Vorstand

22. Januar 2021

CD-2021-02

Allgemeine Informationssicherheits- und Datenschutzpolitik

1. Einleitung

Informationssicherheit und Datenschutz gehören zu den Prioritäten des Verbands CARA bei der Erfüllung seiner Aufgaben im Gesundheitswesen. Der Direktionsausschuss widmet diesen Themen besondere Aufmerksamkeit und achtet darauf, dass alle Beteiligten von CARA diese Grundsätze im Bereich der Data Governance einhalten.

Im vorliegenden Dokument wird die allgemeine Politik des Verbands CARA im Bereich Informationssicherheit und Datenschutz (ISDS) beschrieben. Es werden detailliert die Grundsätze aufgezeigt, nach denen sich die Massnahmen von CARA zur Gewährleistung der Informationssicherheit und des Datenschutzes richten und die den Beteiligten in ihren Tätigkeiten als Richtlinie gelten.

2. Zusammenfassung

Der Verband CARA stellt der Bevölkerung seiner Mitgliedskantone und den Gesundheitsfachpersonen eine eHealth-Plattform zur Verfügung, wodurch er den Austausch von Gesundheitsinformationen vereinfacht und die Sicherheit der Gesundheitsversorgung erhöht. Für CARA dienen die Informationssicherheit und der Datenschutz (ISDS) in diesem Zusammenhang der Versorgungssicherheit.

Anwendungsbereich
Die ISDS-Massnahmen erstrecken sich über alle Bereiche von CARA, namentlich:

- Verbandsorgane,
- eHealth-Plattform, einschliesslich elektronisches Patientendossier und Zusatzdienste (Services),
- angeschlossene Institutionen,
- Patientinnen und Patienten.

Verantwortung
CARA übernimmt die Verantwortung für die Informationssicherheit und den Datenschutz gegenüber allen Beteiligten, insbesondere gegenüber:

- den Nutzerinnen und Nutzern der eHealth-Plattform,
- den Mitgliedskantonen und deren Behörden,
- den öffentlichen und privaten Partnern,
- dem Bund und den Regulierungsinstanzen.

Grundsätze
CARA hält die Grundsätze der Informationssicherheit, insbesondere die Grundsätze von Vertraulichkeit, Integrität und Verfügbarkeit der Daten, jederzeit und unter allen Umständen ein und wendet sie an.

Verpflichtung
Zur Umsetzung der eingeführten ISDS-Massnahmen verpflichtet sich CARA dazu:

- sich mit den nötigen Kompetenzen und Ressourcen zur Umsetzung und zum Monitoring der Massnahmen auszustatten;
- die Massnahmen fortwährend zu überwachen und zu verbessern;
- sicherzustellen, dass die Massnahmen dem aktuellen Gesetzesrahmen entsprechen, insbesondere dem Bundesgesetz über das elektronische Patientendossier und dem Bundesgesetz über den Datenschutz;
- die Massnahmen während der ganzen Zeit bei allen Tätigkeiten, Produkten oder Dienstleistungen von CARA anzuwenden;
- einen proaktiven und reaktiven Sicherheitsansatz zu entwickeln;
- Transparenz über den Stand der Datensicherheit und des Datenschutzes zu gewährleisten.

3. Zielsetzungen

Der Verband CARA schützt seine Datenbestände vor jeglicher interner oder externer, mutwilliger oder unbeabsichtigter Bedrohung. Dabei geht es namentlich um die Daten, die auf elektronischen Datenträgern gespeichert sind, die über Kommunikationsnetzwerke übermittelt, auf Papier ausgedruckt oder in Gesprächen verwendet oder telefonisch besprochen werden.

Der Verband CARA verfolgt in Bezug auf den Schutz seiner Datenbestände das Ziel, zu gewährleisten, dass seine hauptsächlichen Arbeitsgänge und Tätigkeiten in Verbindung mit der Bereitstellung einer eHealth-Plattform, einschliesslich des elektronischen Patientendossiers (EPD) und der Zusatzdienste, konstant und mit möglichst wenigen Störungen funktionieren.

Hierzu setzt CARA über sein Managementsystem für Informationssicherheit und Datenschutz (ISDS-Managementsystem; ISMS – Information Security Management System) die allgemeine Informationssicherheits- und Datenschutzpolitik um.

4. Allgemeine Politik

Die Datenbestände und die IT-Hardware, die den Nutzerinnen und Nutzern, Mitarbeitenden und Dritten ermöglichen, zufriedenstellend zu arbeiten, unterstehen einer gesicherten Kontrolle. Damit wird gewährleistet, dass sie vor vorsätzlichem Schaden oder Verlust, unerlaubter Manipulation, unbeabsichtigten Ausfällen oder unbefugter Offenlegung, sowohl inner- als auch ausserhalb von CARA, geschützt sind.

CARA legt für die Nutzung der IT-Ressourcen Verhaltensregeln fest, die den heutigen Normen und der heutigen Technologie entsprechen.

CARA schützt die Datenbestände der Nutzerinnen, Nutzer und Dritter, die dem Verband vertraulich anvertraut wurden, und behandelt sie gleich wie jedes andere Geheimnis gemäss den anwendbaren Verträgen und Vereinbarungen. Der Verband CARA behandelt jede Information, die über seine IT-Systeme läuft oder darauf gespeichert ist und die nicht explizit als Eigentum eines der Beteiligten identifiziert wurde, gleich wie seine eigenen Datenbestände.

CARA verbietet den unerlaubten Zugriff, die unzulässige Offenlegung, die unerlaubte Kopie und Änderung, den Missbrauch, die unzulässige Vernichtung, den Verlust, die falsche Nutzung oder den Diebstahl dieser Informationen.

Die allgemeine Informationssicherheits- und Datenschutzpolitik stützt sich auf drei Säulen:

Allgemeine Strategie
CARA trägt zur Qualität, Kontinuität und Koordination der Gesundheitsversorgung bei, indem die Interprofessionalität gefördert und der Informationsaustausch erleichtert wird. Hierzu stellt CARA den Gesundheitsfachpersonen sowie den Bürgerinnen und Bürgern eine gemeinsame, benutzerfreundliche, verlässliche und gesicherte eHealth-Plattform zur Verfügung. Die Informationssicherheit dient der Versorgungssicherheit.

Übereinstimmung mit den gesetzlichen und reglementarischen Grundsätzen
Die gesetzlichen und reglementarischen Grundsätze werden im Einklang mit den eidgenössischen und kantonalen gesetzlichen Anforderungen, namentlich dem Bundesgesetz über das elektronische Patientendossier (EPDG) und dem Bundesgesetz über den Datenschutz (DSG), befolgt.

Risiko- und Bedrohungsumfeld
Das Risiko- und Bedrohungsumfeld wird konstant überwacht. Es wird im Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) beschrieben.

5. Grundsätze

CARAs Tätigkeit zur Umsetzung der ISDS-Massnahmen richtet sich nach den folgenden Grundsätzen:

Verfügbarkeit
Die Informationen werden den Mitarbeitenden und Dritten mit einem Minimum an Störungen zur Verfügung gestellt, um zu gewährleisten, dass die Informationen und lebenswichtigen Dienstleistungen im Zusammenhang mit dem Betrieb der eHealth-Plattform für die Nutzerinnen und Nutzer verfügbar sind. Die Plattform CARA stellt ein Sekundärsystem dar. Die Grundsätze in den Bereichen Informationssicherheit und Verfügbarkeit der Primärsysteme fallen nicht unter die Verantwortung von CARA. Parallel und unabhängig von der eHealth-Plattform werden die Informationen der Mitarbeitenden von CARA in ihren jeweiligen Funktionen ebenfalls mit einem Minimum an Störungen zur Verfügung gestellt. Die Informationen und Informationssysteme werden bei Bedarf durch die grundlegenden und unterstützenden Arbeitsgänge und Tätigkeiten von CARA zur Verfügung gestellt.

Integrität
CARA achtet darauf, dass alle Informationen, die der Verband sammelt, verwaltet oder herausgibt, ihre Integrität behalten. Die Integrität und Vollständigkeit der Datenbestände werden erhalten, indem diese vor jeglicher unerlaubter Änderung geschützt werden.

Vertraulichkeit
Um zu gewährleisten, dass besonders schützenswerte Daten vor etwaiger unerlaubter Offenlegung geschützt werden, wird die Vertraulichkeit sämtlicher Informationen gewahrt. Im Rahmen des Managements der eHealth-Plattform und der Informationssysteme von CARA wird eine geeignete Zugriffskontrolle umgesetzt. Die darauf befindlichen Informationen werden vor jeglichem unerlaubten Zugriff geschützt.

Kontinuität
Es wird ein Plan für das betriebliche Kontinuitätsmanagement (Business Continuity) ausgearbeitet, um Unterbrechungen der operationellen Aktivitäten zu verhindern und die kritischen Abläufe vor den Auswirkungen von Störungen, Ausfällen oder Grossereignissen zu schützen. Der Business Continuity Plan wird periodisch getestet.

Rückverfolgbarkeit
CARA erfasst und speichert die durchgeführten Arbeitsgänge, um den Ablauf der Ereignisse bei Bedarf später wiedergeben zu können.

Ausbildung
Es werden Programme zur Sensibilisierung für die Informationssicherheit ausgearbeitet und den Mitarbeitenden und Dritten, die auf die Informationssysteme von CARA zugreifen, zur Verfügung gestellt. Alle Mitarbeitenden, die über besondere Zugriffsrechte für Personendaten oder besonders schützenswerte Daten verfügen, werden in Bezug auf die sicherheitsbezogenen Herausforderungen und anzuwendenden Praktiken geschult.
Auch den angeschlossenen Institutionen werden Ausbildungen zur Informationssicherheit und zum Datenschutz angeboten.

Risk Management
Im Rahmen einer kontinuierlichen Beobachtung des Umfelds analysiert CARA Risiken und Bedrohungen. Da sich die Risiken und Bedrohungen im IT-Bereich fortwährend entwickeln und immer gravierendere Folgen haben, entwickeln sich auch die Massnahmen, die Kontrollen und die Strategie des Risiko- und Bedrohungsmanagements. Das Monitoring dieser Änderungen und die Entwicklung der Massnahmen werden erfasst und dokumentiert.

Kontinuierliche Verbesserung
Das ISDS-Managementsystem entwickelt sich fortlaufend weiter und wird kontinuierlich verbessert. Der Direktionsausschuss führt einmal jährlich eine Revision der ISDS-Massnahmen durch und stellt sicher,

dass seine allgemeine Politik eingehalten wird und dass die ISDS-Massnahmen geeignet, wirksam und effizient sind. Seine Evaluation läuft auf korrigierende Massnahmen hinaus.

Transparenz
Die vorliegende allgemeine Politik sowie die entsprechenden Richtlinien und Verfahren werden den verschiedenen betroffenen Beteiligten zur Verfügung gestellt.

Meldung und Sanktionen
Alle tatsächlichen oder mutmasslichen Verletzungen der Informationssicherheit werden dem Sicherheitsverantwortlichen von CARA gemeldet. CARA verfügt über einen Prozess für das Zwischenfallmanagement und über einen vollständigen und regelmässig getesteten Reaktionsplan bei Zwischenfällen. Bei Verletzungen der und Verstössen gegen die Sicherheitspolitik und -prozesse ergreift CARA gemäss einem formalisierten Verfahren Disziplinarmassnahmen und spricht Sanktionen aus.

6. Verantwortlichkeiten

Direktionsausschuss
Der Direktionsausschuss hat folgende Verantwortlichkeiten:

- Er nimmt die allgemeine Informationssicherheits- und Datenschutzpolitik an;
- Er führt hinsichtlich einer kontinuierlichen Verbesserung eine jährliche Revision der ISDS-Massnahmen durch;
- Er weist die nötigen organisatorischen und technischen Ressourcen für die Umsetzung, das Management und das Monitoring von effizienten ISDS-Massnahmen, die den Grundsätzen aus der allgemeinen Politik entsprechen, zu;
- Er schliesst mit Leistungserbringern unter Berücksichtigung der ISDS-Anforderungen Verträge ab.

Generalsekretariat
Das Generalsekretariat hat folgende Verantwortlichkeiten:

- Es setzt die allgemeine Politik und die ISDS-Massnahmen um;
- Es legt die Regeln und Praktiken in Bezug auf die Informationssicherheit und den Datenschutz fest;
- Es schützt die Ressourcen des IT-Systems, die es kontrolliert und verwaltet, wie Informatikmaterial, Anwendungs- und Systemsoftwares, Daten, Dokumentation, sowie die Mitarbeitenden;
- Es stellt sicher, dass die Mitarbeitenden die vorliegende allgemeine Politik befolgen und die entsprechenden Regeln und Praktiken einhalten;
- Es stellt sicher, dass die Mitarbeitenden ihre Rollen und Verantwortlichkeiten im Bereich Informationssicherheit und Datenschutz sowie im entsprechenden Zwischenfallmanagement verstehen;
- Es kontrolliert, dass mit den ISDS-Massnahmen die gesteckten und erwarteten Ziele in den Bereichen Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der von CARA erhaltenen, aufbewahrten und bearbeiteten Daten erreicht werden können;
- Es wendet einen Risikomanagement-Prozess an und bietet damit allen Beteiligten die Sicherheit, dass diese Risiken bekannt sind und sachgemäss gehandhabt werden;
- Es überwacht, ob die Leistungserbringer die ISDS-Anforderungen einhalten;
- Es gibt regelmässig Sicherheitsaudits in Auftrag;
- Es sorgt dafür, dass seine Räumlichkeiten sicher sind.

Mitarbeitende
Die Mitarbeitenden haben folgende Verantwortlichkeiten:

- Sie stimmen der vorliegenden allgemeinen Politik zu;
- Sie halten sich an die Regeln und Praktiken, die sich daraus ergeben, und wenden diese an;
- Sie melden jeden Zwischenfall in Bezug auf die Informationssicherheit und den Datenschutz.

Angeschlossene Institutionen
Die angeschlossenen Institutionen haben folgende Verantwortlichkeiten:

- Sie bestätigen formell, dass sie die allgemeine Politik von CARA gelesen und verstanden haben und stimmen den ISDS-Massnahmen zu;
- Sie setzen die von CARA erlassenen Anforderungen an die Informationssicherheit und den Datenschutz um;
- Sie überwachen, dass ihre Mitarbeitenden der allgemeinen Politik von CARA zustimmen;
- Sie überprüfen periodisch, dass sie die allgemeine Informationssicherheits- und Datenschutzpolitik von CARA einhalten.