ihre Daten gespeichert und archiviert werden können. Schliesslich akzeptiert sie, dass ihre Daten anonymisiert und dann für statistische und qualitative Zwecke und die Ausbildung der Ärzte ausgewertet werden können. Darüber hinaus werden die Daten an die Krankenkassen übermittelt.

[25] Nach schweizerischem Recht muss jede Datenverarbeitung die Verhältnismässigkeit achten (Grundsatz der Verhältnismässigkeit). Dieser Grundsatz besagt, dass zur Erfüllung des Zwecks die Verarbeitung auf das absolute Minimum beschränkt sein muss, sei es in Bezug auf den Umfang der gesammelten Daten, den Kreis der Personen, von denen sie erhoben werden, den Kreis der Personen, die zu ihrer Bearbeitung befugt sind, den Umfang der auf den Daten ausgeführten Operationen und ihre Speicherdauer.

Die Beziehung zwischen dem Programm und dem Institut sowie allen in einem Programm tätigen Dienstleistern (bspw. Radiologen, Pathologen, Allgemeinmediziner, Apotheker, Labor für FIT Analyse) muss in einem Vertrag schriftlich festgelegt werden. In diesem Vertrag sind die Pflichten und Rechte jeder Partei niederzulegen. In Bezug auf die Aspekte des Datenschutzes **muss im Vertrag festgelegt werden, wie der Dienstleister den Schutz der Daten und der Rechte der betroffenen Personen gewährleistet. Er muss insbesondere eine Vertraulichkeitsklausel enthalten, die garantiert, dass das Institut und seine Mitarbeiter Personendaten und andere Informationen, die bei der Früherkennung gewonnen werden, streng vertraulich behandeln. Diese Verträge müssen auf dem neuesten Stand gehalten und der programmeignen Datenschutzrichtlinie beigefügt werden.**

2.3.3 Eventuelle Erhebung zusätzlicher Daten

Die Datenschutzgesetzgebung schreibt vor, dass nur Daten erhoben und verarbeitet werden, die für den Verarbeitungszweck unbedingt erforderlich sind[26].Manchmal werden im Rahmen eines Programms systematisch *zusätzliche* Daten erhoben werden. Die Notwendigkeit dieser weiteren Datenerhebung muss durch das Programm ordnungsgemäss nachgewiesen werden und verhältnismässig sein. Der Zweck der Datenverarbeitung muss zudem für die zustimmende Person erkennbar sein und danach unverändert bleiben (sog. *Zweckbestimmung*)[27].

Zu beachten ist, dass es in diesem Zusammenhang nicht rechtmässig ist, zusätzliche Daten *für Forschungszwecke* zu erheben, da dies der ausdrücklichen Zustimmung des Teilnehmers bedarf (s. Abschnitt 2.5.9)[28]. Wenn das Ziel die Forschung ist, muss der Teilnehmer im Voraus darüber informiert werden, dass seine Antworten zu diesem Zweck analysiert werden und seine freie, informierte und schriftliche Zustimmung geben. Zudem muss eine Genehmigung der für die medizinische Forschung zuständigen Ethikkommission eingeholt werden[29]. Die Grenze zwischen Forschung und Qualitätskontrolle verläuft nicht immer eindeutig[30]. Wenn das Institut oder das Programm zum Zeitpunkt der Datenerhebung nicht begründen kann, dass die zusätzlichen Daten direkt für die Zwecke der Früherkennung relevant sind, sondern diese Relevanz getestet oder evaluiert werden soll, gilt dies als Forschung.

Beabsichtig das Programm zusätzliche Daten zu erheben, muss es **eine SOP erstellen**. Darin ist beschrieben wie die Daten erhoben werden und wie diese zusätzlichen Informationen dann verarbeitet werden, um das Ziel einer verbesserten Früherkennung zu erreichen (nachstehend **SOP-1**). Dieses Dokument erläutert auch, wie und von wem diese zusätzlichen Daten periodisch ausgewertet werden. **Dieses Dokument wird der DS-Richtlinie beigefügt. Das Programm leitet diese SOP-1 an SCS weiter. SCS koordiniert bei Bedarf die Hinzufügung eines Eingabefeldes im MC-SIS.**

[26] Nach Bundesrecht hat jede Datenverarbeitung „nach Treu und Glauben zu erfolgen und muss verhältnismässig sein." Art. 4 Abs. DSG.
[27] Nach Bundesrecht dürfen nach Artikel 4, Abs. 3 und 4 des DSG „Personendaten [...] nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.
Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein." Das heisst, die Person muss wissen, dass ihre Daten erhoben werden, und über den Zweck der Beschaffung informiert sein. Dieser ihr angegebener Zweck kann grundsätzlich nicht mehr geändert werden.
[28] Die Forschung im medizinischen Bereich unterliegt dem HFG. Dieses Gesetz verlangt jedoch, mit wenigen Ausnahmen, dass der Forschungsteilnehmer seine Einwilligung erteilt. Art. 7 HFG.
[29] Art. 45 HFG.
[30] Vgl. SwissEthics (Schweizerische Ethikkommissionen für die Forschung am Menschen), Arbeitsgruppe 19: Zuständigkeitsabklärung. Unter www.swissethics.ch/doc/ab2014/Zustaendigkeit_d.pdf

A. 2.4 Medizinische Ergebnisse

Dieser Abschnitt ist in sechs Unterabschnitte unterteilt. Zunächst einmal müssen die Daten, die während des Besuchs der betroffenen Person im Institut erhoben wurden, auf ihre Richtigkeit überprüft werden[31]. Die Mammographie-Daten werden von zwei oder sogar drei Radiologen gelesen[32]. Die Resultate der Darmkrebsfrüherkennung werden durch das Labor (FIT) oder den Gastroenterologen/Pathologen (Koloskopie) beurteilt. Abschliessend werden die Ergebnisse an den Teilnehmenden und den von ihm angegebenen Referenzarzt übermittelt. Falls der Teilnehmende keinen Referenzarzt angegeben hat, stellt der medizinische Leiter des Programms die ärztliche Beratung sicher. Der Referenzarzt oder andere behandelnde Ärzte verlangen manchmal gewisse zusätzliche Informationen. Die Weitergabe von Informationen an die kantonalen und eidgenössischen Behörden wird unten in Abschnitt 2.6 behandelt.

2.4.1 Kontrolle der Daten

Das Institut muss die Plausibilität der direkt erhobenen Daten überprüfen.

Zudem kontrolliert das Programm die vom Institut in MC-SIS eingetragene Daten, insbesondere im Hinblick auf ihre interne Kohärenz. MC-SIS ermöglicht den Export von Tabellen einzelner Daten, damit Programme ihre eigenen Validierungen durchführen können. Solche Validierungen sind dringend empfohlen.

Um die Qualität seiner Vorgehensweise zu gewährleisten, muss das Programm eine SOP verfassen, die seine Kontrollschritte beschreibt (einschliesslich der Frage, wer was und wie überprüft, wer was und wie korrigiert und wer was und wie überwacht) (SOP-2).

2.4.2 Datenaustausch zwischen internen Partnern

Der Datenaustausch von Personendaten zwischen internen Screening-Partnern – bspw. Programmmitarbeitern, Analyselabors, Radiologen bzw. bei der Koloskopie Gastroenterologen zum Pathologen – erfolgt grundsätzlich in MC-SIS. Die betroffenen Personen müssen ausdrücklich dazu berechtigt sein, auf die Daten zuzugreifen und sie auszutauschen. Diese Berechtigung muss **in die von jedem Programm definierte Zugriffsmatrix beschrieben und in einer SOP festgehalten werden (SOP-3)**. Art und Inhalt des Datenaustausches werden grundsätzlich von MC-SIS vorgegeben; diese Datenaustausche unterliegen den in der Software integrierten und im CDI-Sicherheitskonzept beschriebenen Sicherheitsmassnahmen.

Diese Datenaustausche sind rechtmässig, weil sie auf dem kantonalen Gesetz zur Früherkennung basieren, was jedoch jedes Programm überprüfen muss. Sie stehen auch in einem angemessenen Verhältnis zu dem verfolgten Ziel, nämlich der Zielgruppe ein qualitativ hochwertiges Screening anzubieten.

[31] Die Bundesgesetzgebung zum Datenschutz legt den Grundsatz der Richtigkeit fest. Im Wortlaut von Art. 5 Abs. 1 DSG: „Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu ergreifen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind." Die kantonale Gesetzgebung enthält im Allgemeinen eine ähnliche Regel.

[32] Vgl. Art. 4 der Qualitätssicherungsverordnung.

2.4.3 Datenanalyse und medizinische Diagnostik[33]

Die für die Erstellung der Diagnose verantwortlichen Fachkräfte haben Zugriff auf alle erhobenen Daten (demographische Daten, Anamnese, Bilder, Labortests) und erfassen die Diagnose in MC-SIS.

Konkret muss das Programm sicherstellen, dass es nicht nur schriftliche Verträge mit dem Institut (bereits oben Abschnitt 2.3.2) **abgeschlossen hat, sondern auch mit den externen Dienstleistern, die mit der Durchführung von Tests (z. B. Labors, Pathologen, Allgemeinmediziner, Apotheker) und der Datenanalyse (z.B. Radiologen, Gastroenterologen) beauftragt wurden.** Diese Verträge müssen die zu erfüllenden Aufgaben genau beschreiben. Sie müssen insbesondere eine Vertraulichkeitsklausel enthalten, die garantiert, dass die externen Partner und ihre Mitarbeiter Personendaten und andere Informationen, die bei der Früherkennung gewonnen werden, streng vertraulich behandeln. Diese Verträge (oder Pflichtenhefte) müssen auf dem neuesten Stand gehalten werden. **Sie sind als Anhang zur programmeigenen Datenschutzrichtlinie angefügt.**

Dieser Datenaustausch des Programms mit den für die Diagnose Verantwortlichen via MC-SIS ist rechtmässig, da er auf dem kantonalen Gesetz zur Früherkennung basiert. Die informierte Einwilligung der betroffenen Person deckt diesen Datenaustausch ebenfalls ab. Er ist notwendig und dem Zweck nach verhältnismässig.

Ein Austausch von Personendaten über andere Kanäle als MC-SIS sollte vermieden werden. So bietet beispielsweise der Versand per Telefon, E-Mail, USB-Stick oder CD-ROM nicht die gleichen Sicherheitsgarantien wie der Austausch über MC-SIS. In solchen Fällen muss das Programm das gleiche Schutzniveau gewährleisten, wie es MC-SIS (z.B. verschlüsselte Email) tut. In der DS-Richtlinie muss erläutert werden, wie dieses Schutzniveau sichergestellt wird.

2.4.4 Weitergabe der Ergebnisse an die betroffene Person

Der für das Programm medizinischen Leiter trägt die Verantwortung für die Mitteilung der Screening-Ergebnisse per Post an die betroffene Person und / oder ihren Referenzarzt (Ergebnis nach FIT mit nachfolgender Koloskopie, Koloskopie und Mammografie). Dieses Ergebnis wird grundsätzlich innerhalb von 8 Tagen nach der Konsultation der Person[34] übermittelt. Oft wird das positive Ergebnis (Krebsverdacht) 24 Stunden im Voraus an den Referenzarzt übermittelt, den die betroffene Person auf der Einwilligungserklärung angegeben hat. Diese frühe Weitergabe ermöglicht es dem jeweiligen Arzt, die Person zu kontaktieren, um allfällige Fragen zu beantworten.

Wenn das Ergebnis positiv ist, wird die Person in dem Schreiben aufgefordert, sich an den Arzt/die Ärzte ihrer Wahl zu wenden[35]. Die Behandlung wird im Einvernehmen zwischen der Person und ihrem medizinischen Team festgelegt, ohne dass das Programm und das Institut dabei involviert sein müssen.

Bei negativem Ergebnis (kein Krebsverdacht) werden die betroffene Person und ihr Arzt informiert. Sie wird eingeladen, weiterhin regelmässig an dem Screening teilzunehmen.

[33] In der Regel handelt es sich um eine Risikoanalyse, die mit einem Krebsverdacht abschliesst, wobei die endgültige Diagnose bei weiteren Untersuchungen nach einer Biopsie und pathologischen Untersuchungen gestellt wird.
[34] Vgl. Art. 9 Abs. 1 der Qualitätssicherungsverordnung.
[35] Vgl. Art. 9 Abs. 2 der Qualitätssicherungsverordnung.

Wird das Drucken und / oder Versenden Antwort an einen externen Dienstleister delegiert, so sind die Ausführungen in Abschnitt 2.2 zu beachten (insbesondere bzgl. des schriftlichen Vertrags).

2.4.5 Nachträglicher Informationsaustausch

Die betreffende Person oder ihre behandelnden Ärzte teilen dem Programm oder dem Institut manchmal von sich aus Informationen über die weitere medizinische Betreuung mit. Diese Informationen können in das MC-SIS-System eingegeben werden. Sie gelten als rechtmässig, wobei das aktive Vorgehen der Person oder ihrer Ärzte (die mit der mutmasslichen Zustimmung der Person handeln) als Einwilligung in die Verarbeitung der Daten gilt.

Es kommt auch vor, dass eine andere medizinische Fachkraft als der Referenzarzt, wie bspw. ein Onkologe, der für die Nachsorge der Person verantwortlich ist, sich direkt an ein Programm wendet und darum bittet, Daten über seine(n) Patienten/in zu erhalten. Das Programm kann diesem Antrag nur stattgeben, wenn es von der betreffenden Person eine **ausdrückliche Genehmigung** erhält (grundsätzlich eine schriftliche und unterschriebene Genehmigung der Person, die ihre Identität durch eine Kopie ihres Reisepasses oder Personalausweises nachweist). Das Programm kann die medizinische Fachkraft *nicht von sich aus informieren*, selbst wenn diese behauptet, von ihrem/r Patienten(in) ordnungsgemäss autorisiert zu sein. Wenn die Genehmigung des/r Patienten(in) vorliegt, übermittelt das Programm dann die nachgefragten Informationen über einen sicheren Kanal an die medizinische Fachkraft (z. B. per verschlüsselter E-Mail, verschlüsseltem USB-Stick, HIN-Netz („Health Info Net"), HPC-Karte der FMH[36]). Das Programm muss zudem mindestens sicherstellen, dass die angegebene E-Mail-Adresse die der beteiligten Fachperson ist.

2.4.6 Kommunikation im Ausland

Weder die Programme noch SCS übermitteln in der Regel Personendaten ins Ausland.

Die betreffende Person kann das Programm jedoch ausdrücklich auffordern, ihre eigenen Daten ins Ausland zu übermitteln oder sie an ihren bevollmächtigten Vertreter, in der Regel einen Arzt, im Ausland weiterzugeben. Diese Situation kann insbesondere dann auftreten, wenn die Person umzieht und die medizinische Behandlung im Ausland fortgesetzt wird.

In diesen in der Praxis selten vorkommenden Situationen erfolgt die Kommunikation nach den Anweisungen der Person und ist auf der Grundlage ihrer Zustimmung rechtmässig. In der Regel wird eine CD-ROM mit ihren Daten gebrannt und ihr übergeben. Das Programm muss auch überprüfen, ob die Anweisungen tatsächlich von der Person, um deren Personendaten es geht, oder von ihrem ordnungsgemäss bevollmächtigten Vertreter stammen. Falls erforderlich, wird das Programm die Person auf die Risiken einer Übertragung ins Ausland hinweisen.

[36] FMH, Rechtliche Grundlagen im medizinischen Alltag, Ein Leitfaden für die Praxis, S. 102.

B. 2.5 Datenspeicherung und Sicherheits- und Zugriffsmassnahmen, Monitoring

In diesem Kapitel werden die Schritte behandelt, die nach der Rückmeldung der Ergebnisse an die betroffene Person folgen. Es ist in neun Teile gegliedert. Der erste Teil betrifft Massnahmen zur Gewährleistung der Sicherheit der von den Programmen erhobenen und verarbeiteten Daten. Er spricht auch die Frage der Zugangsrechte der Programmmitarbeiter an. Der zweite Teil betrachtet die Ernennung eines Datenschutzbeauftragten des Programms. Der dritte präzisiert den Zugang zu Personendaten durch SCS.

Der vierte Teil erinnert daran, dass die an der Früherkennung beteiligten Personen ein Auskunftsrecht in Bezug auf ihre eigenen Daten haben. Fragen im Zusammenhang mit dem Widerruf der Einwilligung und Anträgen auf Datenlöschung, die durch diese Personen vorgelegt werden, werden im anschliessenden Teil behandelt (fünfter Teil).

Die Teile sechs bis neun betreffen die Offenlegung an Dritte; insbesondere werden die Bekanntgabe der Datensammlung an den Datenschutzbeauftragten und die Übermittlung der Daten an andere Behörden, insbesondere an die kantonalen Krebsregister und das BAG, diskutiert.

2.5.1 Sicherheit und Zugriff durch Programmmitarbeiter

Die vom Programm und seinen Partnern erhobenen Daten werden in MC-SIS gespeichert. Das Programm kann jederzeit auf die von ihm eingegebenen Daten zugreifen. Auf die Personendaten eines anderen Programms kann es nicht zugreifen.

Sowohl aus rechtlichen als auch aus ethischen Gründen ist es von grösster Wichtigkeit, dass diese Daten streng geschützt und vertraulich behandelt werden[37]. Darüber hinaus dürfen diese Daten nur in dem Umfang verwendet werden, der zur Erreichung des den Teilnehmern mitgeteilten Zwecks unbedingt erforderlich ist (sogenannte Grundsätze der Verhältnismässigkeit und der Zweckgebundenheit)[38].

In der Praxis fallen bei der Früherkennung die identifizierten Risiken in zwei Hauptgruppen: einerseits technische Ausfälle (Computerausfälle und andere Fehlfunktionen, die Fehler oder Datenverluste verursachen) und andererseits böswillige oder fahrlässige Handlungen (Datenmanipulation, Missbrauch, Diebstahl, Formularverlust).

Konkret muss das Programm über eine DS-Richtlinie verfügen, die durch eine Zugriffsrechte-Matrix und eine SOP ergänzt wird. Zusammengenommen präzisieren diese Dokumente, wer wann, wie und zu welchen Zwecken auf welche Daten (insbesondere in MC-SIS) zugreifen darf. Die Zugriffsrechte-Matrix führt den Namen jedes Mitarbeiters, der ein Zugriffsrecht zu Personendaten hat, zusammen mit dem Umfang dieses Rechts auf. Nur diejenigen Personen, die zur Erfüllung ihrer Aufgaben tatsächlich Zugriff auf Personendaten benötigen, dürfen diese Zugriffserlaubnis erhalten. Ihre Anzahl sollte auf ein Minimum beschränkt werden. Jeder elektronische Zugriff muss individuell (d. h. spezifisch durch den jeweiligen Mitarbeiter und nicht gemeinsam) und nachvollziehbar erfolgen[39]. **Jeder Programmmitarbeiter, auch wenn er keine durch die Matrix zugewiesenen Zugriffsrechte hat, muss eine schriftliche Vertraulichkeitserklärung unterzeichnen.**

[37] Nach Bundesrecht müssen gemäss Art. 7 Abs. 1 DSG „Personendaten [...] durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden." Die Sicherheitsmassnahmen werden auch in den Art. 8 bis 11 VDSG verdeutlicht.
[38] Siehe wiederum Art. 4 DSG.
[39] Art. 9. VDSG.

Um Personen ausserhalb des Programms am Zugriff auf Personendaten zu hindern, müssen die DS-Richtlinie und die Zugriffsrechte-Matrix auch die Zugangsmodalitäten zu den verschiedenen Standorten, die Richtlinien für die Verwaltung schriftlicher Dokumente (insbesondere der von den Teilnehmern auf Papier ausgefüllten Formulare), die Richtlinien für die Druckerverwaltung und den Zugang von Besuchern zu den Räumlichkeiten beschreiben. **Das Programm legt Sicherheits- und Identifizierungsmassnahmen fest, damit Unbefugte weder Gebäude noch Gebäudeteile (insbesondere die Standorte, an denen sich die Zugangsstationen zu MC-SIS befinden) betreten.** Grundsätzlich müssen Besuche vorab angekündigt, genehmigt und kontrolliert werden. Besucher sind in den Räumlichkeiten zu begleiten.

Die Zugriffsrechte-Matrix muss regelmässig aktualisiert werden, insbesondere im Hinblick auf Änderungen der Zugriffsrechte bei Neuzugang oder Austreten von Mitarbeitern. Die dazugehörige SOP beschreibt das Verfahren zur Aktualisierung der Zugriffsrechte (wer das Zugriffsrecht gewährt, auf Basis von welchem Verfahren, wer die Kontrollen durchführt; **SOP-3**).

Eine wesentliche Aufgabe des Programmverantwortlichen besteht darin, das Bewusstsein der Mitarbeiter zu schärfen. Die Erfahrung zeigt, dass die meisten Fälle von rechtswidriger Offenlegung („security breach") von Daten durch Mitarbeiter aufgrund von Fahrlässigkeit begangen werden, die selbst wiederum auf mangelnde Schulung zurückzuführen ist. Das Programm muss daher seine Mitarbeiter in Datenschutzfragen schulen. Die Schulung erfolgt nicht nur bei der Aufnahme ihrer Tätigkeit, sondern wird in regelmässigen Abständen wiederholt, solange die Beziehung zwischen dem Mitarbeiter und dem Programm oder den verschiedenen Dienstleistern andauert. In der Schulung soll näher eingegangen werden auf den Umfang der Geheimhaltung und die Verpflichtung zur Vertraulichkeit, die konkreten Massnahmen, die zu ergreifen oder zu vermeiden sind, die häufigsten Risiken und die Sanktionen im Falle eines Verstosses.

Schliesslich liegt es in der Verantwortung des medizinischen oder administrativen Leiters, die Einhaltung der DS-Richtlinie, der Zugriffsrechte-Matrix und der SOP-3 sowie die Einhaltung der darin festgelegten Verpflichtungen regelmässig zu überprüfen oder überprüfen zu lassen. Insbesondere überprüft er, dass nur Personen, die zum Zugriff auf Personendaten berechtigt sind, auf diese zugegriffen haben.

2.5.2 Datenschutzbeauftragter

Die Programme möchten vielleicht einen unabhängigen Datenschutzbeauftragten ernennen, um die Einhaltung der Datenschutzgesetze und der internen Datenschutzpolitik und -verfahren sicherzustellen[40]. Dieser Beauftragte kann ein Bevollmächtigter ausserhalb des Programms oder ein interner Mitarbeiter sein, sofern dieser über die erforderliche Unabhängigkeit verfügt. Wird ein Datenschutzbeauftragter ernannt, so sind seine Aufgaben schriftlich und in klarer Weise festzulegen.

[40] Art. 11a Abs. 5 Buchst. e DSG u. Art. 12a und 12b VDSG.

2.5.3 Datenzugriff durch SCS

SCS hat keinen Zugriff auf die Personendaten der Programme. Insbesondere nicht auf die Daten von Personen, die zur Früherkennung eingeladen wurden oder an ihr teilgenommen haben. Die Programme werden des Weiteren gebeten, solche Personendaten nicht an SCS zu übermitteln. Sollte dies aus irgendeinem Grund dennoch unvermeidbar sein, sind diese zu anonymisieren.

SCS muss von den Programmen aggregierte und/oder pseudonymisierte Daten erhalten. SCS erstellt damit periodisch einen Monitoringbericht, der die Screening-Ergebnisse anhand von Indikatoren statistisch darstellt[41]. Zu diesem Zweck kann SCS externe Experten mit der Analyse der besagten Daten beauftragen. Die Zusammenarbeit zwischen SCS und diesen Experten wird durch einen schriftlichen Vertrag geregelt, der eine Vertraulichkeitsklausel enthält, in der festgelegt ist, dass die Experten nicht auf personenbezogene, sondern nur auf pseudonymisierte Daten zugreifen. Der daraus hervorgehende Bericht wird veröffentlicht.

Darüber hinaus ist SCS für die technische Sicherheit der Daten im MC-SIS verantwortlich. Zu diesem Zweck beauftragte SCS CDI mit der Entwicklung eines **Sicherheitskonzeptes**, das die im MC-SIS implementierten technischen Sicherheitsmassnahmen beschreibt. Der Berner Datenschutzbeauftragte hat dieses Dokument im Dezember 2018 validiert. Es wird den kantonalen Datenschutzbeauftragten auf Verlangen zur Verfügung gestellt. **Dieses CDI-Sicherheitskonzept beschreibt die (organisatorischen und technischen) Sicherheitsmethoden (Protokollierung, regelmässiges Backup, Hacking-Prävention) im Zusammenhang mit dem Datenzugriff und der Datenverarbeitung.**

2.5.4 Auskunftsrechte der betroffenen Personen

Das Gesetz gibt jeder Person das Recht, danach zu fragen, ob ihre persönlichen Daten – und wenn ja, welche Daten genau – verarbeitet werden[42]. Von diesem Recht können alle Personen Gebrauch machen, auch diejenigen, die nicht am Screening teilgenommen haben. Die Person muss ihren Zugangsantrag direkt an das Programm richten. Sendet sie ihren Antrag an das Institut, so leitet es ihn an das Programm weiter.

Die Person kann eine (schriftliche) Kopie ihrer Akte verlangen, d. h. *aller* sie betreffenden Daten, die sich in den Händen des Verantwortlichen der Datensammlung (auch „Inhaber der Datensammlung" genannt) befinden. Dieses Recht beschränkt sich daher nicht nur auf Daten, die die Person selbst zur Verfügung gestellt hat, sondern auch auf Daten, die von Dritten (z. B.

[41] Siehe z. B. SCS, Rapport du monitoring 2012 des programmes suisses de dépistage du cancer du sein – un bref bilan.

[42] Im Bundesrecht ergibt sich dieses Auskunftsrecht aus Art. 8 DSG und wird in den Art. 1 und 2 VDSG erläutert. Gemäss Art. 8 Absatz 1 DSG kann „[jede] Person [...] vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden." Absatz 2 beschreibt die Daten, die der Inhaber der Datensammlung in der Antwort auf eine solche Anfrage bereitstellen muss. Absatz 3 erlaubt die Übermittlung medizinischer Daten über einen Arzt und nicht direkt an die betroffene Person, wenn sie dies wünscht. Absatz 4 behandelt die Situation, in der der Inhaber der Datensammlung bestimmte Aktivitäten durch einen Dritten ausführen lässt. Nach Absatz 5 erfolgt die Bereitstellung von Daten auf ein Auskunftsersuchen hin grundsätzlich kostenlos. Schliesslich präzisiert Absatz 6, dass es sich um ein unveräusserliches Recht der Person handelt. Die Fälle, in denen der Inhaber der Datensammlung ein Auskunftsersuchen abschlägig bescheiden kann, sind in Art. 9 beschrieben; im Falle der Früherkennung kommt jedoch grundsätzlich keine Ausnahme in Betracht.

Fachärzten) zur Verfügung gestellt werden[43]. Die Herkunft dieser Daten ist anzugeben[44]. Das Programm muss dem Gesuchsteller auch den Zweck der Datensammlung mitteilen[45].

Entdeckt die betroffene Person in ihren Daten Fehler, kann sie diese melden und deren Korrektur verlangen[46]. Die Person muss sich dazu erneut an das Programm wenden. Wendet sie sich an das Institut, verweist dieses sie an das Programm.

Konkret muss das kantonale Programm eine SOP (SOP-4) erstellen, die beschreibt, wie es Auskunfts- und Korrekturanträge bearbeitet. Diese geht insbesondere darauf ein, wie der Antrag zu formulieren und die Identität des Gesuchstellers festzustellen ist (grundsätzlich Identitätskarte oder Reisepass[47]), wer den Antrag bearbeitet, wie die Informationen dann an die Person übermittelt werden, in welcher Form und innerhalb welcher Zeitspanne (max. 30 Tage ab Antrag[48]).

Die Übermittlung der Daten erfolgt grundsätzlich kostenlos[49]. Erfolgt sie nicht zu eigenen Händen, wird sie über ein sicheres Mittel abgewickelt, z. B. eine verschlüsselte E-Mail, nachdem die Richtigkeit der E-Mail-Adresse ordnungsgemäss überprüft wurde. Grundsätzlich darf das Programm Anträge, die sich auf das Vorhandensein von Personendaten beziehen, Anträge auf Zugang zu diesen Daten oder Anträge auf deren Berichtigung nicht ablehnen oder einschränken.

2.5.5 Widerruf der Einwilligung

Jede Person, die in die Teilnahme an der Früherkennung eingewilligt hat, kann ihre Einwilligung jederzeit widerrufen. Sie teilt ihre Entscheidung grundsätzlich dem Programm mit. Wenn sie ihre Entscheidung dem Institut mitgeteilt hat, z. B. vor Ort während des Besuchs, wird sie

[43] Andererseits muss das Programm keine Daten von Dritten anfordern, die es selbst nicht besitzt, auch nicht, wenn die betreffende Person dies verlangt.
[44] Im Bundesgesetz sieht Art. 8 Abs. 2 Buchst. a DSG vor: „Der Inhaber der Datensammlung muss der betroffenen Person mitteilen: a. 1 alle über sie in der Datensammlung vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten".
[45] Im Bundesgesetz, siehe Art. 8 Abs. 2 Buchst. b DSG. Das Programm ist verpflichtet, alle die Person betreffenden Daten, die in der Datensammlung enthalten sind, zu übermitteln, einschliesslich Informationen über die Herkunft der Daten, den Zweck und ggf. die Rechtsgrundlage der Verarbeitung, die Kategorien der bearbeiteten Personendaten, die Beteiligten an der Datensammlung und die Datenempfänger (Personen und Institutionen, denen die Daten übermittelt werden). Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Die Rechte der betroffenen Personen bei der Bearbeitung von Personendaten, S. 7.
[46] Im Bundesgesetz sieht Art. 5 Abs. 2 DSG vor: „Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden."
[47] Der Antrag muss grundsätzlich schriftlich gestellt werden (vgl. im Bundesgesetz Art. 1, Abs. 1 VDSG). Zu Beweiszwecken ist dem Antrag eine Kopie eines Ausweisdokuments beizufügen und der Antrag per Einschreiben zu versenden. Das Auskunftsersuchen und die Übermittlung der angeforderten Informationen kann auf elektronischem Wege erfolgen (Art. 1 Abs. 2 VDSG), sofern das Programm dies ausdrücklich vorsieht und geeignete Massnahmen ergreift, um die Identifizierung der betroffenen Person zu gewährleisten und die Daten der betroffenen Person bei der Übermittlung der Auskünfte vor jedem unbefugten Zugriff Dritter zu schützen (Art. 1, Abs. 2 VDSG). Die Person kann auch mit einem Ausweis ins Sekretariat des Screening-Zentrums kommen. Eine besondere Situation betrifft Anträge von Familienangehörigen der betroffenen Person, wenn diese verstorben ist (dazu Art. 1, Abs. 7 VDSG).
[48] Art. 1, Abs. 4 VDSG.
[49] Die Auskünfte werden in der Regel kostenlos und schriftlich in Form eines Ausdrucks oder einer Fotokopie zur Verfügung gestellt (Art. 1 VDSG und Ausnahme unter Art. 2 VDSG). Medizinische Daten und Mammographiebilder können auf CD-ROM zur Verfügung gestellt werden. Eine Kostenbeteiligung (maximal 300 CHF, Art. 2 Abs. 2 VDSG) kann vom Programm ausnahmsweise verlangt werden (Art. 2 Abs. 1 VDSG), sofern die Person die angeforderten Auskünfte bereits innerhalb der letzten zwölf Monate erhalten hat (es sei denn, sie hat ein berechtigtes Interesse, ein neues Auskunftsersuchen zu stellen) und sofern die Übermittlung der Informationen mit erheblichem Aufwand verbunden ist (z. B. sofern die Daten bereits teilweise anonymisiert wurden oder umfangreiche Recherchen erforderlich sind).

vom Institut an das Programm weitergeleitet. Das Programm muss sicherstellen, dass die erhaltene Willensbekundung von der dazu berechtigten Person stammt (z. B. Identitätsprüfung).

Wenn der Test und die Analyse jedoch bereits stattgefunden haben und die Ergebnisse übermittelt wurden, hat der Widerruf der Einwilligung nur begrenzte Auswirkungen. Es findet keine weitere Verarbeitung statt. Das Programm bleibt gesetzlich dazu verpflichtet, das vollständige Dossier zu speichern und zu archivieren. Es darf daher nicht die gesamte Datei löschen, auch wenn die Person es dazu auffordert.

Wenn die Analyse der Daten, einschliesslich der Bilder, zum Zeitpunkt des Eingangs des Widerrufs noch nicht stattgefunden hat, stellt das Programm die Verarbeitung der Daten ein. Sie werden nicht an Fachärzte oder andere Dritte weitergegeben, sondern nur zu Archivierungszwecken aufbewahrt.

Wenn zum Zeitpunkt der Widerrufserklärung die Analyse bereits stattgefunden hat, das Ergebnis jedoch noch nicht mitgeteilt wurde, wird das Ergebnis nicht gemeldet. Das Programm darf sich vergewissern, dass die Person in dieser Hinsicht eine informierte Entscheidung getroffen hat. Es muss jedoch darauf achten, dass es ihr Recht auf Nicht-Wissen respektiert. Es darf ihr keine Informationen aufzwingen, die sie nicht erhalten möchte. Auch dann nicht, wenn das Screening-Ergebnis positiv (d.h. ein Verdacht auf eine maligne Veränderung) sein sollte.

Die Person kann auch beschliessen, dass sie in Zukunft nicht mehr zur Teilnahme an der Früherkennung eingeladen werden möchte. In diesem Fall nimmt das Programm ihre Entscheidung zur Kenntnis und respektiert diese. In MC-SIS wird ein entsprechender Eintrag vorgenommen.

Die Person kann ihren Widerruf auch widerrufen, d. h. ihre Zustimmung zur Verarbeitung ihrer Daten erneut erteilen. In diesem Fall wird der Vorgang fortgesetzt. Wenn die Daten beispielsweise noch nicht an Fachärzte zur Analyse übermittelt wurden, werden sie weitergeleitet, sobald die Person erneut ihre Zustimmung gibt. Vorbehalten bleibt der Fall, dass die Daten nun zu alt sind, um auf sinnvolle Weise analysiert werden zu können.

2.5.6 Mitteilung an die kantonalen Datenschutzbeauftragten

Einige kantonale Gesetze schreiben vor, dass Sammlungen von Personendaten, insbesondere von schützenswerten medizinischen Daten, gemeldet werden müssen. Davon betroffen sind auch Früherkennungsprogramme. Das Programm muss sich darüber informieren, ob der Kanton und ggf. der Beauftragte an das Meldeverfahren oder den Inhalt besondere Anforderungen[50] stellen. **Das Dokument, mit dem das Programm seine Datensammlung dem Beauftragten meldet, muss schriftlich vorliegen und der DS-Richtlinie beigefügt werden.**

Bei Programmen, die als privatrechtliche Einrichtung (im Gegensatz zu einer Behörde) organisiert sind und die nach kantonalem Recht nicht verpflichtet sind, ihre Datensammlung dem kantonalen Beauftragten zu melden, ist zu prüfen, ob eine Meldung der Datensammlung an

[50] Typischerweise enthält die Mitteilung an den Kantonsbeauftragten die folgenden Elemente: Name und Anschrift des Inhabers der Datensammlung; Name und vollständige Bezeichnung der Datensammlung; die Person oder Stelle, bei der das Auskunftsrecht ausgeübt werden kann; Rechtsgrundlage und Zweck der Datensammlung; die Kategorien der bearbeiteten Daten (in diesem Abschnitt werden die in der Datensammlung enthaltenen Datenarten angegeben, z. B. Name, Anschrift, Beruf, Geburtsdatum); der Kreis der betroffenen Personen und ihre ungefähre Anzahl; die Kategorien der Datenempfänger; die Kategorien der Beteiligten an der Datensammlung. Der Kantonsbeauftragte kann zusätzliche Elemente oder Informationen anfordern.

den Eidgenössischen Datenschutzbeauftragten erforderlich ist[51]. **Die betreffenden Programme wenden sich an den kantonalen Beauftragten, um ihre Verpflichtungen zu klären.**

Grundsätzlich werden dem (eidgenössischen oder kantonalen) Beauftragten keine Personendaten, d. h. keine Daten über die betroffenen Personen (Teilnehmende), mitgeteilt.

2.5.7 Mitteilung an das kantonale Krebsregister

Jedes kantonale Krebsregister ist durch ein entsprechendes kantonales Gesetz befugt, Informationen über im Kantonsgebiet diagnostizierte Krebserkrankungen zu erhalten. Es bedarf dieser Informationen, um die langfristige Wirksamkeit des Screenings auf Kantonsebene zu analysieren. Tatsächlich werden die endgültige Diagnose und/oder die endgültigen Informationen über das Auftreten von Intervallkrebs nur in diesem Register erfasst. Es erfasst alle im Kantonsbereich (innerhalb oder ausserhalb der Screenings) diagnostizierten Krebserkrankungen und führt eine epidemiologische Beobachtung bei den so diagnostizierten Patienten durch.

Das Programm sorgt für die Übermittlung an das genannte Register. Gegebenenfalls sendet das kantonale Register eine Bestätigung der Diagnose an das Programm.

Die Meldung an das kantonale Krebsregister ist rechtmässig, wenn sie auf dem kantonalen Gesetz zur Früherkennung basiert und/oder auf dem kantonalen Gesetz zur Erstellung des kantonalen Krebsregister gründet. Diese Meldung steht auch in einem angemessenen Verhältnis zu dem verfolgten Ziel, nämlich die Qualität und Wirksamkeit des Screenings zu gewährleisten. Dieser Meldungsprozess wird in der DS-Richtlinie des Programms, ggf. in den Anhängen, niedergelegt.

2.5.8 Internes Monitoring des Programms und Meldung an die Behörden

Jedes Programm erstellt einen jährlichen Tätigkeitsbericht[52], der auf den von ihm festgelegten Qualitätsindikatoren basiert. Darüber hinaus hat SCS einen Mindestkatalog von Indikatoren definiert, die auf nationaler Ebene berechnet werden [Anhang V]. Diese Berichte enthalten keine Personendaten, auch wenn sie auf den Personendaten beruhen, auf die das Programm über MC-SIS zugreift.

Programme können einen externen Dienstleister beauftragen, um die Personendaten aus Experten MC-SIS zu analysieren. **In diesem Fall muss die Zusammenarbeit mit diesem Dienstleister durch einen schriftlichen Vertrag, geregelt werden. Der Vertrag muss eine Datenschutzklausel enthalten.**

Diese Berichte können anderen kantonalen oder Bundesbehörden vorgelegt werden. Das Programm überprüft seine Übermittlungspflichten und -modalitäten (insbesondere: wer übermittelt was, wie und wann) und erfasst die Informationen in seiner DS-Richtlinie.

[51] Nach Art. 11a Abs. 3 DSG gilt: „Private Personen müssen Datensammlungen anmelden, wenn: a. regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden". In Absatz 5 desselben Artikels sind jedoch mehrere Ausnahmen von der Anmeldepflicht vorgesehen. Im Bundesrecht regeln die Art. 3 bis 4 VDSG den Inhalt der Erklärung und die Ausnahmen von der Anmeldepflicht.
[52] Vgl. Art. 10 Abs. 1 der Qualitätssicherungsverordnung.

2.5.9 Mitteilung an Drittforscher

Jedes Programm, das beabsichtigt, mit Dritten an Forschungsprojekten zusammenzuarbeiten, und sei es auch nur in Teilbereichen, ist verpflichtet, die Forschungsgesetzgebung (meist das Humanforschungsgesetz (HFG) und seine Verordnungen) einzuhalten. Die systematische Erhebung zusätzlicher Daten für Forschungszwecke muss Gegenstand einer SOP-1 sein (s. dazu bereits Abschnitt 2.3.3).

2.6 Löschung der Daten

Im Laufe der Zeit kann sich die Speicherung von Daten als unverhältnismässig erweisen. Sie ist dann nicht mehr gerechtfertigt und rechtmässig[53]. Das Gesetz verlangt dann die Löschung dieser Daten. Das heisst, sie müssen vollständig und endgültig unzugänglich gemacht werden[54]. Im Einzelfall kann eine teilweise Löschung gerechtfertigt sein (z. B. Löschung älterer und Erhalt neuerer Daten).

Derzeit gibt es kein Gesetz, das die (minimale oder maximale) Aufbewahrungsfrist für Screening-Daten regelt. Die kantonalen Gesetze legen manchmal die Aufbewahrungsfrist von Gesundheitsdaten im Allgemeinen fest. In Ermangelung einer bestimmten Frist, wird oft die Verjährungsfrist für Haftungsklagen (vertragliche oder aus unerlaubter Handlung) als Bezugspunkt herangezogen. Das heisst, solange gegen ein Programm oder Institut von der betroffenen Person eine Haftungsklage eingereicht werden kann, muss es die für seine Verteidigung erforderlichen Daten aufbewahren. Heute beträgt die absolute Verjährungsfrist grundsätzlich 10 Jahre ab der schädigenden Handlung (in diesem Fall die medizinische Handlung, die den Schaden verursacht hat). Am 1. Januar 2020 wird die absolute Frist auf 20 Jahre erhöht werden, wiederum beginnend mit der schädigenden Handlung[55]. Daher sollte die *vollständige* Akte nicht vor Ablauf von 20 Jahren nach der letzten Handlung vernichtet werden. So kann bspw. die Analyse alter Bilder helfen zu erklären, weshalb gewisse Untersuchungen auf eine bestimmte Weise durchgeführt wurden oder nicht.

Die Aufbewahrung der Daten bis zum Ablauf der Verjährungsfrist ist auch dann Pflicht und erlaubt, wenn die betroffene Person eine vorzeitige Löschung verlangt (s. auch Abschnitt 2.5.5).

Konkret muss die programmeigene DS-Richtlinie beschreiben, wie die Datenlöschung erfolgt, und dabei besonders auf die Frage eingehen, wer wie entscheidet, wer die Löschung durchführt und wer die Vollständigkeit der Löschung überprüft. Grundsätzlich liegt die Verantwortung für die Löschung beim medizinischen Leiter der einzelnen Programme. MC-SIS sendet einen Hinweis an das Programm, wenn Personendaten länger als 20 Jahre gespeichert sind.

---

[53] Zur Erinnerung: Die gesamte Datenverarbeitung muss rechtmässig und verhältnismässig sein (Art. 4 Abs. 1 und 2 DSG). Die Speicherung von Personendaten stellt eine Datenverarbeitung dar. Daher muss sich der Inhaber der Datensammlung die Frage stellen, ab welchem Zeitpunkt die Datenspeicherung zur Erreichung des verfolgten Zwecks nicht mehr erforderlich ist und daher unverhältnismässig wird. Von diesem Zeitpunkt an muss die Verarbeitung eingestellt oder in ihrem Umfang eingeschränkt werden.

[54] Datenvernichtung: http://www.thinkdata.ch/fr/glossaire.

[55] Nach Art. 60 Abs.1bis verfügt: „Bei Tötung eines Menschen oder bei Körperverletzung verjährt der Anspruch auf Schadenersatz oder Genugtuung mit Ablauf von drei Jahren von dem Tage an gerechnet, an welchem der Geschädigte Kenntnis vom Schaden und von der Person des Ersatzpflichtigen erlangt hat, jedenfalls aber mit Ablauf von zwanzig Jahren, vom Tage an gerechnet, an welchem das schädigende Verhalten erfolgte oder aufhörte". Nach Art. 128a heisst es: „Forderungen auf Schadenersatz oder Genugtuung aus vertragswidriger Körperverletzung oder Tötung eines Menschen verjähren mit Ablauf von drei Jahren vom Tage an gerechnet, an welchem der Geschädigte Kenntnis vom Schaden erlangt hat, jedenfalls aber mit Ablauf von zwanzig Jahren, vom Tage an gerechnet, an welchem das schädigende Verhalten erfolgte oder aufhörte."

3 Schlussfolgerungen

Damit das Screening seine Ziele erreichen kann, ist das Vertrauen der Bevölkerung unerlässlich. Um dieses Vertrauen zu wahren, müssen die von den einzelnen Personen anvertrauten Daten streng vertraulich behandelt werden. In dieser Hinsicht ist es auch wichtig, dass die Datenschutzrechte von Einzelpersonen, insbesondere das Einwilligungsrecht und das Auskunftsrecht, respektiert werden.

Um dieses Ziel zu erreichen, muss jedes Programm seine internen Prozesse festlegen und deren Einhaltung sicherstellen. Es muss den Screening-Teilnehmern vollständige und zuverlässige Informationen zur Verfügung stellen, die eine freie und informierte Einwilligung ermöglichen. Es sensibilisiert seine Mitarbeiter und externen Partner in regelmässigen Abständen und sorgt dafür, dass die Verwendung nicht anonymisierter Daten auf ein Minimum reduziert wird. Es stellt sicher, dass die Daten korrekt und auf dem neuesten Stand sind. Schliesslich schliesst es Verträge ab, die die Vertraulichkeit der Personendaten gewährleisten.

Zusammenfassend lässt sich sagen, dass die Programmleiter für den Datenschutz verantwortlich sind. Jedes Programm muss über eine DS-Richtlinie verfügen, die die spezifischen Gesetze des Bundes und der Kantone sowie die konkreten Aktivitäten des Programms berücksichtigt. Das Programm sollte, soweit möglich, den kantonalen Datenschutzbeauftragten in die Ausarbeitung dieser Richtlinie einbeziehen. Ggf. meldet es die Datensammlung dem kantonalen oder eidgenössischen Beauftragten.

Datenschutz ist eine anspruchsvolle Aufgabe, die ständige Wachsamkeit erfordert, denn niemand ist jemals gänzlich bewahrt vor Vertraulichkeitsverstössen. Solide interne Verfahren, die allen Mitarbeitern wohlbekannt sind, bilden daher ein wichtiges Instrument, um ein Höchstmass an Schutz zu gewährleisten.

swiss cancer screening

ANLAGEN

Liste:

Anhang I **Begriffe**

Anhang II **Rechtsgrundlagen**

Anhang III **Grundprinzipien und Teilnehmerrechte**

Anhang IV **Vorlagen für die Teilnehmer**

Anhang V **Nationales Monitoring-Konzept**

Anhang VI **Konstituierende Bestandteile der DS-Richtlinie (und deren Anhänge)**

Anhang VII **Zusammenfassung der von den Programmen zu erstellenden Standard Operating Procedures (SOP)**

Anhang VIII **Abkürzungsverzeichnis**

Anhang I: Begriffe

In der Schweiz unterscheidet das Gesetz grundsätzlich zwischen personenbezogenen Daten und anonymen Daten. Die Verarbeitung personenbezogener Daten unterliegt dem Gesetz, während die Verarbeitung anonymisierter Daten grundsätzlich nicht dem Gesetz unterliegt. In der Praxis werden häufig andere Begriffe verwendet; beispielsweise sind sensible Daten eine Unterkategorie von personenbezogenen Daten, die einem erhöhten Schutz unterliegen müssen.

Personendaten: Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3a DSG). Angaben sind sämtliche Informationsarten, unabhängig vom Übertragungsweg und vom Träger. Die im Rahmen der Gesundheit verarbeiteten Daten sind grundsätzlich personenbezogene Daten, da es sich um identifizierte oder identifizierbare natürliche Personen handelt[56]. Mithilfe der identifizierenden Daten lässt sich die Identität einer Person eindeutig bestimmen. Grundsätzlich kann jede Person durch die Kombination einzelner der folgenden Angaben identifiziert werden: Vorname, Name, Geburtsdatum, Foto, Unterschrift, Geschlecht, Grösse und Herkunft. Im medizinischen Bereich fallen auch Identitätsmerkmale wie die Patientenidentifikationsnummer oder die AHV-Nummer in die Kategorie der identifizierenden Daten.

Anonyme Daten: Die anonymisierten Daten sind nicht mehr oder nur mit einem unverhältnismässig grossen Aufwand mit den betroffenen Personen in Verbindung zu bringen. Sie gelten nicht mehr als Personendaten. Folglich ist auch das Datenschutzgesetz nicht mehr anwendbar. Zur Anonymisierung gesundheitsbezogener Personendaten müssen alle Angaben, die für sich allein oder in ihrer Kombination die Wiederherstellung des Bezugs zu einer Person ohne unverhältnismässigen Aufwand erlauben, irreversibel unkenntlich gemacht oder gelöscht werden. Insbesondere unkenntlich gemacht oder gelöscht werden, müssen Name, eindeutig kennzeichnende Identifikationsnummer (Versichertennummer[57], Fallnummer), Geburtsdatum (höchstens der Monat und das Jahr sind anzugeben), genaues Todesdatum (höchstens der Monat und das Jahr sind anzugeben) und die genaue Wohnadresse (lediglich die Gemeindenummer des BFS ist anzugeben). Allerdings sei darauf hingewiesen, dass die medizinischen Daten nie vollständig unkenntlich gemacht werden können, da jeder Fall individuell ist und die Identifizierung eines Patienten selbst mit „anonymisierten“ Daten möglich ist.

Besonders schützenswerte Daten: Personendaten über die Gesundheit (im weiteren Sinne) gelten als besonders schützenswerte Daten (Art. 3c DSG).

Bearbeitung von Personendaten: Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Ändern, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3e DSG).

Bekanntgabe von Personendaten: Das Zugänglichmachen von Personendaten (Art. 3f DSG), insbesondere das Einsichtgewähren, Weitergeben oder Veröffentlichen.

Pseudonymisierte oder verschlüsselte Daten Die Pseudonymisierung (bzw. Verschlüsselung der Identität) ist ein Verfahren zur Trennung der identifizierenden Daten von den übrigen Personendaten. Die zwischen den beiden Datenkategorien hergestellte Beziehung erfolgt mittels eines Pseudonyms bzw. Codes (ein verschlüsselter Identifikator), der einen Rückschluss auf die identifizierenden Daten (oft in Form einer Korrespondenztabelle) sowie auf die übrigen

[56] European Data Protection Supervisor, Avis 1/2015, La santé mobile : concilier innovation techologique et protection des données, p.6
[57] Es gibt einen Vorgang zur Pseudonymisierung der Versichertennummer (Art. 23 Entwurf KRV) (vgl. Kap. 7).

Personendaten (die sog. pseudonymisierten Daten) zulässt. Die Zuordnung der beiden Datenkategorien (Re-Pseudonymisierung / Re-Identifizierung) ist somit nur durch befugte Personen herzustellen, das heisst, nur durch diejenigen, die Zugriff auf die Korrespondenztabelle haben. Die pseudonymisierten Daten bleiben nach wie vor personenbezogene Daten, sofern sie nicht nur durch den Verantwortlichen der Datenverarbeitung, sondern auch durch Dritte, welche die Daten mit fremden Informationen aus externen Quellen verbinden, re-identifiziert werden können. Insbesondere im Rahmen der Forschung wird häufig der Begriff pseudonymisierte Daten verwendet, da die Forschung an diesen Daten weniger strengen Regeln unterliegt als die Personendaten.

Anhang II: Rechtsgrundlagen

In diesem Anhang werden die Rechtsgrundlagen auf internationaler, Bund- und kantonaler Ebene dargestellt. Es wird auch auf die unverbindlichen Regeln (bekannt als "Soft law") für das Screening verwiesen.

A. Von der Schweiz ratifizierte Übereinkommen

Übereinkommen des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV-Nr. 108) unterzeichnet in Strassburg am 28.01.1981: Das Übereinkommen ist für die Schweiz am 1. Februar 1998 in Kraft getreten. Die Vertragsparteien verpflichten sich, das Übereinkommen auf automatisierte Dateien/Datensammlungen und automatische Verarbeitungen von personenbezogenen Daten im öffentlichen und privaten Bereich anzuwenden. Die Bestimmungen dieses Übereinkommens sind jedoch nicht direkt anwendbar (self-executing). Einzelne Personen können daher nicht unmittelbar daraus Recht ableiten (non self-executing). Die Aktualisierung dieses Übereinkommens und die Modernisierung der darin festgelegten Grundsätze erfolgte in der Europäischen Datenschutzrichtlinie von 1995 und anschliessend in der Allgemeinen Datenschutzverordnung (DGPS). Das DGPS ist für die gesamte Europäische Union verbindlich. Sie gilt nicht für Krebsvorsorgeprogramme in der Schweiz.

B. Bundesrechtliche Gesetzesgrundlagen

Dieser Abschnitt listet und beschreibt kurz alle Bundesgesetze, die sich auf die eine oder andere Weise mit medizinischen Daten befassen. Es sei jedoch darauf hingewiesen, dass das DSG nach wie vor der am weitesten verbreitete Text ist, zumal es in der Regel als Modell für die Kantone dient.

Bundesverfassung (Art. 13), SR 101: Die Bundesverfassung gewährt jeder Person das grundlegende Recht auf „Schutz vor Missbrauch ihrer persönlichen Daten“ (Art. 13 Abs. 2 BV). Sie garantiert somit das Recht auf informationelle Selbstbestimmung, das heisst, dass der Einzelne grundsätzlich selbst darüber bestimmen darf, wann und wem er persönliche Lebenssachverhalte offenbart. Die Kantonsverfassungen enthalten ähnliche Bestimmungen (Art. 21 Genfer Verfassung, Art. 12 Freiburger Verfassung, Art. 15 Verfassung des Kantons Waadt, Art. 18 Verfassung des Kantons Bern, etc.).

Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1 und Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG), SR 235.11: Das Bundesgesetz über den Datenschutz gilt für alle von der Bundesverwaltung oder im persönlichen Bereich durchgeführten Bearbeitungen personenbezogener Daten. Die kantonalen Programme, die den Datenschutzbestimmungen der Kantone unterliegen, sind dem Bundesgesetz also nicht unmittelbar unterstellt. Gesundheitsbezogene Daten – wie beispielsweise Aufzeichnungen über den Verlauf einer Behandlung, Symptombeschreibungen, Diagnosen, Verordnungen von Arzneimitteln, Laborresultate, Röntgenbilder – sind besonders schützenswerte Personendaten, für deren Bearbeitung ein spezieller Schutz erforderlich ist. Das vorliegende Grundlagendokument beruht in erster Linie auf dem DSG.

Gesetz über die Registrierung von Krebserkrankungen (KRG), SR 818, 33 und Verordnungsentwurf (KRV), SR 818.331
Die Daten in den kantonalen Krebsregistern werden an eine vom Bund finanzierte nationale Stelle für Krebsregistrierung übermittelt, die diese sammelt, auswertet und veröffentlicht. Künftig soll ein Mindestdatensatz, der insbesondere die genaue Diagnose, das Datum, an dem die

Diagnose gestellt wurde, und das Datum, an dem die Behandlung begonnen hat, für jeden einzelnen Fall erhoben werden. Der Patient kann die folgenden Rechte zum Schutz personenbezogener Daten ausüben: Information (Art. 5 KRG), Widerspruch (Art. 6 KRG), Anspruch auf Unterstützung und Auskunft (Art. 7 KRG).

Strahlenschutzgesetz (StSG), SR 814.50: Das Strahlenschutzgesetz sieht vor, dass der mit der medizinischen Untersuchung beauftragte Arzt der Aufsichtsbehörde die Daten bekanntgibt, die für die medizinische Überwachung und das Erstellen von Statistiken notwendig sind (Art. 14 StSG).

Gesetz über das elektronische Patientendossier (EPDG), SR 816.1 und weitere geplante Gesetze im Bereich eHealth: Das Gesetz über das elektronische Patientendossier weist auf die freie und aufgeklärte Einwilligung des Patienten hinsichtlich der Bearbeitung der eigenen Daten (Art. 3 EPDG) und auf das dem Patienten zustehende Zugriffsrecht auf die eigenen Daten (Art. 4 EPDG) hin. Ebenso sind Regelungen von Bund und Kantonen in Sachen eHealth mit Auswirkungen auf den Bereich Datenschutz vorgesehen; die Entwicklungen in diesem Bereich sind aufmerksam zu verfolgen.

Bundesgesetz über die Forschung am Menschen (HFG), SR 810.30 und Art. 321 Schweizerisches Strafgesetzbuch SR 311.0: Das Humanforschungsgesetz enthält Vorschriften zu Transparenz und Datenschutz. Nun stellt sich jedoch die Frage, ob das Gesetz Auswirkungen im Bereich Screening hat. Laut Art. 3 HFG gilt die Forschung als eine methodengeleitete Suche nach verallgemeinerbaren Erkenntnissen und wird durchgeführt an gesundheitsbezogenen Personendaten. In diesem Sinne wäre das Screening im Bereich der Forschung anzusiedeln. Ebenso wären Daten, die im Rahmen des Programmes erhoben und zum Erhalt neuer Erkenntnisse verwendet werden, der Forschung zuzuordnen. Somit wären die Vorschriften des Humanforschungsgesetzes anwendbar.

Strafgesetzbuch Art. 321. Die Weitergabe von Patientendaten an Dritte ist nur zulässig, wenn der Patient den Arzt von seiner Schweigepflicht entbindet oder wenn das Gesetz dies erlaubt. Die strafrechtliche Geheimhaltungspflicht (Art. 321 StGB) gilt nur für die darin genannten Berufe, d. h. Ärzte und deren Assistenten. Krankenschwestern und medizinische Assistenten können als Hilfskräfte betrachtet werden. Ein Verstoss gegen die Geheimhaltungspflicht kann auf Antrag des Geschädigten zu einem Strafverfahren führen.

Verordnung über die Qualitätssicherung bei Programmen zur Früherkennung von Brustkrebs durch Mammographie, SR 832.102.4: Die Verordnung legt die Mindestvoraussetzungen fest, die die organisierten Programme zur Früherkennung von Brustkrebs erfüllen müssen, sie enthält jedoch keine speziellen Vorschriften zum Datenschutz.

C. Kantonale Gesetzesgrundlagen

Kantonale Gesetze zum Datenschutz: Fast jeder Kanton verfügt über ein eigenes Gesetz zum Datenschutz. Die kantonalen Datenschutzgesetze regeln die Bearbeitung von Daten durch Kantonsverwaltungen, zu denen u.a. auch die Früherkennungsprogramme gehören. Die Rechtsgrundlagen gelten für sämtliche kantonale Behörden und sind daher nicht speziell für die Bearbeitung medizinischer Daten ausgelegt. Sie legen die allgemeinen Datenschutzgrundsätze fest sowie die Rechte von Personen, deren Daten durch öffentliche Stellen bearbeitet werden. Es ist Aufgabe des Programms, zusammen mit dem kantonalen Datenschutzbeauftragten den Schutz der Daten und die Einhaltung der Bestimmungen auf kantonaler Ebene sicherzustellen. Nachstehend folgt eine Auflistung der unterschiedlichen kantonalen Gesetze:

Rechtsgrundlagen auf kantonaler Ebene: http://www.privatim.ch/de/internaldatenschutz-gesetzgebung-kantone/

Kantonale Gesundheitsgesetze und dazugehörige Verordnungen: Die kantonalen Gesundheitsgesetze und die dazugehörigen Verordnungen können Bestimmungen über die Krebs-Früherkennung und den Datenschutz, insbesondere über die Patientenakte, enthalten. Zuweilen gibt es eine spezielle Verordnung betreffend die kantonalen Früherkennungsprogramme (zum Beispiel in Freiburg).

D. Soft law

Hierbei handelt es sich um Richtlinien, bewährte Praktiken oder Qualitätsstandards, die in der Schweiz anwendbar, jedoch nicht verbindlich sind.

Qualitätsstandards für die organisierte Brustkrebs-Früherkennung in der Schweiz (2014): Die Qualitätsstandards der Krebsliga Schweiz enthalten Vorschriften über die Aufbewahrung und Archivierung von Mammographien (S. 6 §d), den Zugang der Programme zu den Bevölkerungsdaten (S. 7 §o und §s), die Anwendung der Datenschutzgesetze (S. 7 §r), den Datenaustausch (S. 8 §t), die Qualitätskontrolle und -sicherung (S. 10 §k et p.11 §c).

European Guidelines for quality assurance in breast cancer screening and diagnosis Fourth Edition: Das Dokument weist darauf hin, dass gemäss der Richtlinie 95/46/EG zur Überprüfung der Datenerhebung, der Schutz personenbezogener Daten ein Grundrecht jedes EU-Bürgers ist. Die europäischen Leitlinien sehen vor, dass die Einladung zum Programm Informationen über den Datenschutz und die Vertraulichkeit enthalten muss. Ausserdem hebt das Dokument hervor, dass bei der Implementierung eines Krebs-Früherkennungsprogramms (S. 398), bei der Datenerhebung, der Registrierung, der Datenverwaltung und -auswertung (S. 399) und beim Monitoring (S. 399) ein besonderes Augenmerk auf die Datenschutzvorschriften zu legen ist.

European Guidelines for quality assurance in colorectal cancer screening and diagnosis First Edition: Das Dokument fordert einen adäquaten Schutz für sämtliche im Rahmen des Programms bearbeiteten Personendaten sowie die Einhaltung der Europäischen Richtlinien zum Datenschutz und der nationalen Gesetze (S. 56). Der Zugriff auf die Melderegister bedarf einer gesetzlichen Grundlage (S. 42).

Anhang III: Grundsätze und Teilnehmerrechte

In der Schweiz ist der Schutz vor Missbrauch der persönlichen Daten in der Bundesverfassung verankert und wird dann in einer Vielzahl von Gesetzestexten und Empfehlungen spezifiziert. Dieser gewinnt insbesondere im Gesundheitsbereich an Bedeutung, denn *„je mehr elektronische Gesundheitsdienste etabliert werden, desto mehr Daten müssen kurzfristig und sicher dort verfügbar sein, wo sie gebraucht werden und effizient verarbeitet werden können. (…) Die Bearbeitung medizinischer Daten bedeutet einen Eingriff in die Grund- bzw. Persönlichkeitsrechte der betroffenen Personen (z.B. der Patientinnen und Patienten). Damit der Eingriff legitim ist, müssen rechtliche, organisatorische und technische Massnahmen getroffen werden.* Dieser Abschnitt ist in zwei Teile gegliedert. Die erste fasst die Prinzipien zusammen, die in der schweizerischen Gesetzgebung festgelegt sind oder sich daraus ableiten. Der zweite Abschnitt fasst die wichtigsten Rechte der betroffenen Personen zusammen.

Grundsätze

Grundsatz der Rechtmässigkeit der Erhebung (Art. 4 Abs. 1 DSG): Personendaten dürfen nur rechtmässig bearbeitet werden, das heisst, die Bearbeitung muss auf einer gesetzlichen Grundlage beruhen oder ausdrücklich von der betroffenen Person genehmigt worden sein. Ausserdem dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSG): Die Bearbeitung der Personendaten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein. Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Es dürfen nur Personendaten beschafft werden, die sowohl nötig als auch geeignet sind, um einen bestimmten Zweck zu erreichen. Der Grundsatz der Verhältnismässigkeit ist insbesondere für die Auswahl der erfassten Variablen bei der Sammlung der Daten zu berücksichtigen.

Selbst die Einwilligung der betroffenen Person rechtfertigt nicht eine Bearbeitung, die nicht im Einklang mit dem Grundsatz der Verhältnismässigkeit steht, da jede Bearbeitung von Personendaten verhältnismässig sein muss (die Bearbeitung von Personendaten steht nicht im Einklang mit dem Grundsatz der Verhältnismässigkeit, wenn das Verhältnis zwischen dem verfolgten Ziel und den eingesetzten Mitteln nicht angemessen ist).

Grundsatz der Zweckmässigkeit (Art. 4 Abs. 3 DSG): Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

Grundsatz der Richtigkeit (Art. 5 Abs. 1 DSG): Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.

Teilnehmerrechte

Auskunftsrecht: Das DSG gewährt jeder Person das Recht zu erfahren, ob und wenn ja, welche Daten über sie verarbeitet werden. Auf diese Weise ist die Person in der Lage, eine

gewisse Kontrolle über ihr Recht auf Privatsphäre und informationelle Selbstbestimmung auszuüben. Ihr Antrag braucht nicht begründet zu werden. Sie ist an den Inhaber der Datensammlung adressiert. Dies kann per Post, elektronisch oder persönlich erfolgen, sofern der Verwalter der Datensammlung die Identität der Person korrekt überprüfen kann. Der Verwalter muss grundsätzlich innerhalb von 30 Tagen antworten und die erforderlichen Daten kostenlos zur Verfügung stellen. In Ausnahmefällen, wenn der Inhaber der Datensammlung die Herausgabe der Daten verweigert, muss er seine Entscheidung begründen.

https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/das-auskunftsrecht.html

Recht auf Widerruf der Einwilligung: Jede Person, die ihre Zustimmung zur Verarbeitung ihrer Daten erteilt hat, kann ihre Zustimmung zur Verarbeitung widerrufen. Ein solcher Widerruf kann jederzeit mitgeteilt werden. Er kann schriftlich oder mündlich erfolgen. Der für die Verwalter der Datensammlung muss sicherstellen, dass der Widerruf von der Person stammt, deren Daten verarbeitet werden. Er muss überprüfen, ob die Person wirklich ihren freien und informierten Willen ausdrückt. Der Widerruf der Einwilligung bedeutet, dass sich der Verwalter der Datensammlung von nun an nicht mehr auf die Einwilligung als Grund für die Rechtmässigkeit der Verarbeitung berufen kann. Die vor dem Widerruf durchgeführten Verarbeitungen bleiben im Rahmen des Gesetzes. Beabsichtigt der Verwalter die Daten nach dem Widerruf weiter zu verarbeiten (einschliesslich ihrer Speicherung), muss er sich auf eine andere Begründung berufen können (z. B. eine Rechtsgrundlage, ein übergeordnetes privates Interesse).

Recht auf Berichtigung unrichtiger Daten: Jede Person, deren personenbezogene Daten verarbeitet werden, kann verlangen, dass "ihre" falschen Daten korrigiert werden. Dieses Recht gilt auch für Daten, die als unvollständig gelten. Die betreffende Person übermittelt ihren Antrag an den Inhaber der Datensammlung. Wenn die Daten ungenau sind, muss er sie korrigieren. Wenn die Daten unvollständig sind und daher irreführend sein können, ist der Inhaber der Datensammlung verpflichtet, sie zu vervollständigen. Die Berichtigung oder Ergänzung muss für die betroffene Person grundsätzlich innerhalb von 30 Tagen kostenlos erfolgen. Auch hier muss die Identität der Person, die die Korrektur beantragt, ordnungsgemäss überprüft werden.

Anhang IV: Vorlagen für Teilnehmer

Informationsbroschüre und Flyer:

Brustkrebs: https://www.swisscancerscreening.ch/krebs-frueherkennung/brust/broschueren-und-flyer

Darmkrebs: https://www.swisscancerscreening.ch/?id=278

Anhang V: Nationales Monitoring

Teilnahmeindikatoren: Abdeckungsrate durch Einladungen [%], Teilnahmerate innerhalb von 12 Monaten [%], Teilnahmerate nach Ersteinladung [%], Teilnahmerate für wiederholte Einladung [%].

Leistungsindikatoren: Karzinomentdeckungsrate [1/1000], Abklärungsrate [1/1000], Falsch-positiv-Rate [1/1000], Positive predictive value [%].

Prognoseindikatoren: Rate der invasiven Karzinome [%], DCIS-Rate [%], Karzinom im Frühstadium, Fortgeschrittenes Karzinom [%].

Anhang VI: Inhaltsverzeichnis für programmeigene Datenschutzrichtlinie

1. Zusammenfassung
2. Kantonale Rechtsgrundlagen, die die Verarbeitung personenbezogener Daten erlauben
3. Workflow des Programmes
4. Identifizierung der Schritte mit einem Sicherheitsverletzungsrisiko / kumulierten Datenschutzrisiko (insbesondere, wenn die Daten über andere Kanäle als MC-SIS gesendet werden).
5. SOP-1-4, sowie die Update-Richtlinie
6. Richtlinien Zugang zu den Räumlichkeiten, Dokumentenmanagement (einschliesslich der von den Teilnehmern ausgefüllten Papierformulare), Druckerverwaltung und Zugang der Besucher.
7. Sensibilisierungsmassnahmen für die Mitarbeiter
8. Datenaustauschrichtlinien, mit dem Krebsregister oder über andere Kanäle als MC-SIS (z.B. USB-Stick, etc.).
9. Aufbewahrungsdauer und Löschverfahren der Daten
10. Anmeldung der Datensammlung beim Datenschutz- und Öffentlichkeitsbeauftragten

Anhänge

11. Verträge mit Dritten (Institute, externe Dienstleister)
12. Muster-Einladungsschreiben
13. Muster-Einverständniserklärung
14. Informationsbroschüre

Anhang VII: Minimalset von Standard Operating Procedures (SOPs) und Anhängen zum Thema Datenschutz:

SOP-1: Programmverfahren Verfahren zur systematischen Erfassung von Zusatzdaten

SOP-2: Programmverfahren Verfahren zur Verifizierung der Datenerhebung

SOP-3: Beschreibt den Prozess zur Aktualisierung und Kontrolle der Zugriffsrechte-Matrix

Zugriffsrechte-Matrix Listet Zugriffsrechte auf das MC-SIS-System und die Räumlichkeiten mit einer nominalen Liste der Mitarbeiter und ihrer Aufgaben auf.

SOP-4: Verfahren zur Regelung der Zugangsanfragen von betroffenen Personen.

Anhang VIII: Abkürzungsverzeichnis

ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (SR 830.1)
BAG	Bundesamt für Gesundheit
BFS	Bundesamt für Statistik
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
CDI	Conseils et développements informatiques SA
DSG	Bundesgesetz über den Datenschutz (RS 235.1)
DSGVO	Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch die meisten Datenverarbeiter EU-weit vereinheitlicht werden. Diese Verordnung ist auf die Krebsfrüherkennungsprogramme der Schweiz nicht anwendbar.
DS-Richtlinie	Datenschutzrichtline: Dokument welches die Datenschutzerklärung des Programmes dokumentiert.
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
FIT-Test	Fecal immunochemical test
FMH	Verband der Schweizer Ärztinnen und Ärzte
HFG	Bundesgesetz über die Forschung am Menschen (RS 810.30)
Institut	Institut für Radiologie oder Gastroenterologie, das mit den Programmen zusammenarbeitet
MC-SIS	Multi-Cancer Screening Information-System
KLV	Krankenpflege-Leistungsverordnung (RS 832.112.31)
KRG	Bundesgesetz über die Registrierung von Krebserkrankungen (RS 818.33)
KRV	Verordnung über die Registrierung von Krebserkrankungen (RS 818.331)
KVG	Bundesgesetz über die Krankenversicherung (RS 832.10)
SAQM	Schweizerische Akademie für Qualität in der Medizin
SCS	Swiss Cancer Screening
SOP	Standard Operating Procedures