Im Auftrag des BAG

Digitale Gesundheitsanwendungen: Cybersicherheit und Datenschutzvorgaben

Auftraggeber	Bundesamt für Gesundheit (BAG), Direktionsbereich Kranken- und Unfallversicherung (KUV)
Autoren	Prof. Dr. Rudolf Blankart, Universität Bern (KPM/sitem) Prof. Dr. Tobias Eule, Universität Bern (Institut für öffentliches Recht) Benjamin Wyss, Universität Bern (KPM/sitem)
Mitwirkung	
Datum	26.06.2024
Version	4.b.
Kontakt	Universität Bern Kompetenzzentrum für Public Management (KPM) Swiss Institute for Translational and Entrepreneurial Medicine (sitem-insel) Freiburgstrasse 3 3010 Bern Tel. +41 31 666 44 30 www.kpm.unibe.ch www.sitem-insel.ch

Zusammenfassung (Management Summary)

Die verstärkte Nutzung digitaler Technologien im Gesundheitswesen, die Produktion und Verknüpfung von immer mehr schützenswerten und besonders schützenswerten Daten sowie die Entstehung neuer Geschäftsmodelle rücken zwei Themen in den Fokus: Cybersicherheit und Datenschutz. Bei Cybersicherheit geht es um Massnahmen, die die Integrität, Vertraulichkeit und die Verfügbarkeit der Daten stärken sollen. Dabei steht insbesondere die Verbesserung des Schutzes von Informationssystemen vor Angriffen von innen und aussen im Fokus. Bei Datenschutz geht es um den Schutz der individuellen Privatsphäre vor missbräuchlicher Datenverarbeitung sowie die Einhaltung des Rechts auf informationelle Selbstbestimmung, des Persönlichkeitsrechts bei der Datenverarbeitung, beziehungsweise um den Schutz der personenbezogenen Daten. Ziel dieses Berichtes ist es eine Reihe vordefinierter Fragestellungen des Bundesamtes für Gesundheit zu klären und bei der Schaffung eines Verständnisses zu unterstützen, um Herausforderungen im Bereich des Datenschutzes und der Cybersicherheit bei digitalen Gesundheitsanwendungen (dGA) speziell im Bereich der Kostenübernahme durch die obligatorische Krankenpflegeversicherung (OKP) zu verstehen. Dies insbesondere um gegebenenfalls notwendige regulatorische Änderungen anzustossen oder zu ergreifen.

Das dreistufige Vorgehen zur Erstellung dieses Berichtes sah eine Konzeptionsphase, eine Interview- und Recherchephase und eine Analysephase vor. Mit einer ersten Literaturrecherche wurde das Grundverständnis der aktuellen Situation geschaffen. In der zweiten Phase wurden Schlüsseldokumente weiter vertieft und kritische Aspekte und Unklarheiten mit semi-strukturierten Interviews abgedeckt. In der abschliessenden Analysephase wurden Perspektiven der Verwaltung, der Verbände der Leistungszahler, Leistungserbringer, Patienten und Hersteller einbezogen und entsprechende Handlungsempfehlungen formuliert.

Der Fachbericht verortet die Rolle des Bundesamts für Gesundheit (BAG) im sich ständig verändernden Feld der Digitalisierung von Gesundheit. Der Bericht beschreibt, welche aktuellen rechtlichen Vorgaben dGAs sicherer machen und die Privatsphäre Einzelner besser schützen sollen. Er weist ferner aus, inwieweit auch Stellen der Verwaltung die Themen Cybersicherheit und Datenschutz künftig mehr in den Blick nehmen können.

Basierend auf den durchgeführten Analysen, den Einblicken in den Interviews und der Beantwortung der spezifischen Fragen wurden Handlungsempfehlungen mit kurz- und langfristigem Horizont für die Verwaltung und weitere Stakeholdergruppen entwickelt.

Kurzfristige Handlungsempfehlungen (unter 3 Jahren):

- Bei den Stakeholdern bestehen Unsicherheiten bezüglich Einordnung, Vergütung, Verantwortlichkeiten und weiteren Aspekten. Die meisten Stakeholder zeigten sich jedoch offen und inte-

ressiert an einem Austausch mitzuwirken, der zum Beispiel im Rahmen von moderierten Stakeholderworkshops des BAGs durchgeführt werden könnte. Die Ausgestaltung eines solchen Workshops und auch der spezifische Beitrag der Stakeholder müsste im Weiteren noch definiert werden. Teile dieses Berichtes könnten für die Vorbereitung eine Grundlage bilden.

- Basierend auf den Analysen der Autoren besteht kein Änderungsbedarf in Bezug auf Datenschutz und Cybersicherheit auf Gesetzes- und Verordnungsebene des Heilmittelgesetzes (HMG, SR 810.30) sowie des Bundesgesetzes über die Krankenversicherung (KVG, SR 832.10) mit Verordnung über die Krankenversicherung (KVV, SR 832.102) und Krankenpflege-Leistungsverordnung (KLV, 832.112.31). Bei allen allfälligen Anpassungen ist zu beachten, dass Schweiz-spezifische Änderungen, zusätzliche Anforderungen aus Sicht der Hersteller darstellen und daher negative Implikationen auf die Versorgungssicherheit als auch auf den Zugang zu neuartigen Technologien haben könnten.
- Das Grundlagendokument *Operationalisierung der Kriterien «Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit*» sollte bezüglich dGAs spezifiziert und um die Themen Cybersicherheit und Datenschutz ergänzt werden. Im Dokument müsste eine methodische Ergänzung vorgenommen werden, die darlegt, wie diese Elemente in den Prüfprozess einbezogen werden.
- Die bestehenden Antragsprozesse und -dokumente sollten präzisiert werden, dass diese dGAs besser gerecht werden. Zum Beispiel könnte eine Erklärung des Herstellers über die Einhaltung der Datenschutzanforderungen vom BAG im Rahmen der Entscheidung über die Vergütung eingefordert werden sowie in Abstimmung mit dem Bundesamt für Cybersicherheit (BACS) spezifische Fragen zur Cybersicherheit und mit dem Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) spezifische Fragen zum Datenschutz entwickelt werden. Vorab sollte im BAG jedoch im Grundsatz klären, ob die Verantwortung für Cybersicherheit und Datenschutz beim BAG liegt. Neben dem vom BAG publizierten Dokument zur Operationalisierung der Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit (WZW) Kriterien gibt es keine explizite gesetzliche Verpflichtung für diese Aufgaben.

Handlungsempfehlungen mit einem langfristigen Zeithorizont (über 3 Jahren):

- Um der Komplexität der Themen Cybersicherheit und Datenschutz gerecht zu werden, sollte ein kontinuierlicher Austausch zwischen der Bundesverwaltung, Kantonen und den verschiedenen Stakeholdern etabliert werden. Möglich wäre auch die Schaffung eines neuen gesundheitssektorspezifischen Zentrums für Informationsaustausch und Analyse (ähnlich dem Information Sharing and Analysis Center [ISAC] der EU) oder auch die Integration in bestehende Strukturen, zum Beispiel eHealth Suisse. Dabei ist darauf zu achten, dass bestehende Gefässe und Initiativen genutzt werden und keine Doppelstrukturen aufgebaut werden.

- Die Kantone könnten eine Harmonisierung der Anforderungen für die Zulassung und Überwachung von nach kantonalem Recht zugelassenen Abgabestellen für Mittel und Gegenstände anstreben, um schweizweit eine einheitliche Struktur- und Prozessqualität zu garantieren. Dies ist für dGAs umso wichtiger, da kantonale Abgabestellen für dGAs ohne Hürden schweizweit agieren können.
- Die Verbände der Leistungserbringer, Versicherer und Hersteller sollten Instrumente entwickeln, mit denen sie ihre Mitglieder über die gesetzlichen Vorgaben im Bereich Cybersicherheit und Datenschutz zielgruppengerecht informieren können.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis & Glossar

Begriff	Erläuterung
AL	Die Analysenliste (AL) bildet den Anhang 3 der Krankenpflege-Leistungsverordnung (KLV). Die AL enthält diejenigen Analysen, die von medizinischen Laboratorien nach Art. 54 der Verordnung über die Krankenversicherung (KVV) erbracht werden und von der obligatorischen Krankenpflegeversicherung (OKP) übernommen werden (Bundesamt für Gesundheit BAG, o. J.-a).
BACS	Bundesamt für Cybersicherheit (ehemals NCSC).
BAG	Bundesamt für Gesundheit.
BAKOM	Bundesamt für Kommunikation.
Besonders schützenswerte Personendaten	Nach Art. 5 lit. c. des Bundesgesetzes über den Datenschutz (DSG) sind besonders schützenswerte Personendaten: ▪ Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, ▪ Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, ▪ genetische Daten, ▪ biometrische Daten, die eine natürliche Person eindeutig identifizieren, ▪ Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen, ▪ Daten über Massnahmen der sozialen Hilfe.
BfArM	Bundesamt für Arzneimittel und Medizinprodukte (Deutschland).
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft (SR 101).
CH-REP	Schweizer Bevollmächtigter.
Cyberangriff	Cybervorfall, der absichtlich ausgelöst wurde (Nationales Zentrum für Cybersicherheit (NCSC), 2023).
Cyberkriminalität	Cyberkriminalität umfasst die Gesamtheit aller strafbaren Handlungen und Unterlassungen im Cyberraum. Unterschieden wird zwischen «Cyberkriminalität» und «digitalisierter Kriminalität». «Cyberkriminalität» bezeichnet Straftaten die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten und technische Ermittlungsarbeit auf Seiten der Strafverfolgungsbehörden erfordern. «Digitalisierte Kriminalität» bezeichnet Straftaten, die bisher überwiegend in der analogen Welt begangen worden sind. Aufgrund der zunehmenden Digitalisierung werden diese klassischen Delikte vermehrt mit Hilfe von Informationstechnik verübt (Nationales Zentrum für Cybersicherheit (NCSC), 2023).
Cybersicherheit (Englisch Cybersecurity)	Anzustrebender Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert (Der Schweizerische Bundesrat, 2021).
Cybervorfall	Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist (Nationales Zentrum für Cybersicherheit (NCSC), 2023).
CyRV	Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (SR 120.73).
Datenschutz	Der Schutz vor missbräuchlicher Datenverarbeitung sowie die Einhaltung des Rechts auf informationelle Selbstbestimmung, des Persönlichkeitsrechts bei der Datenverarbeitung und der Privatsphäre, beziehungsweise um den Schutz der personenbezogenen Daten.
dGA	Unter dGAs werden gemäss dem BAG (2022) Produkte verstanden, deren medizinischer Zweck durch die Hauptfunktion der digitalen Technologien erzielt wird. Dies umfasst Anwendungen im Bereich der Telemedizin, dem Telemonitoring sowie Apps und mobile Geräte. Digitale Applikationen, die lediglich dazu dienen, die Tätigkeiten von Gesundheitsfachpersonen zu unterstützen, z.B. Auslesen und Analysieren von Daten oder Steuern eines Gerätes, werden nicht dem Begriff der dGAs zugeordnet.

Begriff	Erläuterung
DiGA	Digitale Gesundheitsanwendung. Im Schweizer Recht findet sich bis dato keine Definition des Begriffs «digitale Gesundheitsanwendung». Der Begriff stammt aus Deutschland und wurde dort mit Erlass des Digitale-Versorgung-Gesetzes («DVG») vom 9. Dezember 2019 eingeführt. Nach dem DiGA-Leitfaden des Deutschen Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) ist eine DiGA ein «Medizinprodukt der Risikoklasse I oder IIa [nach Medical Device Regulation MDR) [...]», welches eine Reihe von spezifischen Eigenschaften aufweist.
DiGAV	Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV).
DSA	Datenschutzaufsichtsstelle.
DSG	Bundesgesetz über den Datenschutz (SR 235.1).
DSGVO	Datenschutz-Grundverordnung (Englisch: General Data Protection Regulation).
DSV	Verordnung über den Datenschutz (SR 235.11).
DTS	Digitale Transformation und Steuerung (Abteilung des BAGs).
EAMGK	Eidgenössische Kommission für Analysen, Mittel und Gegenstände (Schweizerische Eidgenossenschaft., o. J.).
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter.
EDSA	Europäischer Datenschutzausschuss. Der EDSA ist ein unabhängiges Gremium, das dafür sorgt, dass die einschlägigen EU-Vorschriften – insbesondere die Datenschutz-Grundverordnung (DSGVO) und die Richtlinie zum Datenschutz bei der Strafverfolgung – in allen Ländern, in denen sie anwendbar sind, einheitlich angewendet werden.
EMRK	Europäische Menschenrechtskonvention.
EU	Europäische Union.
EU IVDR	Verordnung (EU) 2017/746 über In-vitro-Diagnostika.
EU MDR	Die Medizinprodukteverordnung (Medical Device Regulation) wurde vom Europäischen Parlament im Jahr 2017 verabschiedet und regelt die Vorgaben, die Hersteller und andere Wirtschaftsakteure einhalten müssen. Sie ersetzt die Medizinprodukterichtlinie (93/42/EWG) sowie die Richtlinie über aktive implantierbare medizinische Geräte (90/385/EWG) (TÜV Süd, o. J.).
fedpol	Bundesamt für Polizei.
FMH	Verbindung der Schweizer Ärztinnen und Ärzte (Berufsverband).
GPSR	Die Verordnung über die allgemeine Produktsicherheit (GPSR) ist ein neues Schlüsselinstrument im EU-Rechtsrahmen für die Produktsicherheit, dass ab dem 13. Dezember 2024 die derzeitige Richtlinie über die allgemeine Produktsicherheit und die Richtlinie über Lebensmittelimitate ersetzen wird (European Commission, o. J.).
GSPR	Grundlegende Sicherheits- und Leistungsanforderungen definiert im Anhang I der EU MDR.
HFG	Humanforschungsgesetz: Bundesgesetz über die Forschung am Menschen (SR 810.30).
HMG	Heilmittelgesetz: Bundesgesetz über Heilmittel und Medizinprodukte (SR 812.21).
IoT	Internet der Dinge (Englisch: Internet of Things).
ISAC	Information Sharing and Analysis Centers.
ISG	Bundesgesetz über die Informationssicherheit beim Bund (SR 128).
ISMS	Managementsystem für Informationssicherheit (Englisch: Information Security Management System).
IVD	In-vitro-Diagnostika sind Tests, bei denen anhand biologischer Proben der Gesundheitszustand einer Person bestimmt wird.
IvDV	Verordnung über In-vitro-Diagnostika (SR 812.219).

Begriff	Erläuterung
KBS	Bezeichnet eine Konformitätsbewertungsstelle. Eine von der Behörde für eine bestimmte Konformitätsbewertung zertifizierte KBS, zum Beispiel für die Prüfung der Voraussetzung für die Inverkehrbringung von Medizinprodukten, wird bezeichnete Stelle oder im englischen Notified Body genannt. Bezeichnete Stellen überprüfen bei Herstellern Medizinprodukte auf ihre Übereinstimmung mit den gesetzlichen Anforderungen. Bezeichnete Stellen führen dazu Konformitätsbewertungsverfahren für all diejenigen Produkte durch, die ausserhalb der niedrigsten Risikoeinstufung klassifiziert sind. Nach erfolgreich abgeschlossenen Verfahren werden den Herstellern die entsprechenden Konformitätsbescheinigungen ausgestellt, was diese ermächtigt, ihre Produkte konform in Verkehr zu bringen (Swissmedic - Schweizerisches Heilmittelinstitut, o. J.-a).
KI (Englisch AI)	Künstliche Intelligenz (englisch: Artificial Intelligence).
KlinV-Mep	Verordnung über klinische Versuche mit Medizinprodukten (SR 810.306).
KLV	Krankenpflege-Leistungsverordnung (SR 832.112.31).
KUV	Direktionsbereich Kranken- und Unfallversicherung des BAGs.
KVG	Bundesgesetz über die Krankenversicherung (SR 832.10).
KVV	Verordnung über die Krankenversicherung (SR 832.102).
Marktüberwachung	Unter Marktüberwachung wird die kontinuierliche Überwachung der Qualität, Sicherheit und Wirksamkeit von Arzneimitteln und Medizinprodukten nach der Marktzulassung durch die zuständige Behörde, in der Schweiz Swissmedic, verstanden.
MD-Kennzeichnung	Konformitätsbezeichnung analog zu CE-Kennzeichnung jedoch lediglich für den Schweizer Markt.
MDCG	Koordinierungsgruppe Medizinprodukte (Englisch Medical Device Coordination Group).
Medizinprodukt	Medizinprodukte sind Produkte mit medizinischer Zweckbestimmung, die vom Hersteller für die Anwendung beim Menschen bestimmt sind. Dazu gehören Implantate, Produkte zur Injektion, Infusion, Transfusion und Dialyse, humanmedizinische Instrumente, Software, Katheter, Herzschrittmacher, Dentalprodukte, Verbandsstoffe, Sehhilfen, Röntgengeräte, Kondome, ärztliche Instrumente, Labordiagnostika, Produkte zur Empfängnisregelung sowie In-vitro-Diagnostika (Bundesministerium für Gesundheit, 2022).
MepV	Medizinprodukteverordnung (SR 812.213): gesetzliche Bestimmungen für Medizinprodukte der Schweiz.
Mittel- und Gegenständeliste (MiGeL)	Die Mittel- und Gegenständeliste (MiGeL) bildet den Anhang 2 der KLV. Die MiGeL enthält die Mittel und Gegenstände, die von den Versicherten selbst oder einer nichtberuflich an der Untersuchung oder Behandlung mitwirkenden Person oder von Pflegeheimen, Organisationen der Krankenpflege und Hilfe zu Hause oder Pflegefachpersonen im Rahmen der Pflegeleistungen nach Art. 25*a* KVG angewendet werden und von der OKP übernommen werden (Bundesamt für Gesundheit BAG, o. J.-b).
NCS	Nationale Cyberstrategie der Schweiz.
NCSC [alt] neu BACS	Nationales Zentrum für Cybersicherheit: Kompetenzzentrum des Bundes für Cybersicherheit.
NIS-2	The Network and Information Security (NIS) Directive. Sie regelt die Cyber- und Informationssicherheit von Unternehmen und Institutionen. Bis Oktober 2024 müssen die EU-Mitgliedsstaaten diese in nationales Recht überführen.
o.J.	Ohne Jahr.
OKP	Die OKP bezeichnet die obligatorische Krankenpflegeversicherung – oft auch Kranken- oder Grundversicherung genannt.
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht).
Personendaten	Umfassen nach Art. 5 lit. a. des DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.
PrHG	Bundesgesetz über die Produktehaftpflicht (SR 221.112.944).

Begriff	Erläuterung
Profiling	Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (DSGVO, Art. 4 Ziff. 4).
SAS	Die Schweizerische Akkreditierungsstelle (SAS) begutachtet und akkreditiert Konformitätsbewertungsstellen (KBS) aufgrund entsprechender internationaler Normen.
SBK	Schweizer Berufsverband für Pflegefachpersonal.
SL	Die Spezialitätenliste (SL) ist eine Positivliste von zugelassenen und OKP-leistungspflichtigen Arzneimitteln.
SPO	Schweizerische Stiftung SPO Patientenorganisation.
SQS	Schweizerische Vereinigung für Qualitäts- und Management-Systeme.
SVDI	Schweizerischer Verband der Diagnostikindustrie.
Swissmedic	Swissmedic ist die schweizerische Zulassungs- und Kontrollbehörde für Heilmittel. Basis für die Tätigkeit der Swissmedic ist das Heilmittelrecht (Swissmedic - Schweizerisches Heilmittelinstitut, o. J.-b).
VDSZ	Verordnung über Datenschutzzertifizierungen (SR 235.13).
Verwaltung/Behörden	Unter Verwaltung/Behörden verstehen wir grundsätzlich die Kantonsverwaltung (zum Beispiel kantonale Datenschutzaufsichtsstelle) und die Bundesverwaltung (insbesondere die dezentralisierten Verwaltungseinheiten wie zum Beispiel das BAG) gemeinsam. Ist eine spezifische Einheit gemeint, wird diese namentlich erwähnt.
WZW	Die Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit (WZW-Kriterien) gehören nach Art. 32 Abs. 1 KVG zu den grundlegend, kumulativ zu erfüllenden Voraussetzungen der von der OKP übernommenen Leistungen (Eidgenössisches Departement des Innern EDI - Bundesamt für Gesundheit BAG, 2022).

1 Einleitung

1.1 Ausgangslage

Die Digitalisierung im Gesundheitswesen schreitet immer schneller voran. Neue digitale Anwendungen entstehen, analoge Produkte werden mit digitalen Komponenten versehen, Geräte und Produkte werden verknüpft und in Gesamtsysteme integriert, zentrale und dezentrale Datenbanken werden aufgebaut und Leistungserbringer, Dienstleister und Patient haben von verschiedenen Orten Zugriff auf ihre Gesundheitsdaten. Die verstärkte Nutzung digitaler Technologien, die Produktion und Verknüpfung von immer mehr schützenswerten und besonders schützenswerten Daten sowie die Entstehung neuer Geschäftsmodelle rücken zwei Themen in den Fokus: Cybersicherheit und Datenschutz. Bei Cybersicherheit geht es um Massnahmen, die die Integrität, Vertraulichkeit und die Verfügbarkeit der Daten stärken sollen, insbesondere um den Schutz der Systeme vor Angriffen von aussen zu erhöhen. Kontinuierliche Massnahmen im Bereich der Daten- und Informationssicherheit, also der Cybersicherheit, sind gleichzeitig auch unabdingbare Faktoren für die Gewährleistung des Datenschutzes. Bei Datenschutz geht es um den Schutz der individuellen Privatsphäre vor missbräuchlicher Datenverarbeitung sowie die Einhaltung des Rechts auf informationelle Selbstbestimmung, des Persönlichkeitsrechts bei der Datenverarbeitung, beziehungsweise um den Schutz der personenbezogenen Daten.

Sowohl Cybersicherheit als auch Datenschutz sind Querschnittsthemen, die nicht nur den Gesundheitsbereich, sondern alle Branchen betreffen. Die Themen spielen im Gesundheitsbereich aber eine besondere Rolle, da die gesammelten Daten oft als besonders schützenswert gelten und ein Ausfall der kritischen Gesundheitsinfrastruktur verheerende Folgen haben kann. Gerade im Gesundheitswesen wurden zahlreiche Vorfälle von Cyberaktivitäten in den letzten Jahren ausgelöst und die Hacker, deren Zahl sich stark vermehrt hat, sind so aktiv wie nie zuvor (Angerer et al., 2021). Auch ist die Anzahl Meldungen zu Datenschutzfragen durch Patienten gemäss Interviewpartnern signifikant gestiegen. In der Schweiz werden Anforderungen an die Cybersicherheit insbesondere durch das Informationssicherheitsgesetz (ISG, SR 128), die Nationale Cyberstrategie (NCS) und die Medizinprodukteverordnung (MepV, SR 812.213) geregelt. Weiterhin könnte gegebenenfalls das Bundesgesetz über die Produktehaftpflicht (PrHG, SR 221.112.944) herangezogen werden, um Hersteller für Cyberschäden haftbar zu machen. Das PrHG verpflichtet die Hersteller für die Schäden, die durch einen Fehler ihres Produkts entstehen, einzustehen. Ein Produkt ist fehlerhaft, wenn es nicht die Sicherheit bietet, welche die Verbraucher berechtigterweise erwarten dürfen. Daher haben die Hersteller von Produkten den Stand der Wissenschaft und der Technik, beziehungsweise die entsprechenden Normen, anzuwenden. In Bezug auf Cybersicherheit könnte dies bedeuten, dass wenn ein digitales Produkt oder eine Dienstleistung einen Sicherheitsmangel aufweist, der zu einem Datenverlust oder einem anderen Schaden führt, die Hersteller haftbar gemacht werden können. Hersteller sind daher dafür verantwortlich, dass die Anforderungen an

die Cybersicherheit sowohl in der Produktentwicklung als auch im Betrieb der digitalen Dienste eingehalten werden. Darüber hinaus verabschiedete der Bundesrat zusammen mit den Kantonen im Jahr 2023 die NCS. Die Strategie definiert fünf Ziele und 17 Massnahmen (siehe Abbildung 1), um dem das die Gesellschaft durchdringende Thema gerecht zu werden. Dabei zeigt die Strategie insbesondere auf, wo die Zuständigkeiten für Cybersicherheit liegen. Zusätzlich wird für Medizinprodukte das Thema Cybersicherheit im Rahmen der Erfüllung der Anforderungen des Heilmittelgesetz: Bundesgesetz über Heilmittel und Medizinprodukte (HMG, SR 812.21), insbesondere des Risikomanagements, geregelt. Hersteller von Medizinprodukten müssen ein Risikomanagementsystem einrichten, dokumentieren, anwenden und aufrechterhalten (Anhang I Abschnitt 3 Medizinprodukteverordnung [EU MDR]). Im Risikomanagementsystem müssen auch Cyberrisiken abgedeckt und soweit wie möglich reduziert werden (Medical Device Coordination Group, 2019a). Dies schliesst Risiken ein, die sich aus der Wechselwirkung verschiedener Systeme ergeben (Wenner, 2023). Die Konformität digitaler Produkte mit aktuellen Standards der Qualitäts- und Risikomanagementsysteme ist zertifizierbar. Bei Medizinprodukten mit einer höheren Risikoklasse als I muss eine Benannte Stelle am Konformitätsbewertungsverfahren beteiligt werden, die die Übereinstimmung mit den gesetzlichen Vorgaben nach einheitlichen Bewertungsmassstäben bescheinigt.

5 strategische Ziele		17 Massnahmen
Selbstbefähigung	→	**M1** Bildung, Forschung und Innovation in der Cybersicherheit **M2** Sensibilisierung **M3** Bedrohungslage **M4** Analyse von Trends, Risiken und Abhängigkeiten
Sichere digitale Dienstleistungen und Infrastrukturen	→	**M5** Schwachstellen erkennen und verhindern **M6** Resilienz, Standardisierung und Regulierung **M7** Ausbau der Zusammenarbeit zwischen den Behörden
Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cybervorfällen	→	**M8** Vorfallmanagement **M9** Attribution **M10** Krisenmanagement **M11** Cyberdefence
Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität	→	**M12** Ausbau der Zusammenarbeit der Strafverfolgungsbehörden **M13** Fallübersicht **M14** Ausbildung der Strafverfolgungsbehörden
Führende Rolle in der internationalen Zusammenarbeit	→	**M15** Stärkung des digitalen internationalen Genfs **M16** Internationale Regeln im Cyberraum **M17** Bilaterale Zusammenarbeit zu strategischen Partnern und internationalen Kompetenzzentren

Abbildung 1. Ziele und Massnahmen der nationalen Cyberstrategie *(Nationales Zentrum für Cybersicherheit (NCSC), 2023)*

Das nationale Datenschutzrecht wurde totalrevidiert und das neue Datenschutzgesetz (DSG, SR 235.1) und deren Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV, SR 235.11) traten zum 1. September 2023 in Kraft. Das DSG bezweckt den Schutz der Persönlichkeit und der Grundrechte

von natürlichen Personen, über die Personendaten durch private Personen und durch Bundesorgane bearbeitet werden. Das DSG erfordert, dass die Verantwortlichen (zum Beispiel Hersteller) technische und organisatorische Massnahmen ergreifen, die dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sind (Privacy-by-Design). Weiterhin müssen die Verantwortlichen über geeignete Voreinstellungen sicherstellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (Privacy-by-Default, Art. 7 DSG). Darüber hinaus erfordert das DSG eine Datenschutzfolgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann (Art. 22f DSG). Das hohe Risiko ergibt sich – insbesondere bei Verwendung neuer Technologien – aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Insbesondere liegt ein hohes Risiko dann vor, wenn ein Profiling mit hohem Risiko oder umfangreiche Bearbeitungen besonders schützenswerter Personendaten geplant sind (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 2023b). Die meisten erhobenen Daten im Gesundheitswesen dürften als besonders schützenswert gelten. Art. 5 DSG nennt dabei explizit (i) Daten über die Gesundheit, (ii) genetische Daten sowie (iii) biometrische Daten, die eine natürliche Person eindeutig identifizieren. Die Datenschutzkonformität ist durch von der Schweizerischen Akkreditierungsstelle (SAS) akkreditierten unabhängigen Zertifizierungsstellen zertifizierbar (Art. 13 DSG). Diese Stellen können sowohl Organisationen und Verfahren (Managementsysteme) als auch Produkte (Software und Hardware) sowie Dienstleistungen und Prozesse zertifizieren (Art. 1 Abs. 2 Verordnung über Datenschutzzertifizierungen [VDSZ, SR 235.13]). Während normalerweise das nationale Recht zur Anwendung kommt, kommt das kantonale Datenschutz Recht zur Anwendung, wenn Institutionen aufgrund kantonalen Leistungsaufträgen Leistungen erbringen. Dies ist insbesondere der Fall bei Spitälern, die auf der Spitalliste stehen und «Spitallistenleistungen» erbringen oder bei Ärzten, die im Auftrag des Kantons handeln, wie zum Beispiel Schul- oder Amtsärzte.

1.2 Ziel des Berichtes

Die wachsende Anzahl an neuen digitalen Produkten, die mit neuen Herausforderungen in den Bereichen Cybersicherheit und Datenschutz einhergehen, erfordert ein solides Verständnis der Materie und den Verantwortlichkeiten in den zuständigen Stellen. Ziel dieses Fachberichtes ist es somit, spezifische Fragestellungen zu digitalen Gesundheitsanwendungen (dGA) und deren Herausforderungen im Bereich Datenschutz sowie der Cybersicherheit zu beantworten. Weiter soll der Bericht es dem Gesetzgeber und der Verwaltung ermöglichen, die Herausforderungen im Bereich des Datenschutzes und der Cybersicherheit bei dGA zu erkennen und zu verstehen. Der Bericht schliesst mit Empfehlungen, insbesondere für das BAG.

2 Methodik

Die erste Phase beinhaltete eine Dokumentenanalyse in Zusammenarbeit mit den Projektpartnern. In der zweiten Phase wurden die Ergebnisse durch semi-strukturierte Validierungsinterviews gestärkt und ergänzt sowie weitere explorative Fragestellungen adressiert. Als Interviewpartner wurden Hersteller, Leistungserbringer, Leistungszahler sowie die Verwaltung identifiziert. Grundsätzlich wurden die Fragen vorwiegend an Verbände, in einzelnen Fällen aber auch an grössere marktbeherrschende Unternehmen oder Experten gestellt. In der dritten Phase wurden die Ergebnisse konsolidiert und Handlungsempfehlungen formuliert.

2.1 Phase 1: Konzept und Grundverständnis

Nach Finalisierung und Verabschiedung des Analysekonzepts, war es Ziel der ersten Phase, ein Grundverständnis zu schaffen und darauf aufbauend den Interviewleitfaden zu entwickeln und mit dem Auftraggeber abzustimmen. Die Dokumentenanalyse hat die von der Auftraggeberin zur Verfügung gestellten Unterlagen, darunter unter anderem das Faktenblatt zur Vergütung von dGA, die unterschiedlichen Antragsprozesse, die gesetzlichen Regelungen: Bundesgesetz über die Krankenversicherung (KVG; SR 832.10), Verordnung über die Krankenversicherung (KVV, SR 832.102), Krankenpflege-Leistungsverordnung (KLV, SR 832.112.31), HMG, MepV, DSG sowie weitere öffentlich zugängliche Berichte, zum Beispiel Papiere der Verbände, einbezogen. Zugleich wurden aktuelle nationale und internationale regulatorische Debatten zum Thema, etwa um die Umsetzung von der neuen Cybersicherheitsrichtlinie (Network and Information Security Directive [NIS-2]) in der Europäischen Union (EU) oder Projekte zu kritischen Infrastrukturen des Bundesamtes für Cybersicherheit (ehemals Nationale Zentrum für Cybersicherheit [NCSC], neu Bundesamt für Cybersicherheit [BACS]) nachvollzogen. Die Phase 1 schloss mit der Ausarbeitung der Auslegeordnung der rechtlichen Grundlagen und Zuständigkeiten, dem erstellten Interviewleitfaden sowie der Einigung auf die Interviewpartner (siehe Tabelle 1) ab.

2.2 Phase 2: Validierung der Auslegeordnung und Exploration

Die Interviewpartner wurden gemeinsam mit dem Auftraggeber identifiziert und umfassten insbesondere Vertreter der Verbände der Leistungsanbieter und Leistungszahler sowie Experten der Verwaltung. Unter den Leistungsanbietern verstehen wir auch Importeure von Medizinprodukten, die Software enthalten, welche in anderen Jurisdiktionen entwickelt wurden oder weiterhin unterstützt werden (importierte Cybersicherheitsrisiken). Für die Interviews wurde ein Leitfaden entwickelt, um eine strukturierte Befragung zu ermöglichen (siehe Anhang Kapitel 6.1). Insgesamt wurden 12 Interviews durchgeführt (siehe Tabelle 1), welche vornehmlich online stattgefunden haben. Darüber hinaus wurde verschiedentlich für Rückfragen ein weiterer Termin mit den Interviewpartnern organisiert und mit weiteren Experten informelle Gespräche geführt. Die Interviews wurden für die internen Analysen aufgezeichnet und kurz-transkribiert, beziehungsweise zusammengefasst. Die Interviewpartner wurden dem

Auftraggeber bekannt gegeben, ohne dabei Rückverfolgbarkeit der Aussagen auf die involvierten Personen zu ermöglichen und somit eine gewisse Vertraulichkeit zu garantieren.

Tabelle 1: Übersicht der Interviewpartner

Leistungsanbieter	Leistungszahler	Verwaltung	Experten
– Verbindung der Schweizer Ärztinnen und Ärzte – FMH (Anwender) – Schweizer Berufsverband für Pflegefachpersonal – SBK (Anwender) – Schweizerischer Verband der Diagnostikindustrie (SVDI) – Schweizerische Stiftung SPO Patientenorganisation (Leistungsempfänger)	– santésuisse	– BAG (KUV, DTS) – Swissmedic – Datenschutzaufsichtsstelle des Kantons Bern (DSA) – Bundesamt für Cybersicherheit – Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB	– Industrie & Beratung – Mitglied Eidgenössische Kommission für Analysen, Mittel und Gegenstände (EAMGK)

2.3 Phase 3: Handlungsempfehlungen

In der dritten und letzten Phase wurden die Ergebnisse aus der Dokumentenanalyse und den Interviews konsolidiert und synthetisiert. Die Handlungsempfehlungen beinhalten auch Hinweise zu möglichem Anpassungsbedarf der bestehenden BAG-Prozesse/Dokumente oder neu zu erstellenden Guidance Dokumenten/Checklisten.

3 Datenschutz und Cybersicherheit

Datenschutz und Cybersicherheit sind eng miteinander verbundene Begriffe, die die Sicherheit von Daten und Informationen aus unterschiedlichen Perspektiven behandeln. Im Datenschutz wird die grundrechtlich geschützte Privatsphäre (Art. 13 Bundesverfassung [BV, SR 10] und Art. 8 Europäische Menschenrechtskonvention [EMRK, SR 0.101]) einzelner Personen auf den Kontext der Datenverarbeitung, -speicherung und -kommunikation angewandt. Insbesondere personenbezogene Daten – alle, mit denen eine Person identifiziert werden kann – müssen «sicher», also vertraulich und integer verarbeitet werden und für den Nutzer verfügbar sein. Die Bearbeitung von Daten muss für den Nutzer transparent sein. In der Schweiz regelt das DSG den Datenschutz, in der EU die Datenschutz-Grundverordnung (DSGVO) (Sandmann, 2022). Im Gesundheitsbereich werden Personendaten durch öffentliche und private Gesundheitseinrichtungen und Leistungserbringer, Krankenkassen, aber auch durch Dienstleister und Hersteller individueller dGA verarbeitet. Unter dGAs werden gemäss dem BAG (2022) aktuell Produkte verstanden, deren medizinischer Zweck durch die Hauptfunktion der digitalen Technologien erzielt wird. Dies umfasst Anwendungen im Bereich der Telemedizin, dem Telemonitoring sowie Apps und mobile Geräte. Digitale Applikationen, die lediglich dazu dienen, die Tätigkeiten von Gesundheitsfachpersonen zu unterstützen (z.B. Auslesen und Analysieren von Daten oder Steuern eines Gerätes) werden nicht dem Begriff der dGAs zugeordnet.

Cybersicherheit beschäftigt sich mit Fragen der Datensicherheit aus einer systemischen Perspektive. «Sicher» sind digitale Prozesse gemäss Art. 3 lit. a Cyberrisikenverordnung (CyRV, SR 120.73) dann, wenn *«die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert»*. Da Cybersicherheit einen nie definitiv erreichten Zustand beschreibt, reguliert der Gesetzgeber im Regelfall lediglich die Pflichten, angemessene Massnahmen zu treffen und diese regelmässig im Rahmen eines Risikomanagements zu überprüfen. Dazu gehören alle Schritte, die *«der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen»* (Art. 6a CyRV). Im Bereich Datensicherheit geht es primär darum, Manipulation, Datenverlust oder Unbefugten Zugriff auf Daten zu verhindern; Informationssicherheit beschreibt die Unversehrtheit eines informations- und kommunikationstechnischen Systems. Ein Cybervorfall liegt dann vor, wenn *«ein unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann»* (Art. 3b CyRV). Zum Ergreifen von Massnahmen zur Stärkung der Cybersicherheit werden neben öffentlichen Einrichtungen auch private Unternehmen, die etwa an kritischen Infrastrukturen wie dem Gesundheitswesen beteiligt sind und zunehmend auch Hersteller von Produkten für den Einsatz in diesen Infrastrukturen, verpflichtet.

3.1 Entwicklung von MedTech-Software: Was muss bei der Entwicklung bezüglich Datenschutzes/Cybersicherheit allgemein erfüllt, respektive berücksichtigt werden?

dGA müssen wie alle digitalen Anwendungen und Produkte allgemeinen rechtlichen Anforderungen genügen. Dies gilt insbesondere für den Datenschutz (DSG und DSV), aber auch für gesetzmässige Grundlagen der Produktesicherheit, die in der Schweiz sektorenspezifisch, für Medizinprodukte also im HMG und in der MepV geregelt sind. In der EU gelten ab Dezember 2024 mit der General Product Safety Regulation (GPSR) horizontal vereinheitlichte Produktsicherheitsstandards, die Hersteller verpflichten, digitale Sicherheitsaspekte stärker zu beachten. Neu können hier auch digitale Änderungen an mehrheitlich analogen Produkten als wesentlich erachtet werden und daher Hersteller zum Beispiel dazu verpflichten, neue Risikoüberprüfungen durchzuführen. In unseren Interviews wird der potenzielle Einfluss der GPSR auf dGA als hoch angesehen, da sie grundlegend, also zusätzlich zur EU MDR gilt. Schliesslich müssen Produkte oder Netztechnologien, die über das Internet kommunizieren («Internet of Things»/IoT Objekte) die Konformitätsvorschriften des Bundesamtes für Kommunikation (BAKOM) einhalten und unter Umständen den Registrierungserfordernissen des BAKOM für Fernmeldedienstanbieter entsprechen.

Im Bereich Cybersicherheit ist mit dem revidierten ISG eine rechtliche Grundlage geschaffen worden, die für Bundesorgane, wichtige Unternehmen und Einrichtungen der kritischen Infrastrukturen zentrale Vorgaben macht. Konkret verlangt die Informationssicherheitsverordnung (ISV, SR 128.1) die Einrichtung eines Information Security Management System (ISMS), das den Schutzbedarf verarbeiteter Daten ermitteln und bewerten soll (Art. 5 ISV), die Etablierung eines Risikomanagements (Art. 8 ISV) und Sicherheitsverfahren auch in Zusammenarbeit mit Dritten, aber auch personelle Massnahmen, und den Umgang mit physischen Gefahren voraussetzt. Im Bereich Cybersicherheit sieht das revidierte ISG ebenso unter anderem für Spitäler eine Meldepflicht nach Cyberangriffen vor.

In der EU gilt ab Herbst 2024 die NIS-2-Richtlinie, die das Cybersicherheitsniveau in der EU vereinheitlichen und anheben soll. Da sie auch Partnerorganisationen und Lieferketten einschliesst, ist sie in Teilen auch für die Schweiz relevant. Die Umsetzung der NIS-2-Richtlinie wird Herstellern von Medizinprodukten (der Koordinierungsgruppe Medizinprodukte [MDCG]) als gleichzeitig zur EU MDR geltend anempfohlen (MDCG 2019-16 Rev. 1, Kap. 7). Die NIS-2-Richtlinie sieht neben einem Risikomanagement und grundlegenden Informationssicherheitspraktiken insbesondere auch die Weiterbildung allen Cyberrisiken ausgesetzten Personals, der Inventur aller medizinischen Geräte, Sicherheitsprozeduren für Drittgeräte und die Vermeidung von nicht mehr oder nur noch selten geupdateten digitalen Produkten vor. Die Umsetzung der NIS-2 Richtlinie wird nach Ansicht einiger Interviewpartner auch für die Hersteller dGAs Anpassungen erfordern, insbesondere was den Betrieb und den Support älterer dGA angeht.

3.1.1 Allgemeine Anforderungen im Datenschutz

Seit dem 1. September 2023 ist das totalrevidierte DSG mit den Ausführungsbestimmungen in der DSV und der VDSZ in Kraft. Die neuen Regelungen sollen für einen besseren Schutz persönlicher Daten sorgen, in dem die Selbstbestimmung über die persönlichen Daten gestärkt sowie die Transparenz bei der Beschaffung von Personendaten erhöht werden. Mit dem DSG wird das Schweizer Datenschutzrecht im Wesentlichen dem Datenschutzstandard des Europäischen Rechtsraums, der DSGVO, angepasst. Insgesamt sind die beiden Datenschutzrechte ähnlich. Es ist grundsätzlich festzuhalten, dass das Datenschutzrecht von Bund und Kantonen der Schweiz dem Europäischen zwar nicht im Wortlaut gleicht, aber ein im Endergebnis gleichwertiges Schutzniveau vorsieht (Rovelli & Epiney, 2020). Dies ist notwendig, um zu vermeiden, dass die EU zusätzliche Schutzmassnahmen im Datenaustausch mit Schweizer Servern verlangt (der sogenannte Angemessenheitsbeschluss nach Art. 45 DSGVO). Es gibt jedoch im Detail Unterschiede (insbesondere im Bereich der Vorkonsultationspflicht, der Meldepflicht und der Einschränkungsmöglichkeit spezifischer Regelungen durch das Allgemeine Gleichbehandlungsgesetz), die Unternehmen und Organisationen bei der Datenverarbeitung beachten müssen (Rosenthal, 2020). Hierauf wurden wir auch wiederholt in den Interviews hingewiesen. Eine Europäische Zertifizierung sollte also den Anforderungen des neuen schweizerischen Datenschutzrechts genügen, da sich das schweizerische Datenschutzrecht am Schutzstandard der EU orientiert. Die wichtigsten relevanten Neuerungen im Datenschutzrecht sind zur Übersicht in den folgenden Abschnitten kurz definiert und erläuternd dargelegt.

Recht auf Vergessen/Löschen | Art. 30 & 31 DSG

Aus dem Recht auf Vergessen ergibt sich für die Betroffenen der Anspruch, gewisse Daten bei einer Persönlichkeitsverletzung löschen zu lassen. Bei überwiegenden Interessen, die in Art. 31 Abs. 2 lit. a-f DSG festgehalten sind, kann der Anspruch nach Durchführung einer Güterabwägung erlöschen.

Das Recht auf Vergessen gibt den betroffenen Personen, deren Daten bearbeitet werden, den Anspruch auf die Veranlassung der Löschung entsprechender Daten. Dieser Anspruch ergibt sich gemäss Art. 30 DSG, wenn entgegen der ausdrücklichen Willenserklärung der betroffenen Person trotzdem Personendaten bearbeitet werden und weder eine gesetzliche Grundlage noch überwiegende private Interessen Dritter als Rechtfertigung dienen. In einem solchen Fall liegt eine Persönlichkeitsverletzung vor. Aus der Persönlichkeitsverletzung ergibt sich ein Recht auf Datenlöschung, wenn nicht ein überwiegendes Interesse gemäss Art. 31 Abs. 2 DSG vorliegt, das zum Beispiel auch die Bearbeitung der Personendaten über den Vertragspartner zum Abschluss oder Abwicklung eines Vertrages beinhaltet, oder auch zu Forschungs-, Planungs- oder Statistikzwecken unter gewissen Voraussetzungen die Datenbearbeitung erlaubt (EIT.swiss, o. J.). Das überwiegende Interesse als Einschränkung des Rechts auf Vergessen setzt die Vornahme einer Güterabwägung zwischen dem Rechtfertigungsgrund für die Persön-

lichkeitsverletzung und das Recht auf Vergessen voraus. Die ausführliche Liste von Rechtfertigungsgründen, die bei entsprechender Güterabwägung als überwiegendes Interesse in Frage kommen, befindet sich in Art. 31 Abs. 2 lit. a-f DSG.

Privacy-by-Design | Art. 7 Abs. 1 & 2 DSG

Privacy-by-Design hält fest, dass die datenschutzrechtlichen Anforderungen bei Produkten und Softwareangeboten, bei denen personenbezogene Daten verarbeitet werden, bereits in der Anfangsphase der Produktentwicklung, sowie während der gesamten Nutzungsdauer zu berücksichtigen und im Design zu integrieren sind.

Privacy-by-Design bedeutet, dass die Datenbearbeitung so auszugestalten ist, dass sie technisch und organisatorisch dazu geeignet ist, die Grundsätze der Datenbearbeitung einzuhalten und gemäss dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung einen angemessenen Schutz der Daten der betroffenen Person zu gewährleisten. Mit dem Begriff wird ein Prinzip im neuen DSG verankert, welches grundsätzlich unter dem alten Recht schon galt. Die Privacy-by-Design-Vorgaben sind nur für Verantwortliche einzuhalten, wobei sowohl Private wie auch Bundesorgane angesprochen sind. Auftragsverarbeitende, Hersteller, Entwickler und Anbieter technischer Produkte sind nicht zur Einhaltung der daraus fliessenden Vorgaben verpflichtet (Lang, 2024).

Im Wesentlichen müssen Verantwortliche die Datenbearbeitungssysteme so gestalten, dass sie den Grundsätzen von Art. 6 DSG und den Anforderungen der Datensicherheit gemäss Art. 8 DSG entsprechen. Zusammenfassend verpflichtet Privacy-by-Design die Verantwortlichen dazu, die Datenschutzgrundsätze (zum Beispiel Datenminimierung) wirksam umzusetzen, die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen des DSG zu genügen sowie die Rechte der betroffenen Personen zu schützen. Ziel dieses Prinzips ist es, ein hohes Datenschutzniveau sicherzustellen, ohne dass die Verbraucher den Schutz ihrer Daten erst durch umständliche Einstellungen im Gerät herbeiführen müssen.

Aus dem Prinzip haben sich zwei neue ISO-Normen ergeben. Einerseits enthält ISO 31700-1 allgemeine Anleitungen und Hinweise zur Entwicklung von Funktionen, die es den Verbrauchenden ermöglichen, ihre Datenschutzrechte durchzusetzen. Umsetzungshinweise zu den allgemeinen Anleitungen werden in der ISO 31700-2 in einem separaten Dokument anhand von spezifischen Beispielen erläutert. Die ISO-Normen sind als Empfehlung zu verstehen und könnten besonders interessant für Verantwortliche sein, die regelmässig mit der Entwicklung von Produkten, Systemen oder Dienstleistungen beschäftigt sind und dabei den Schutz personenbezogener Daten gewährleisten wollen.

Privacy-by-Default | Art. 7 Abs. 3 DSG

Definition: Privacy-by-Default ist ein Teilgehalt von Privacy-by-Design. Daraus ergibt sich die Pflicht für Verantwortliche, dort wo verschiedene Einstell- oder Wahlmöglichkeiten bestehen, die datenschutzfreundlichste Kombination als Grundeinstellung vorzusehen.

Privacy-by-Default beinhaltet, dass die Voreinstellungen bei der Datenbearbeitung so auszugestalten sind, dass lediglich ein Mindestmass der Daten erhoben und genutzt wird. Erweiterungen der Datenerhebung, Datennutzung und der öffentlichen Einsehbarkeit müssen erst durch aktives Eingreifen der betroffenen Person erfolgen. Damit können die Betroffenen ausgehend von der datenschutzfreundlichsten Voreinstellung eine andere Wahl treffen und damit auch weitergehende Datenbearbeitungen erlauben. Ob verschiedene Einstellungsmöglichkeiten vorzusehen sind, ist unter dem Aspekt von Privacy-by-Design zu prüfen.

Unter dem Gesichtspunkt des Prinzips Privacy-by-Default entsprechen Voreinstellungen mit einer sogenannten Abwahlmöglichkeit (Opt-out-Voreinstellung) nicht den erforderlichen Einstellungsmöglichkeiten, weil die Erweiterung beziehungsweise die Abweichung von der datenschutzfreundlichsten Grundeinstellung ein aktives Verhalten erfordert (Kanzlei.biz, 2024). Somit müssen die datenschutzfreundlichsten Auswahlfelder bereits vorab aktiviert sein, während die weniger datenschutzfreundlichen Optionen erst auf aktives Tun des Betroffenen hin aktiviert werden dürfen. Das Prinzip von Privacy-by-Default schafft bei den Betroffenen die berechtigte Erwartung, dass sie ohne Vornahme eigener Anpassungen jederzeit von der datenschutzfreundlichsten Einstellung profitieren.

Die Leitlinie des Europäischen Datenschutzausschusses – EDSA-Leitlinie 4/2019 (European Data Protection Board, 2020) gibt dabei Anweisungen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, die auf die Anforderungen im DSG anwendbar sind. Praktische Hinweise in Bezug zu den Prinzipien Privacy-by-Design und Privacy-by-Default liefert eHealth Suisse im Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer (2022a). Zudem haben Backer-Heuveldop et al. (2022) von der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie eine Praxishilfe für mobile Apps im Gesundheitswesen erarbeitet.

Meldepflicht für Bundesorgane | Art. 12 DSG

Definition: Bei Datenbearbeitungen durch Bundesorgane, die im Bereich des DSG fallen, müssen die jeweiligen Bundesorgane gewisse Informationen betreffend die Datenbearbeitung sammeln und diese dem EDÖB mitteilen.

Die Verantwortlichen sowie die Auftragsbearbeiter bei Datenbearbeitungen müssen per Gesetz ein Verzeichnis ihrer Bearbeitungstätigkeiten führen. Dies umfasst die Identität des Verantwortlichen, den Bearbeitungszweck, eine Beschreibung der Kategorien, der betroffenen Personen sowie die Kategorie der

bearbeiteten Personendaten sowie die Kategorien der Empfänger. Zudem muss bei Möglichkeit die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung der Dauer bestimmt werden. Eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit (Art. 8 DSG) ist, wenn möglich, auch anzugeben. Falls die Daten ins Ausland bekanntgegeben werden, müssen sowohl die empfangenden Staaten als auch die Garantien nach Art. 16 Abs. 2 DSG angegeben werden. Für die Erstellung des Verzeichnisses hat die FMH (2023) einen Leitfaden erstellt.

Meldepflicht bei Datenverletzungen | Art. 24 DSG

Definition: Wenn die Vertraulichkeit, die Integrität oder die Verfügbarkeit von Personendaten verletzt wird, etwa dadurch, dass Daten verloren gehen, versehentlich oder unerlaubt gelöscht, vernichtet oder verändert werden oder für nicht berechtigte Personen zugänglich werden, muss der EDÖB informiert werden. Eine Meldung an die von der Verletzung betroffene Person kann ebenfalls notwendig sein oder vom EDÖB verlangt werden.

Bei einer Verletzung der Datensicherheit, beziehungsweise der Kenntnis davon, muss der Verantwortliche so rasch wie möglich eine Meldung an den EDÖB machen, wenn voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person besteht. Eine solche Meldung muss auch der Auftragsbearbeiter dem Verantwortlichen machen. Zudem kann auch eine Meldung an die betroffene Person durch den Verantwortlichen notwendig sein, oder auch vom EDÖB verlangt werden. Die Meldung an die betroffene Person kann unter anderem aufgrund überwiegender Interessen Dritter oder (im Falle eines Bundesorganes als Datenbearbeiter) überwiegender öffentlicher Interessen, der Gefährdung von Untersuchungen, Ermittlungen oder behördliche oder gerichtliche Verfahren, beschränkt werden. Die meldepflichtige Person kann nur mit deren Einverständnis aufgrund der Meldung einem Strafverfahren unterstellt werden.

Datenschutz-Folgeabschätzung | Art. 22 & 23 DSG

Definition: Beim Vorliegen eines hohen Risikos für den Betroffenen muss der Verantwortliche eine Datenschutzfolgeabschätzung vornehmen. Daten über die Gesundheit einer Person gehören zu besonders schützenswerten Daten, die gemäss Art. 22 Abs. 2 lit. a DSG stets zu einem hohen Risiko führen. Stellt der Verantwortliche durch die Durchführung der Datenschutz-Folgenabschätzung fest, dass durch die geplanten Datenbearbeitung trotz der getroffenen Massnahmen weiterhin ein hohes Risiko besteht, muss der EDÖB vor der Datenbearbeitung konsultiert werden.

Bei der Datenschutz-Folgeabschätzung geht es darum, potenzielle Risiken aus einer Datenbearbeitung zu erkennen und zu bewerten. Ob eine Datenschutz-Folgeabschätzung durchgeführt werden muss, kann mittels einer Vorabschätzung bestimmt werden. Diese Vorabschätzung muss jeweils im Einzelfall und

im Voraus durchgeführt werden. Die Leitlinien der EU zur Datenschutz-Folgenabschätzung der Europäischen Kommission (European Commission, 2017) liefern Hilfestellungen bei Entscheidung über die Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung.

Die Datenschutz-Folgeabschätzung stellt eine Rechenschaftspflicht für bestimmte Datenbearbeitungen dar. Sie dient dazu sicherzustellen, dass eine geplante Datenbearbeitung nicht zu einer Verletzung des DSG führt. Eine Anleitung zur Durchführung einer Datenschutz-Folgeabschätzung liefert das Merkblatt des EDÖB (2023a).

Von einer Datenschutz-Folgenabschätzung kann abgesehen werden, wenn die Bearbeitung aufgrund einer gesetzlichen Vorgabe erfolgt, wenn die eingesetzten Systeme, Produkte oder Dienstleistungen für die vorgesehene Bearbeitung zertifiziert sind oder wenn ein dem EDÖB vorgelegter Verhaltenskodex eingehalten wird.

Schlussfolgerungen:

Der Schutz persönlicher Daten und die Sicherheit von Informationssystemen vor Cyberangriffen sind auch in der Schweiz wichtige rechtspolitische Themen. Hierfür sind zunehmend nicht mehr nur Akteure der öffentlichen Hand, sondern auch private Spitalbetreiber, Dienstleister und auch Hersteller von dGA in der Pflicht.

Im Datenschutz ist dabei von einem einheitlichen Schutzniveau in der EU und der Schweiz auszugehen. Im Bereich Cybersicherheit sind wir uns mit unseren Interviewpartnern einig, dass gerade die Entwicklung auf europäischer Ebene (GPSR und NIS-2-Richtlinie) starke Auswirkungen für die Herstellung von dGA und für digitale Gesundheitsdienstleistungen insgesamt haben werden, da sie zusätzlich und grundlegend zur sektorspezifischen Regulierung der EU MDR gelten.

3.2 Rechtliche Grundlagen: Was sind die spezifischen rechtlichen Grundlagen für dGA im Bereich Cybersicherheit und Datenschutz?

Da alle Gesundheitsdaten *grundsätzlich* zu den besonders schützenswerten Personendaten (DSG Art. 5 lit. c Abs. 2) zählen und da das Gesundheitswesen als kritische Infrastruktur grundsätzlich für das Wohlergehen der Bevölkerung essenziell ist (siehe dazu auch die Nationale Strategie zum Schutz kritischer Infrastrukturen), hat der Gesetzgeber in der Schweiz wie in den meisten anderen Ländern zusätzlich geltende Pflichten und Massnahmen definiert, die den Datenschutz und die Cybersicherheit im Gesundheitsbereich betreffen. Der nächste Abschnitt beschreibt die rechtlichen Grundlagen dieser zusätzlichen Pflichten, für Informationen zu allgemeinen Regeln digitaler Produkte wird auf die einschlägige Literatur verwiesen.

Das HMG regelt den Umgang mit Heilmitteln, insbesondere auch deren Herstellung und ihr Inverkehrbringen, wobei der Begriff Heilmittel als Oberbegriff zu verstehen ist und sowohl Arzneimittel als auch Medizinprodukte umfasst. Art. 62a HMG ist die gesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Personendaten durch Stellen des Bundes und der Kantone, regionale Zentren und mit Vollzugsaufgaben betraute Dritte. Art. 62c HMG beschreibt die Pflicht der Swissmedic zur Führung eines Informationssystems über Medizinprodukte. Dieses dient speziell der Gewährleistung der Sicherheit von Medizinprodukten sowie von deren Vigilanz und Überwachung. Dieses enthält insbesondere schützenswerte Personendaten nach Art. 62a HMG. Genaueres regeln Art. 83-92 MepV.

Die Reglementierung der Medizinprodukte erfolgt in der Schweiz vornehmlich in der MepV. Diese orientiert sich grundsätzlich an der EU MDR. Art. 6 MepV legt dabei die grundlegenden Sicherheits- und Leistungsanforderungen fest und verweist inhaltlich in Abs. 2 auf den Anhang I der EU MDR. Hier werden neben allgemeinen fachlichen und betrieblichen Anforderungen und notwendigen Risikoabwägungen und Risikomanagementsysteme unter anderem auch festgelegt, welchen Anforderungen Produkte genügen müssen, wenn sie in Wechselwirkung mit ihrer Umgebung stehen (Art. 14 Anhang I EU MDR). Cybersicherheit und Datenschutz werden dabei im Rahmen des vorgegebenen Entwicklungsansatz impliziert, da ein angemessenes Sicherheitskonzept verlangt wird.

3.2.1 Spezifische Anforderungen bei der Inverkehrbringung von dGAs

Für die Inverkehrbringung einer dGA mit medizinischem Zweck oder digitaler In-vitro-Diagnostika (IVDs) müssen grundsätzlich die gleichen Anforderungen wie für Medizinprodukte erfüllt werden. Die dafür wichtigsten Rechtsgrundlagen für die Inverkehrbringung sind:

- Bundesgesetz über Arzneimittel und Medizinprodukte (HMG)
- Medizinprodukteverordnung (MepV)
- Verordnung über In-vitro Diagnostika (IvDV, SR 812.219)

Darüber hinaus sind die folgenden Rechtsgrundlagen für die Entwicklung relevant:

- Bundesgesetz über die Forschung am Menschen (HFG, SR 810.30)
- Verordnung über klinische Versuche mit Medizinprodukten (KlinV-Mep, SR 810.306)

Das HMG, sowie die beiden Verordnungen MepV und IvDV wurden nach Inkrafttreten der Verordnung EU MDR/In-vitro-Diagnostika (EU IVDR) in der EU überarbeitet und weitestgehend angeglichen. Sowohl die MepV als auch die IvDV nehmen in weiten Teilen direkten Bezug auf die EU-Regularien. Die MepV ist seit dem 26. Mai 2021 und die IvDV seit 26. Mai 2022 in Kraft.
Die in der MepV/IvDV dargelegten Anforderungen sind umfassend und beinhalten neben Sicherheits- und Leistungsanforderungen weitere Elemente wie Qualitäts- und Risikomanagement sowie Anforderungen an die Post-market-Surveillance. Die grundlegenden Sicherheits- und Leistungsanforderungen sind als Minimalanforderungen zu verstehen und werden jeweils in den Anhängen 1 der

EU MDR/IVDR beschrieben. Als Teil des Risikomanagements müssen auch Datenschutz- und Cybersicherheitsrisiken beurteilt werden (eHealth Suisse, 2022).

Die Hersteller sind selbst verantwortlich, dass ihre Produkte die grundlegenden Sicherheits- und Leistungsanforderungen sowie die weiteren Anforderungen des HMGs erfüllen (eHealth Suisse, 2022). Für die Erfüllung der Anforderungen können sich die Hersteller teilweise an harmonisierte Normen halten. Hält ein Hersteller diese ein, wird von einer Erfüllung der wesentlichen Anforderungen ausgegangen (Konformitätsvermutung). Swissmedic notiert in ihrem Merkblatt relevante Normen für Medizinprodukte-Software (2021), die durch den Leitfaden von e-Health Suisse (2022b) ergänzt werden. Darunter sind:

- ISO 13485: Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke
- ISO 14971: Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte
- IEC62366-1: Anwendung der Gebrauchstauglichkeit auf Medizinprodukte
- EN 62304: Medizingeräte-Software – Software – Lebenszyklus – Prozesse
- EN ISO/IEC 15408: Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie
- IEC 80001: Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten
- IEC TR 60601-4-5: Medizinische Technische Geräte – Leitfaden und Bewertung – Sicherheitsbezogene technische Anforderungen für Security
- IEC 81001-5-1: Sicherheit, Effektivität und Sicherheit von Gesundheitssoftware und Gesundheits-IT-Systemen

3.2.2 Konformitätsbewertungsstellen

Für die Inverkehrbringung von dGAs müssen diese den Anforderungen des HMG entsprechen und das Konformitätsbewertungsverfahren erfolgreich durchlaufen haben. Die Konformität wird durch die CE-Kennzeichnung auf dem Medizinprodukt sichtbar gemacht. Bei dGAs der Risikoklassen Is/m/r und höher muss die Konformität durch eine externe benannte Stelle (Notified Body) geprüft werden. Benannte Stellen sind unabhängige, staatlich autorisierte Drittfirmen, die im Auftrag der Medizinprodukteheersteller die Konformitätsbewertung überprüfen. Die Wahl der benannten Stelle steht dem Hersteller frei, solange die benannte Stelle von der zuständigen Behörde im betreffenden EWR-Staat oder der Türkei akkreditiert ist und selbst für die jeweilige Produktgruppe zertifiziert ist. Hersteller, die ihr Produkt nach der EU MDR/IVDR zertifiziert haben, können dieses Produkt in der Schweiz mit Hilfe eines schweizerischen Bevollmächtigten (CH-REP) auf den Markt bringen. Falls Hersteller die dGA nur auf dem Schweizer Markt Inverkehrbringen möchten, können diese auch dem zu CE-analogen Schweizer MD-Konformitätsbewertungsverfahren folgen (MD-Kennzeichnung nach Anhang 5 MepV sowie Anhang 4 IvDV). Als benannte Stelle für das MD-Konformitätsbewertungsverfahren agiert, die in der Schweiz beheimatete Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS).

Die von der Swissmedic (bezeichnende Behörde) benannten und überwachten Konformitätsbewertungsstellen, respektive benannten Stellen überprüfen bei Herstellern Medizinprodukte auf ihre Übereinstimmung mit den gesetzlichen Anforderungen. Dies beinhaltet die Überprüfung aller spezifischen gesetzlichen Anforderungen für Medizinprodukte im Bereich von Cybersicherheit und Datenschutz. Die benannten Stellen führen dazu Konformitätsbewertungsverfahren für all diejenigen Produkte durch, die ausserhalb der niedrigsten Risikoeinstufung (Risikoklasse I) klassifiziert sind. Nach erfolgreich abgeschlossenen Verfahren werden den Herstellern die entsprechenden Konformitätsbescheinigungen ausgestellt, was diese ermächtigt, ihre Produkte konform in Verkehr zu bringen (Swissmedic - Schweizerisches Heilmittelinstitut, o. J.-a).

Folgende konkrete Aufgaben können zusammengefasst werden (abhängig vom Konformitätsbewertungsverfahren):

- die technische Dokumentation zu prüfen oder/und
- jedes einzelne Produkt zu prüfen oder/und
- ein Baumuster zu prüfen oder/und
- ein Qualitätsmanagementsystem zu auditieren, zu zertifizieren und zu überwachen, welches insbesondere auch das Risikomanagementsystem beinhaltet (Johner Institut, o. J.).

3.2.3 Anforderungen im Lebenszyklus von dGA

Anhang I EU MDR wird im Fachbericht der MDCG (MDCG 2019-16 Rev.1) in Bezug auf Cybersicherheit und Datenschutz ausführlich ausgelegt. Hauptzweck dieses Dokuments ist es, den Herstellern eine Anleitung zu geben, wie sie alle einschlägigen grundlegenden Anforderungen des Anhangs I der EU MDR und der EU IVDR im Hinblick auf die Cybersicherheit zu erfüllen.

Der Fachbericht beschreibt Bedingungen für sicheres Design und Herstellung, Dokumentationsempfehlungen und Aktivitäten nach der Inverkehrbringung (siehe Abbildungen 2 und 3). Besonders wichtig ist hier, dass Massnahmen zur Stärkung Cybersicherheit nicht mit der Entwicklung eines Produkts «erreicht» sind, sondern nur durch regelmässige Updates gewährleistet werden können («state of the art», Sektionen 1, 4, 17.2 EU MDR Annex I).

Die Weiterentwicklung nach Inverkehrbringung durch regelmässige Wartung und Aktualisierung ist aus dieser Perspektive also nicht freiwillig, sondern zwingend im Rahmen der Cybersicherheitspflichten zu gewährleisten. Eine Zertifizierung bei Inverkehrbringung hat über diesen notwendigen Teil der Cybersicherheitsmassnahmen keine Aussagekraft. In unseren Fachgesprächen sowohl mit Behörden als auch Gesundheitseinrichtungen werden diese Post-market-Aktivitäten der Hersteller aber in vielen Fällen als defizitär angesehen. Mehrere Gesprächspartner äusserten hierbei die Ansicht, dass es die gesundheitspolitische Aufgabe des BAG sei, Hersteller zur Erfüllung ihrer Pflichten nach Inverkehrbringung der Produkte aufzurufen.

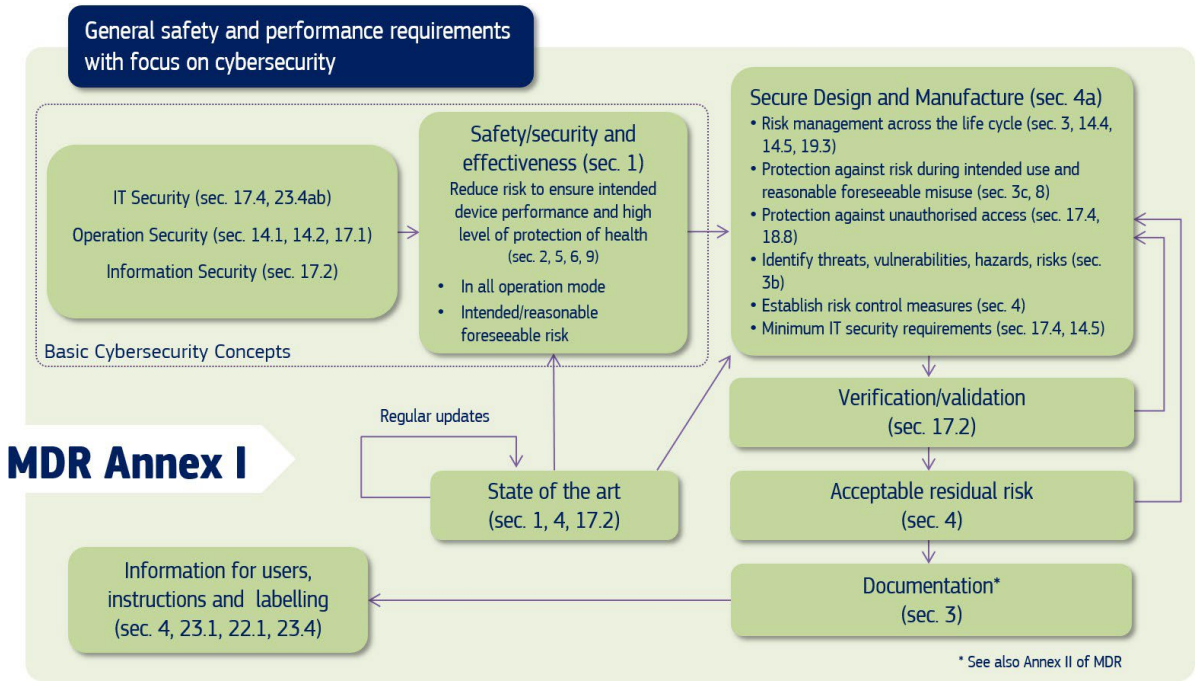

Abbildung 2: Cybersicherheitsanforderungen nach MDCG 2019-16 Rev.1 *(Medical Device Coordination Group, 2019a)*

Dass auch Hersteller die Interpretation des Fachberichts MDCG 2019-16 Rev.1 akzeptieren, belegen diverse Stellungnahmen. So sieht etwa die European Trade Association of the Medical Technology Industry (MedTech Europe), die sich aus europäischen Unternehmen unterschiedlicher Grösse zusammensetzt, die EU MDR und die MDCG 2019-16 Rev.1 als sinnvolle und praktikable Rahmensetzung für die Cybersicherheit von dGA. MedTech Europe verpflichtet sich der Beachtung und Einhaltung der darin enthaltenen Vorgaben (MedTech Europe, 2023).

dGA, die den MDCG-Standards nicht genügen, drohen als inkompatibel eingestuft zu werden sowie den europäischen Vollstreckungsbehörden unterstellt zu werden. Es ist daher anzunehmen, dass Hersteller signifikante Anpassungen im Bereich des Risikomanagements und des Supports während des Lebenszyklus vornehmen müssen, um künftig den Anforderungen der MDCG 2019-16 Rev. 1 zu entsprechen (Vollebregt, 2020). Ein ähnliches Bild ergibt sich in der Schweiz, wo auch Swissmedic (2021) die MDCG 2019-16 Rev.1 als relevantes Rahmenwerk auflistet, die bei der Herstellung von Medizinprodukten zu beachten ist. Auch im Herstellerkreis wird die Guidance als bedeutsam für die Schweizer Medizinindustrie eingestuft (Isler & Bichsel, 2021).

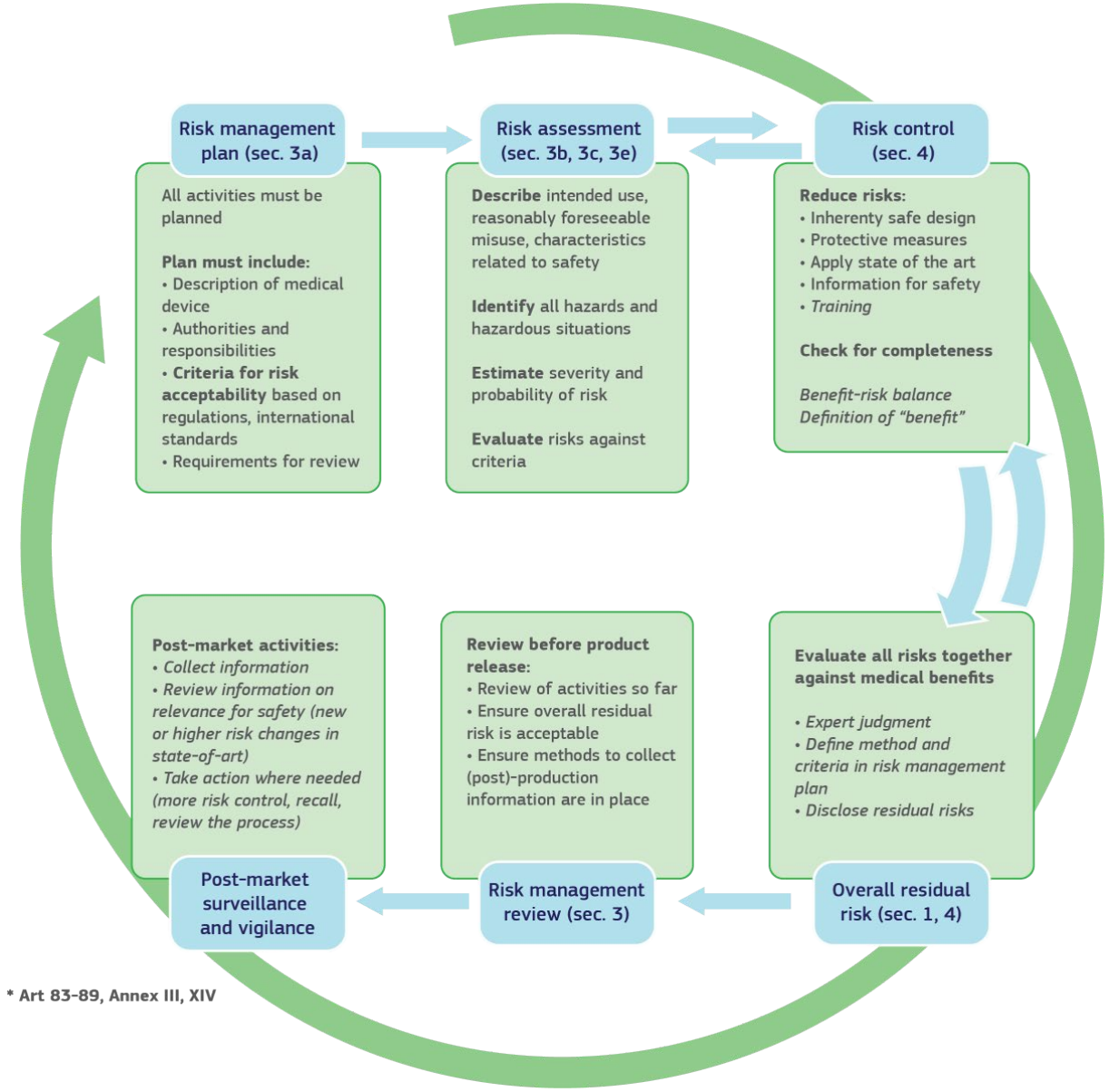

Abbildung 3: Cybersicherheit im Lebenszyklus nach MDCG 2019-16 Rev. 1 *(Medical Device Coordination Group, 2019a, S. 1)*

Schlussfolgerungen:

Neben den allgemeingültigen Anforderungen gelten für dGA im Bereich Datenschutz und Cybersicherheit die Regelungen des HMGs, dass mit Überarbeitung der MepV und IvDV an den Europäischen Rechtsstandard angeglichen wurde. Neben dem Einhalten von Standards bei der Inverkehrbringung, um einer Zertifizierung zu genügen, verpflichtet nach allgemeiner Auffassung Annex I der EU MDR die Hersteller von Medizingeräten dazu, auch digitale Komponenten auf dem neuesten Stand zu halten, um die Cybersicherheit im Gesundheitsbereich kontinuierlich zu stärken. Die übereinstimmenden Aussagen unserer Gesprächspartner weisen gleichzeitig darauf hin, dass dies noch nicht ausreichend stattfindet. Hier wird eine grössere gesundheitspolitische Einwirkung des BAG gewünscht.

3.2.4 Überwachung und mögliche Sanktionen

Der Gesetzgeber sieht eine grosse Eigenverantwortlichkeit der Hersteller und Inverkehrbringer in der Compliance mit der MepV vor. Diese sorgen im Regelfall selbstständig für die Einhaltung der massgeblichen Vorgaben und lassen sich diese über Notified Bodies zertifizieren. Schweizer Hersteller müssen auf eine bezeichnete Stelle in der EU zurückgreifen, wenn sie ihre Produkte auch auf den europäischen Markt bringen wollen (eHealth Suisse, 2022). Wichtig für die Gewährleistung der Informationssicherheit und Datensicherheit sind dabei industriespezifische Normen. Swissmedic überprüft die technische Dokumentation, inklusive des Risikomanagements.

Zwar gewährt der Gesetzgeber Swissmedic und den Kantonen in Art. 75ff. in Verbindung mit Art. 66 HMG und Art. 93-95, 97 und 98 EU MDR weitgehende Kompetenzen zur Marktüberwachung, de facto reagieren diese allerdings primär auf Selbstmeldungen im Rahmen der Vigilanz der Hersteller und Spitäler (Art. 66-67 MepV) (Swissmedic - Schweizerisches Heilmittelinstitut, 2023).

Art. 74 MepV bestimmt die gesetzlichen Vorgaben zur Cybersicherheit von Medizinprodukten. Der Gesetzgeber verpflichtet dabei Gesundheitseinrichtungen, alle technischen und organisatorischen Massnahmen vorzunehmen, die nach dem Stand der Technik notwendig sind, um bei netzwerkfähigen Produkten den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen. Mit dieser Norm schafft der Gesetzgeber also eine doppelte Verantwortlichkeit für die Sicherheit von dGAs: Neben den Herstellern und Betreibern von Produkten im Rahmen ihrer allgemeinen und besonderen Sicherheits- und Leistungspflichten sind in der kritischen Infrastruktur Gesundheit *zusätzlich* auch alle Organisationen, deren Hauptzweck in der Versorgung oder Behandlung von Patienten oder der Förderung der öffentlichen Gesundheit besteht (vergleiche Art. 4 Abs. 1 lit. k MepV), verpflichtet, Massnahmen zur Cybersicherheit zu ergreifen.

Das Inverkehrbringen von Medizinprodukten, die nicht den gesetzlichen Anforderungen entsprechen, hat sowohl verwaltungsrechtliche als auch strafrechtliche Konsequenzen. Die einzelnen Vollzugsorgane, insbesondere Swissmedic, aber auch Kantone und Zollorgane, sind gestützt auf Art. 66 HMG befugt, mittels Verwaltungsmassnahmen nichtkonformen Medizinprodukten entgegenzuwirken. Darüber hinaus erfüllt das Inverkehrbringen von Medizinprodukten, die den gesetzlichen Anforderungen nicht entsprechen, den Straftatbestand von Art. 86 Abs. 1 Buchst. e HMG, der die betreffenden Widerhandlungen mit Gefängnis oder einer Geldstrafe bestraft.

Beim Einsatz nichtzertifizierter Medizinprodukte-Software drohen sowohl Herstellern wie auch Leistungserbringern haftungsrechtliche Konsequenzen gemäss den einschlägigen Bestimmungen des schweizerischen Obligationenrechts (Art. 41ff OR) sowie des PrHG. Im Bereich der Produktehaftpflicht ergeben sich in der Schweiz für digitale Produkte allerdings derzeit noch keine gesonderten Anforderungen. Eine Revision des PrHG ist aber zeitnah zu erwarten, da in der EU seit Ende 2022 ein Entwurf einer neuen, um digitale Produkte und Datenschäden erweiterte Produkthaftungsrichtlinie diskutiert wird (Das Schweizer Parlament, 2018).

Schlussfolgerungen:

Ohne Änderungen des Produktesicherheitsrechts oder Produktehaftpflichtrechts bleibt die Eigenverantwortlichkeit der Hersteller und Inverkehrbringer auch für Datenschutz und Cybersicherheit zentrale Doktrin. In den Interviews haben keine der Aufsichtsstellen grösseren Bedarf an aktiven Marktüberwachungsmitteln geäussert.

3.3 Was gilt spezifisch bezüglich Datenschutzes/Cybersicherheit für Apps im Bereich der dGA?

Auch Software, die für den Gebrauch in Mobiltelefonen oder Tablets entwickelt wurde, muss die oben beschriebenen Grundsätze des Datenschutzes und – so sie in einem relevanten Kontext eingesetzt werden oder als Medizinprodukt zu klassifizieren sind – der Cybersicherheit einhalten. In der Schweiz gibt es keine zusätzliche spezifische Regulierung. Allerdings ergibt sich laut Literatur, aber auch gemäss der Einschätzung der Aufsichtsstellen bei Apps, also reinen Software-Applikationen gewisse Grauzonen bei der Einordnung als Medizinprodukte (Leins-Zurmühle, 2021). Ob alle Apps, die als Medizinprodukte zu klassifizieren wären, also in jedem Fall die Richtlinien der EU MDR (und insbesondere Annex I) einhalten, ist fraglich. In unseren Interviews wurde hier von einem «Wildwuchs» von Grauzonenangeboten gesprochen.

Schlussfolgerungen:

Für Apps gelten dieselben rechtlichen Anforderungen wie für andere dGAs. Gemäss unseren Informationen ist hier aber unklar, ob alle Apps, die als Medizinprodukte klassifizierbar wären, auch die rechtlichen Grundlagen wirklich einhalten.

3.4 Wer hat in der Schweiz welche Aufsichtspflichten (Kantone, Bund etc.)?

Der digitale Raum ist ein Querschnittsthema, das sich nicht einer einzelnen Behörde zuteilen lässt. Dies gilt umso mehr für die Schweiz, in welcher die Aufgabenzuteilung ohnehin durch den Föderalismus geprägt ist. Obwohl digitale Interaktionen kaum territorial zu verorten sind, bleibt das verfassungsmässige Prinzip der föderalen Zuständigkeit auch im Digitalen bestehen. Auf dieser Grundlage haben Bund und Kantone ihre jeweiligen Organisationen entwickelt.

Im Bereich Datenschutz beaufsichtigt auf Bundesebene der EDÖB die Anwendung der bundesrechtlichen Datenschutzvorschriften (Art. 4 DSG). Der EDÖB ist die zuständige Behörde für den Datenschutz bei Datenbearbeitungen durch Private (zum Beispiel Unternehmen) sowie durch Bundesorgane. Datenbearbeitungen der kommunalen und kantonalen Behörden fallen in den Zuständigkeitsbereich der Datenschutzaufsicht der Kantone beziehungsweise Gemeinden (Art. 16 DSG). Die Verfolgung und die Beurteilung strafbarer Handlungen obliegen den Kantonen (Art. 65 Abs. 1 DSG).

Zuständig für die Kernaufgaben im Bereich Cybersicherheit sowie für die Koordination mit allen weiteren beteiligten Stellen ist das BACS. Betreiber kritischer Infrastrukturen – nach Art. 74b Abs. 1 lit. f-h auch im Gesundheitswesen – haben bei schwerwiegenden Cybervorfällen gemäss revidiertem Informationssicherheitsgesetz eine Meldepflicht an das BACS.

Das BACS übernimmt jedoch keine Aufsichts- oder Regulierungsaufgaben von den Fachbehörden in den Sektoren. Diese bleiben für die Zulassung und laufende operative Aufsichtstätigkeiten der Industrie und konzessionierte Unternehmen bezüglich sektorspezifischen Cybersicherheits-Vorgaben zuständig. Das BACS arbeitet direkt mit den Fachämtern zusammen und stellt ihnen Fachwissen zur Cybersicherheit zur Verfügung. In den rechtlichen Grundlagen der Organisationen wird präzisiert, welche Kompetenzen die zuständigen Stellen haben. Gleichzeitig sorgen die Verwaltungseinheiten untereinander, im durch das Recht gesetzten Rahmen, über einen laufenden Informations- und Erfahrungsaustausch für eine optimale Abstimmung und die Nutzung von Synergien.

Der Bereich der Cyberstrafverfolgung liegt primär in der Zuständigkeit der Kantone. Seitens des Bundes sind das Bundesamt für Polizei (fedpol) und die Bundesanwaltschaft zuständig.

Die Kantone definieren ihre Organisation der Cybersicherheit selbständig und angepasst an ihren Bedarf. Sie können sich dabei an der «Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation»

orientieren, welche vom Sicherheitsverbund Schweiz erarbeitet wurde und von der Kantonalen Konferenz der Kantonalen Justiz- und Polizeidirektoren im Jahr 2020 verabschiedet wurde (Sicherheitsverbund Schweiz, 2021).

Im Bereich der Medizinprodukte liegt die Zuständigkeit für die Marktüberwachung gemäss Art. 76 MepV bei Swissmedic im Bereich Konformitätsüberwachung, der Instandhaltung und Aufbereitung von Produkten in Spitälern oder für Spitäler beziehungsweise den Kantonen bei den Abgabestellen, den anwendenden Fachpersonen und in den übrigen Gesundheitseinrichtungen. Im Rahmen der Marktüberwachung sind auch die *zusätzlichen* Anforderungen im Bereich Cybersicherheit zu berücksichtigen.

Sofern das BAG Daten bearbeiten oder einsehen möchte, muss in Bezug auf digitale Gesundheitsprodukte ein Gesetz im formellen Sinn bestehen (Art. 34 Abs. 2 lit. b DSG). Dies dient dem Schutz des Rechts auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV, Art. 8 EMRK und Art. 17 UNO Pakt II). Dabei sind auch die Anforderungen an die Normdichte zu beachten, obwohl sie in Art. 34 DSG nicht explizit erwähnt sind. Als Stelle des Bundes darf das BAG gemäss Art. 62a HMG ausgewählte besonders schützenswerte Personendaten bearbeiten, sowie dies zur Erfüllung ihrer Aufgaben nach dem HMG erforderlich ist. Die MepV sieht keine gesonderte Datenbearbeitung des BAG bei Medizinprodukten vor, ausser, es würde von Swissmedic beauftragt (Art. 79 MepV).

Schlussfolgerungen:

Im Bereich Datenschutz liegt die Aufsichtspflicht bei Datenbearbeitungen von Privaten und Bundesorganen beim Bund (EDÖB), bei Datenbearbeitungen der kommunalen und kantonalen Behörden fallen bei der Datenschutzaufsicht der Kantone und Gemeinden. Die Verfolgung und die Beurteilung strafbarer Handlungen obliegen den Kantonen. Zuständig für die Kernaufgaben im Bereich Cybersicherheit sowie für die Koordination mit allen weiteren beteiligten Stellen ist das BACS. Betreiber kritischer Infrastrukturen – auch im Gesundheitswesen – haben bei schwerwiegenden Cybervorfällen eine Meldepflicht an das BACS.

Im Bereich der Medizinprodukte liegt die Zuständigkeit im Bereich Konformitätsüberwachung, der Instandhaltung und Aufbereitung von Produkten in Spitälern oder für Spitäler bei Swissmedic, bei den Abgabestellen, den anwendenden Fachpersonen und in den übrigen Gesundheitseinrichtungen bei den Kantonen. Das BAG ist hier bisher nicht als Aufsichtsbehörde vorgesehen.

3.5 Gesetzliche Verpflichtungen des BAGs und Versicherer : Haben das BAG oder die vergütenden Versicherer in der Überprüfung der entsprechenden Erfüllung der Anforderungen bezüglich Datenschutzes/Cybersicherheit gesetzliche Verpflichtungen?

Weder das Datenschutzrecht noch Massnahmen zur Cybersicherheit verpflichten das BAG, die Anforderungen bezüglich Datenschutzes oder Cybersicherheit zu überprüfen, da es keine Aufsichtsfunktion

für die Bereiche oder für Medizinprodukte wahrnimmt. Stattdessen hat sich das BAG selbst verpflichtet, Cybersicherheit und Datenschutz im Rahmen der Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit- (WZW) Prüfung zu subsumieren.

Gemäss Art. 32 Abs. 1 KVG müssen die Leistungen nach den Art. 25-31 KVG wirksam, zweckmässig und wirtschaftlich sein. Im Rahmen des Grundlagendokuments «Operationalisierung der Kriterien Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit» (Eidgenössisches Departement des Innern EDI - Bundesamt für Gesundheit BAG, 2022) hat das BAG (2022) festgelegt, dass im Kriterium Zweckmässigkeit auch rechtliche (Kapitel 2.3.4) und ethische (Kapitel 2.3.5) Fragen zu berücksichtigen sind. Kapitel 2.3.4 geht dabei explizit auf Datenschutz, Kapitel 2.3.5 explizit auf die Privatsphäre ein. Damit sind gemäss diesem BAG-eigenem Dokument Datenschutzrechtliche Aspekte zu prüfen. Dies gilt auch für den Bereich Cybersicherheit. Zwar lässt sich die Cybersicherheit wohl nicht unter dem Sicherheitsaspekt des Wirksamkeitskriteriums subsumieren, da die gesellschaftlichen Aspekte unter Kapitel 2.3.6 der WZW-Operationalisierung aber sowohl technologie-assoziierte Schaden- oder Sicherheitsrisiken als auch volkswirtschaftliche Kosten inkludieren, muss hier Cybersicherheit mitgedacht werden.

Da WZW als Anspruchsvoraussetzungen auf zwei Ebenen verstanden wird (Eidgenössisches Departement des Innern EDI - Bundesamt für Gesundheit BAG, 2022), wären gemäss WZW-Operationalisierung des BAG auch die Krankenversicherer im Sinne der Prüfung der Vergütungsvoraussetzung im konkreten Einzelfall verpflichtet, Datenschutz- und Cybersicherheitsrechtliche Aspekte zu prüfen.

Es ist wichtig zu betonen, dass auf Grund der sich ständig ändernden Sicherheitslage und technologischen Weiterentwicklung weder Datenschutz noch Cybersicherheit generisch oder abschliessend geprüft werden können. Art. 32 Abs. 2 KVG sieht zwar eine «periodische» Überprüfung vor, aber auch diese kann keine allgemeingültigen Aussagen zu Datenschutz und Cybersicherheit einzelner Produkte treffen, vor allem dann nicht, wenn es um die generische Umschreibung einer Position im Rahmen der Mittel- und Gegenständeliste (MiGeL) geht. Dies liegt insbesondere daran, dass die Bewertung über die Sicherheit eines Produktes auf den konkreten Kontext ihrer Anwendung in einer Informationsinfrastruktur ankommt, es also einer kontextspezifischen Risikoabschätzung bedarf. Dies ist pauschal für das BAG nicht prüfbar.

Denkbar wäre eher, dass im Rahmen der WZW-Prüfung Vulnerabilitäten oder Risiken im Bereich Datenschutz und Cybersicherheit festgestellt werden, die analog zu den bestehenden Limitationen aufgenommen werden könnten. Diese könnten dann den Versicherern als Grundlage für die Prüfung der Vergütungsvoraussetzung im konkreten Einzelfall dienen.

Schlussfolgerungen:

Die BAG-eigene Operationalisierung der WZW-Prüfung nach Art. 32 Abs. 1 KVG verpflichtet das BAG, generisch die Cybersicherheit und Datenschutz eines Medizinproduktes zu überprüfen. Dies erscheint auf Grund des Lebens- und Risikozyklus von dGA aber unrealistisch.

Denkbar ist eher, dass bei der Aufnahme einer generischen Produktbeschreibung bekannte Risiken analog zu den bestehenden Limitationen aufgenommen werden.

Konkret könnten solch generische Limitationen dreierlei Vermerke für dGA in einer Position beinhalten

(1) Ein Hinweis, dass schützenswerte Daten bearbeitet werden und hier also der Datenschutz gewährleistet sein muss (dies könnte analog zum "hohen Risiko" in der Datenschutzfolgeabschätzung abgefragt werden);
(2) Ein Hinweis zur Verwendung im Informationsnetzwerk kritischer Infrastrukturen (hier: insbesondere Spitälern), was ein besonderes Risikomanagement im Bereich Cybersicherheit voraussetzt (dies könnte analog zu den Mindestanforderungen von Medizinprodukten aus dem Leitfaden von H+ (o.J.) entnommen werden);
(3) Ein Hinweis auf die Notwendigkeit des kontinuierlichen Supports im Bereich Cybersicherheit und Datenschutz basierend auf Annex I des EU MDR. Ein nicht mehr oder nur unzureichend unterstütztes Produkt, auf das a) oder b) zutrifft, sollte nicht vergütet werden.

3.6 Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit: Wie muss der Hersteller/Entwickler die WZW seines Produktes hinsichtlich Erfüllung der in der Schweiz geltenden Anforderungen an Datenschutz und Cybersicherheit beweisen und dokumentieren?

Die Anforderungen an den Datenschutz sind in der EU in der DSGVO und in der Schweiz im nationalen DSG und den kantonalen Datenschutzgesetzen geregelt. Weiterhin unterliegen Hersteller den Anforderungen des PrHG, die Hersteller haftbar machen, wenn das Produkt fehlerhaft ist oder wenn es nicht die Sicherheit bietet, die man unter Berücksichtigung aller Umstände zu erwarten berechtigt ist. Dies beinhaltet unter anderem die Gewährleistung von Cybersicherheit. Bei Medizinprodukten werden Cybersicherheitsrisiken zusätzlich über den risikobasierten Ansatz abgedeckt und dokumentiert. In der MepV wird die Bedeutung der Cybersicherheit für Medizinprodukte hervorgehoben und die Grundlegende Sicherheits- und Leistungsanforderungen (GSPRs) enthalten spezifische Anforderungen an Software und IT-Sicherheit. Die MepV verlangt insbesondere, dass Hersteller ihre Produkte gemäss dem Stand der Technik entwickeln und herstellen, unter Berücksichtigung von Risikomanagementprinzipien, einschliesslich der Informationssicherheit. Diese Anforderungen gelten für alle medizinischen Geräte, die

elektronische programmierbare Systeme und Software enthalten. Arzneimittel, die eine Softwarekomponente enthalten, müssen im Zulassungsprozess eine Stellungnahme einer benannten Stelle zum Medizinprodukteteil einbringen und somit die gleichen Anforderungen wie bei Medizinprodukten erfüllen.

Im Grundlagendokument des BAGs zur «Operationalisierung der WZW-Kriterien gemäss Art. 32 KVG» werden im Rahmen der Prüfung der Zweckmässigkeit, rechtliche Aspekte spezifiziert (Eidgenössisches Departement des Innern EDI - Bundesamt für Gesundheit BAG, 2022). Diese rechtlichen Aspekte umfassen unter anderem die Überprüfung des Datenschutzes, der eng mit Cybersicherheit verknüpft ist. Zurzeit werden vom BAG bei der Überprüfung des Datenschutzes/Cybersicherheit bei Aufnahmeanträgen für Allgemeine Leistungen, für die MiGeL, die AL (Analysenliste) sowie die SL (Spezialitätenliste) keine weiteren Dokumente oder Unterlagen eingefordert. Für die Inverkehrbringung von Medizinprodukten oder IVD und die Zulassung eines Arzneimittels müssen jedoch Nachweise für die Erfüllung von Qualität und Leistung erbracht werden. Hier gilt grundsätzlich – also auch für die Daten- und Informationssicherheit und das Risikomanagement– die Konformitätsvermutung. Eine EU-Konformitätserklärung dürfte also Dokumentation für die WZW-Prüfung bei Inverkehrbringung ausreichend sein, insbesondere da Swissmedic und nicht das BAG für die Marktüberwachung zuständig ist. Datenschutzanforderungen werden im Rahmen der MepV nicht im Detail geprüft. Hier könnte das BAG weitere Anforderungen spezifizieren und prüfen, etwa analog zur Beurteilung des hohen Risikos. Alternativ könnte dies ähnlich wie die Digitale Gesundheitsanwendungen-Verordnung (DiGAV) in Deutschland Themenfelder, wie Einwilligung, Zweckbindung, Datenminimierung und Angemessenheit, Integrität und Vertraulichkeit, Richtigkeit, Erforderlichkeit, Datenportabilität, Informationspflichten, Datenschutz-Management, Datenschutz-Folgenabschätzung und Risikomanagement, Nachweispflicht, Verarbeitung im Auftrag, Datenweitergabe an Dritte oder Verarbeitung im Ausland umfassen.

Schlussfolgerungen:

Im Rahmen der Inverkehrbringung eines Medizinproduktes verfolgt der Hersteller einen risikobasierten Ansatz, der auch Cybersicherheit abdeckt. Das BAG sollte sich auf die Bescheinigungen und die EU-Konformitätserklärungen (CE-Kennzeichnung) verlassen können, dass die Anforderungen an die Cybersicherheit gewährleistet sind. Darüber hinaus ist Swissmedic für die Marktüberwachung zuständig.

Die Datenschutzthematik wird im Rahmen des HMGs nicht geregelt und liegt auch nicht grundsätzlich im rechtlichen Zuständigkeitsbereich des BAG. Falls das BAG diese im Rahmen ihrer eigenen WZW-Operationalisierung für vergütete Produkte durchsetzen möchte, könnte es die Risikoabschätzung analog zur Prüfung des hohen Risikos in der Datenschutzfolgeabschätzung abfragen. Alternativ würde es sich anbieten, Nachweise für die Themenfelder Einwilligung, Zweckbindung, Datenminimierung und Angemessenheit, Integrität und Vertraulichkeit, Richtigkeit, Erforderlichkeit, Datenportabilität, Informationspflichten, Datenschutz-Management, Datenschutz-Folgenabschätzung und Risikomanagement, Nachweispflicht, Verarbeitung im Auftrag, Datenweitergabe an Dritte oder Verarbeitung im Ausland einzufordern.

3.7 Unterlagen zu Datenschutz/Cybersicherheit: Welche sind öffentlich verfügbar, welche kann das BAG von den Herstellern einfordern?

Einsicht in die detaillierten Unterlagen zu Datenschutz/Cybersicherheit erhalten in der Regel die Notified Bodies und Swissmedic gegebenenfalls im Rahmen des Notifizierens beim Inverkehrbringen sowie Swissmedic und die Kantone bei der Marktüberwachung. Die EU-Konformitätserklärung kann prinzipiell eingefordert werden.

Sowohl Europäische als auch schweizerische Initiativen zur Erstellung von Datenbanken von Medizinprodukten sind im Aufbau (eudamed und swissdamed). Sie sollen grundsätzlich Informationen auch der Öffentlichkeit zur Verfügung stellen und auch (Re-)Zertifizierungen und Lebenszyklusabschätzungen möglich machen. Dies sollte insbesondere im Bereich der Cybersicherheit für mehr Transparenz sorgen.

Swissmedic veröffentlicht neben Berichten zur Marktüberwachung alle Sicherheitskorrekturmassnahmen, mit denen Hersteller Probleme mit Medizinprodukten und deren Behebung kommunizieren[1]. Gemäss Swissmedic werden aber insgesamt nur wenige Sicherheitsmängel kommuniziert.

Wichtig dabei zu verstehen ist, dass Informations- und Datensicherheit nicht statisch sind und sich nur begrenzt anhand von Dokumenten oder Zertifikaten ablesen lassen. Dies ist Grundlage der Cybersicher-

[1] Siehe https://fsca.swissmedic.ch/mep/#/

heit und wurde von vielen Gesprächspartnern wiederholt betont. Alle dGAs, gleich welcher Art, bedürfen regelmässiger Softwareupdates. Diese können bestehende Sicherheitslücken beheben, aber auch neue schaffen. Hersteller verfügen häufig über zugängliche Update-Logs, die Auskunft über Art, Häufigkeit und Ausmass der Updates geben und möglicherweise ein aussagekräftigeres Bild über die ordnungsgemässe Betreibung von dGA geben können als einmalige Zertifizierungen bei Inverkehrbringung. Da das BAG hier allerdings keine Aufsichtspflichten hat, ist unklar, auf welcher Rechtsgrundlage es von Herstellern zusätzliche Informationen einfordern kann. Anders ist dies im Fall von Swissmedic oder den Kantonen (Art. 79 MepV in Verbindung mit Art. 16 MepV).

Schlussfolgerungen:

Während bei zertifizierten dGA die Konformitätsvermutung gilt, sind Dokumente über den Lebenszyklus von dGA schwerer zu erlangen. Die Datenbanken eudamed und swissdamed könnten hier Abhilfe schaffen.

3.8 Kontinuierliche Weiterentwicklung: Wenn neue Versionen (nach Updates) zusätzliche Funktionen aufweisen, müssten diese erneut auf WZW geprüft werden?

Grundsätzlich ist zwischen verschiedenen möglichen Änderungen der dGAs zu unterscheiden: (1) Änderungen in den Funktionen für den Nutzer, (2) Sicherheitsupdates und (3) Änderungen hinsichtlich Cybersicherheit und Datenschutz.

Eine Nutzungsänderung ist aktuell nicht offensichtlich prüfbar. Dies soll sich zumindest im Europäischen Recht mit der Einführung der GPSR ändern, wo auch digitale Veränderungen von Produkten unter Umständen eine veröffentlichungspflichtige Herstellermeldung erfordern. Bei Änderungen der Funktionen für den Nutzer, das heisst den Patienten oder den Leistungserbringer, ist zu überprüfen, ob die dGA überhaupt noch die in der KLV Anhang 1, SL, AL oder MiGeL definierten Anforderungen erfüllt. Wenn nicht, ist das Produkt nicht mehr leistungspflichtig in der obligatorischen Krankenpflegeversicherung (OKP), wenn ja, ändert sich erst einmal nichts. Denkbar ist etwa, dass Hersteller selbst ein neues Antragsverfahren zum Erhalt eines höheren Preises oder angepasster Indikation/Limitation anstreben. Wenn es sich um das Einspielen von Sicherheitsupdates handelt, gehört dies zu den laufenden Aktivitäten der Hersteller im Rahmen des Risikomanagements. Dieses ist nach allgemeiner Auffassung zwingend notwendig und Teil des Lebenszyklus eines Medizinproduktes. Ändert sich die Zweckmässigkeit des Produktes grundsätzlich, kann es sein, dass ein Produkt beispielsweise nicht mehr die Anforderungen der MiGeL erfüllt und somit nicht mehr unter die MiGeL-Position fällt. Diese Überprüfung obliegt den Krankenkassen, ist aber praktisch dadurch erschwert, das spezifische Produkte in spezifischen Anwendungskontexten Schwachstellen im Bereich Datenschutz oder Cybersicherheit aufweisen können, die MiGeL aber nur generische Positionen beschreibt.

Denkbar wäre es aber, über die Limitationen der generischen Positionen Hinweise für die Beendigung der Vergütung zu geben. So könnten zum Beispiel Produkte, bei denen ein hohes Risiko durch die Verarbeitung und den Austausch besonders schützenswerter Daten oder den Einsatz im Kontext kritischer Infrastrukturen besteht und deren Software nicht mehr regelmässig aktualisiert wird von der Vergütung ausgeschlossen werden.

Schlussfolgerungen:

Falls die dGAs neue Funktionen aufweisen, führt dies nicht automatisch zu einer neuen Prüfung der WZW-Kriterien, insbesondere wenn es sich um zusätzliche Funktionen handelt. Falls ein Hersteller eine höhere Vergütung oder angepasste Limitation dafür anstrebt, wird dies einen neuen Antragsprozess nach sich ziehen.

Sicherheitsupdates gehören zum normalen Risikomanagement eines digitalen Medizinprodukts und führen nicht zu einer erneuten Zertifizierung und es ist nicht davon auszugehen, dass das BAG dies noch einmal prüfen müsste.

Änderungen im Cybersicherheit und Datenschutz kann die Zweckmässigkeit ändern. Dabei handelt es sich um produktspezifische Änderungen, deren Überprüfung durch die Krankenkassen erfolgen muss. Hier können die Limitationen der generischen Produktbeschreibung Hinweise geben, zum Beispiel im Bereich «state of the art» nach Annex I EU MDR.

3.9 Was sind die aktuellen Herausforderungen für den Gesetzgeber?

Viele der Regelungen im Bereich Cybersicherheit und Datenschutz sind noch sehr neu, oder treten erst im Laufe des Jahres in Kraft. Über ihre Auswirkungen auf dGA und möglicherweise resultierender Nachsteuerungsbedarf lässt sich noch keine verlässliche Aussage treffen. Allerdings erwarten viele unserer Interviewpartner, dass es hier entweder durch Gerichtsurteile oder Gesetzesrevisionen Konkretisierungen geben wird, da es zum Beispiel im Bereich der Interoperabilität von dGA und der Datensicherheit in Verbindung mit der ärztlichen Schweigepflicht offene rechtliche Fragen geben könnten.

Absehbar werden aber vor allem Fragen der rechtlichen Harmonisierung des Schweizer mit dem Europäischen Rechtsraum zentral bleiben. Dies gilt sicherlich für die an verschiedenen Stellen erwähnte Einführung des horizontalen Produktsicherheitsrechts, der GPSR, in der EU. Bereits erwähnt wurde auch die Erweiterung der Produktehaftlicht auf digitale Produkte mit der Einführung eigener Schadensbegriffe für Datenschäden. Hier hat das Europäische Parlament im März 2024 einem gemeinsamen Gesetzesentwurf zugestimmt und dem Europäischen Rat zur Genehmigung und Veröffentlichung vorgelegt, was ein Inkrafttreten ab 2026 wahrscheinlich macht. Da das schweizerische Produktehaftlichtrecht bislang keine digitale Komponente hat, ist hier eine Revision fast unumgänglich.

Die Regulierung der Künstlichen Intelligenz (KI) wird zeitnah ein Thema auch in der schweizerischen Gesetzgebung sein. Am 9. Dezember 2023 haben die Europäischen Institutionen eine provisorische Ei-

nigung zum EU AI-Act erreicht, der die Anwendung KI in Produkten regulieren soll (European Parliament, 2023), auch hier ist von einem Inkrafttreten ab 2026 zu rechnen. Viele dGA werden hiervon betroffen sein. Für solche Produkte fordert der EU AI-Act eine eigene Konformitätsbewertung vor Marktzulassung, das Vorhandensein eines Qualitäts- und Risikomanagementsystems und die Marktüberwachung. Die Übernahme oder Angleichung des schweizerischen Rechts wird in diesem Bereich in den nächsten Jahren diskutiert werden.

Schliesslich ist nicht auszuschliessen, dass auf Grund der Komplexität und relativen begrifflichen Offenheit der DSG-Entscheidungen in Streitverfahren weiteren regulatorischen Konkretisierungs- oder Nachbesserungsbedarf offenlegen. Dies kann Folgen für die Herstellung und den Betrieb von dGA haben.

4 Handlungsempfehlungen

Ziel dieses Fachberichtes war es, spezifische Fragestellungen zu dGAs und insbesondere deren Herausforderungen im Bereich Datenschutz sowie der Cybersicherheit zu beantworten. Darauf aufbauend wurden Empfehlungen für die Verwaltung und weitere Stakeholdergruppen entwickelt, die entweder eher einen kurzfristigen Zeithorizont (0-3 Jahre) oder langfristigen Zeithorizont haben (grösser als 3 Jahre).

4.1 Empfehlungen mit kurzfristigem Zeithorizont

4.1.1 Transparente und offene Kommunikation

Während Datenschutz und Cybersicherheit in IT-Fachkreisen seit Jahrzehnten wichtige Themen sind, haben regulatorische Anpassungen vor allem im Gesundheitsbereich erst in den letzten Jahren stattgefunden. Bislang existiert eine komplexe und von Partikularperspektiven geprägte Landschaft. Dem BAG kommt die besondere Rolle zu, die Bedeutung der verwandten Themen Cybersicherheit und Datenschutz im Gesundheitsbereich zu betonen und von Herstellern wie auch Anwendern einzufordern, ohne den Hauptzweck des Gesundheitswesens aus den Augen zu verlieren. Unsere Interviews zeigen, dass bei den verschiedenen Stakeholdern Unsicherheiten bezüglich Einordnung, Vergütung, Verantwortlichkeiten und weiteren Aspekten bestehen.

Die meisten Stakeholder zeigten sich offen und interessiert an einem Austausch mit der Verwaltung mitzuwirken. Dieser könnte zum Beispiel im Rahmen eines moderierten Stakeholderworkshops des BAGs durchgeführt werden. Die Ausgestaltung eines solchen Workshops und auch der spezifische Beitrag der Stakeholder müsste im Weiteren noch definiert werden. Teile dieses Berichtes könnten für die Vorbereitung eine Grundlage bilden.

4.1.2 Gesetzliche Anpassungen

Basierend auf den Analysen sehen wir keinen Änderungsbedarf auf Gesetzes- und Verordnungsebene des HMG sowie des KVG mit KVV und KLV. Dies ist unter anderem darauf zurückzuführen, dass die Schweiz im Bereich der Medizinprodukte aber auch im Bereich des Datenschutzes sehr eng mit der EU verwoben ist. Eine Änderung im Bereich der Cybersicherheit oder des Datenschutzes auf Schweizer Seite, bedeutet daher für Hersteller eine zusätzliche Anforderung und könnte negative Implikationen auf die Versorgungssicherheit als auch auf den Zugang zu neuartigen Technologien haben. Darüber hinaus würden allfällige Marktrückzüge die Kostendämpfungsbemühungen des BAGs konterkarieren. Schweiz-spezifische Änderungen sind daher möglichst zu vermeiden und die gesundheitspolitisch wichtige Harmonisierung der Regularien auch ohne Rahmenabkommen zu gewährleisten. Dies betrifft insbesondere die GPSR und NIS-2. Die erforderlichen Änderungen können unserer Einschätzung nach auf Prozessebene und durch Anpassungen von amtlichen Dokumenten erreicht werden. Ausserhalb des gesundheitspolitischen Spektrums werden gesetzliche Anpassungen an die EU-Gesetzgebungen zur KI und digitaler Produktehaftpflicht bis 2026 notwendig sein.

4.1.3 Anpassungen an den Prozessen und amtlichen Dokumenten

Das Grundlagendokument *Operationalisierung der Kriterien «Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit»* inkludiert bereits explizit den Datenschutz und nach unserer Lesart auch Cybersicherheit. Gleichzeitig ist dieses Dokument das einzige, dass dem BAG eine Aufsichtspflicht in diesem Bereich zuweist. Sollten die Aspekte der Cybersicherheit und des Datenschutzes integraler Bestandteil der WZW sein, wäre es daher wichtig, in dem Dokument eine methodische Ergänzung vorzunehmen, die darlegt, wie diese Elemente in den Prüfprozess einbezogen werden können.

Bei der Aufnahme einer generischen Produktebeschreibung könnten bekannte Risiken analog zu den bestehenden Limitationen vermerkt werden:

(1) ein Hinweis, dass schützenswerte Daten bearbeitet werden und hier also der Datenschutz gewährleistet sein muss (dies könnte analog zum "hohen Risiko" in der Datenschutzfolgeabschätzung abgefragt werden);
(2) ein Hinweis zur Verwendung im Informationsnetzwerk kritischer Infrastrukturen (hier: insbesondere Spitälern), was ein besonderes Risikomanagement im Bereich Cybersicherheit voraussetzt (dies könnte analog zu den Mindestanforderungen von Medizinprodukten aus dem Leitfaden von H+ (o. J.) entnommen werden);
(3) ein Hinweis auf die Notwendigkeit des kontinuierlichen Supports im Bereich Cybersicherheit und Datenschutz basierend auf Annex I der EU MDR. Ein nicht mehr oder nur unzureichend unterstütztes Produkt, auf das a) oder b) zutrifft, sollte nicht vergütet werden.

Wir empfehlen, spezifische Fragen in Abstimmung mit dem BACS (Cybersicherheit) bzw. EDÖB (Datenschutz) zu erarbeiten. Die entwickelten spezifischen Fragen sind dann auch in den folgenden Antragsformularen zu ergänzen:

- *Antrag auf Kostenübernahme durch die OKP betreffend Leistungen*
- *Antrag auf Aufnahme des folgenden Produktes auf MiGeL oder Anpassung der folgenden Position in der MiGeL*
- *Antrag auf Neuaufnahme einer Analyse in die Analysenliste oder auf Änderung einer in der AL bereits aufgeführten Analyse*
- *Checklisten auf Neuaufnahmegesuche von Arzneimitteln (Anhang 01a-h sowie 03a-f und 03m)*

Grundsätzlich empfehlen wir die bestehenden Antragsprozesse und -dokumente zu präzisieren, so dass sie den dGAs besser gerecht werden. Wir empfehlen dabei, ähnlich wie bei den bestehenden WZW-Prüfungspunkten, zum Beispiel Prüfung des Vorliegens einer Konformitätserklärung, vor allem auf Selbstdeklarationen und auf die Verantwortung der Hersteller im gesamten Produktlebenszyklus zu set-

zen. Dies da Zertifikate und Erklärungen ohne genaue Analyse des Einsatzbereiches und Umfeldes wenig aussagekräftig sind. Dabei sollte auch auf eine Beschleunigung der Antragsprozesse hingearbeitet werden. Dafür wäre ein Aufbau zusätzlicher Kompetenzen und Ressourcen beim BAG zu prüfen.

4.2 Empfehlungen mit langfristigem Zeithorizont

4.2.1 Stakeholderkommunikation und Öffentlichkeitsarbeit

Cybersicherheit und Datenschutz sind Themen, die sich ständig weiterentwickeln werden und nicht einmalig gelöst werden können. Daher empfehlen wir, einen kontinuierlichen Austausch zwischen der Bundesverwaltung, Kantonen und den verschiedenen Stakeholdern zu organisieren. Ein solcher Austausch könnte zum Beispiel im Rahmen regelmässiger Round Tables stattfinden. Möglich wäre auch die Schaffung eines neuen gesundheitssektorspezifischen Zentrums für Informationsaustausch und Analyse (ähnlich dem Information Sharing and Analysis Center [ISAC] der EU) oder auch die Integration in bestehende Strukturen, zum Beispiel eHealth Suisse. Dabei ist darauf zu achten, dass bestehende Gefässe und Initiativen genutzt werden und keine Doppelstrukturen aufgebaut werden.

4.2.2 Nach kantonalem Recht zugelassene Abgabestellen

Die Zulassungsbedingungen von Abgabestellen sind kantonal unterschiedlich geregelt. Während Abgabestellen von physischen Produkten, normalerweise ihre Produkte regional sehr begrenzt abgeben, können kantonale Abgabestellen von dGAs ohne Hürden schweizweit agieren. Abgabestellen von dGA haben daher den Anreiz, sich in Kantonen mit niedrigen Zulassungsbedingungen und tendenziell schwacher Aufsicht niederzulassen. Von dort können sie Patienten aus allen Kantonen bedienen, ohne dass diese Kantone auf die Struktur- und Prozessqualität Einfluss nehmen können. Wir empfehlen daher, dass sich die Kantone auf gemeinsame, einheitliche Cybersicherheits- und Datenschutzstandards für nach kantonalem Recht zugelassene Abgabestellen einigen, um einen einheitlichen Schutz der Bevölkerung zu gewährleisten.

4.2.3 Entwicklung weiterer Leitlinien

Die Interviews haben gezeigt, dass grosse Unsicherheit im Umgang mit den Themen Cybersicherheit und Datenschutz vorherrscht und, dass es Informationsbedarf bei den Mitgliedern der Verbände der Leistungserbringer, der Hersteller und Versicherer gibt. Wir empfehlen den Verbänden, Instrumente zu entwickeln, ihre Mitglieder über die gesetzlichen Vorgaben im Bereich Cybersicherheit und Datenschutz zielgruppengerecht zu informieren.

5 Literaturverzeichnis

Angerer, A., Hollenstein, E., & Russ, C. (2021). *Der Digital Health Report 21/22. Die Zukunft des Schweizer Gesundheitswesens*. ZHAW School of Management and Law.

Backer-Heuveldop, A., Crookes, J., Große Dütting, D., Rüdlin, M., Schütze, B., & Spyra, G. (2022). *Mobile Apps im Gesundheitswesen: Anforderungen aus dem Datenschutz*.

Bundesamt für Gesundheit BAG. (o. J.-a). *Analysenliste (AL)*. Abgerufen 1. Dezember 2023, von https://www.bag.admin.ch/bag/de/home/versicherungen/krankenversicherung/krankenversicherung-leistungen-tarife/Analysenliste.html

Bundesamt für Gesundheit BAG. (o. J.-b). *Mittel und Gegenständeliste (MiGeL)*. Abgerufen 1. Dezember 2023, von https://www.bag.admin.ch/bag/de/home/versicherungen/krankenversicherung/krankenversicherung-leistungen-tarife/Mittel-und-Gegenstaendeliste.html

Bundesamt für Gesundheit BAG. Direktionsbereich Kranken- und Unfallversicherung. (2022). *Faktenblatt. Vergütung von digitalen Gesundheitsanwendungen im Rahmen der OKP*.

Bundesministerium für Gesundheit. (2022, Oktober 31). *Was sind Medizinprodukte?* https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/medizinprodukte/definition-und-wirtschaftliche-bedeutung

Der Schweizerische Bundesrat. (2021). *Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV)*.

eHealth Suisse. (2022a). *Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer. Praktische Hinweise.*

eHealth Suisse (Hrsg.). (2022b). *Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer. Praktische Hinweise.*

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. (2023a). *Merkblatt zur Datenschutz-Folgenabschätzung (DSFA) nach den Art. 22 und 23 DSG*.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. (2023b, November 21). *Das neue Datenschutzgesetz aus Sicht des EDÖB*. https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/2021/20210305_ndsg_sicht_edoeb.html

Eidgenössisches Departement des Innern EDI - Bundesamt für Gesundheit BAG (Hrsg.). (2022). *Operationalisierung der Kriterien „Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit" nach Artikel 32 des Bundesgesetzes über die Krankenversicherung (KVG)*. https://www.bag.admin.ch/bag/de/home/versicherungen/krankenversicherung/krankenversicherung-bezeichnung-der-leistungen.html

EIT.swiss. (o. J.). *Neues Datenschutzgesetz (DSG) ab 1.9.2023*. Abgerufen 15. Januar 2024, von https://www.eit.swiss/de/neues-datenschutzgesetz-dsg-1-1

European Commission. (o. J.). *General Product Safety Regulation*. Abgerufen 1. Februar 2024, von https://commission.europa.eu/business-economy-euro/product-safety-and-requirements/product-safety/general-product-safety-regulation_en

European Commission. (2017). *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"*. https://www.datenschutz-bayern.de/technik/orient/wp248.pdf

European Data Protection Board. (2020). *Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Version 2.0*.

European Parliament. (2023, Dezember 9). *Artificial Intelligence Act: Deal on comprehensive rules for trustworthy AI*. https://www.europarl.europa.eu/news/en/press-

room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

FMH – Verbindung der Schweizer Ärztinnen und Ärzte. (2023). *Leitfaden Verzeichnis der Bearbeitungstätigkeiten*. https://www.fmh.ch/files/pdf28/leitfaden-verzeichnis-der-bearbeitungstaetigkeiten.pdf

Grell, A.-S. (2021, September 1). *SaMD versus MDSW: what's the difference between Software as a Medical Device and Medical Device Software?* https://qbdgroup.com/en/blog/samd-mdsw-difference

H+ Die Spitäler der Schweiz. (o. J.). *Informationssicherheit und Datenschutz Anforderungen zur ICT-Sicherheit von Fremdsystemen. Version 1.2*. https://www.hplus.ch/fileadmin/hplus.ch/public/Politik/Cyber_Security/Leitfaden_Cyber_Security_D.pdf

Isler, M., & Bichsel, B. (2021, April 21). *Software/Apps als Medizinprodukte. Was gilt ab 26. Mai 2021?*

Johner Institut. (o. J.). *Benannte Stellen: Aufgaben und Rechte*. Abgerufen 24. November 2023, von https://www.johner-institut.de/blog/tag/benannte-stellen/

Kanzlei.biz. (2024, Januar 4). *Entscheidung über Schadensersatz wegen des Facebook-Datenlecks*. https://www.kanzlei.biz/entscheidung-ueber-schadensersatz-wegen-des-facebook-datenlecks-12-01-2024/

Lang, M. (2024, Januar 11). Privacy by Design: Umsetzungstipps für die Praxis. *Datenschutz Praxis*. https://www.datenschutz-praxis.de/datenschutzbeauftragte/privacy-by-design-umsetzungstipps-fuer-die-praxis/

Leins-Zurmühle, S. (2021). Mobile Applikationen als Medizinprodukte. *Life Science Recht*, *3*(2021).

Medical Device Coordination Group. (2019a). *MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices*. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

Medical Device Coordination Group. (2019b). *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR*.

MedTech Europe. (2023). *Position Paper. MedTech Europe's vision for cybersecurity in the medical technology ecosystem*. https://www.medtecheurope.org/wp-content/uploads/2023/05/medtech-europe-cybersecurity-position-paper-1.pdf

Nationales Zentrum für Cybersicherheit (NCSC). (2023). *Nationale Cyberstrategie (NCS)*.

Schweizerische Eidgenossenschaft. (o. J.). *Eidgenössische Kommission für Analysen, Mittel und Gegenstände (EAMGK)*. Abgerufen 8. Januar 2024, von https://www.admin.ch/ch/d/cf/ko/Gremien_interessenbindung_10587.html

Sicherheitsverbund Schweiz. (2021). *Empfehlung für die Umsetzung zur kantonalen Cyber-Organisation.* https://www.svs.admin.ch/content/svs-internet/de/themen-/cybersicherheit/cybersicherheit-kantone/_jcr_content/contentPar/tabs/items/441_1612790888827/tabPar/downloadlist_1137108/downloadItems/303_1615194437757.download/Empfehlung%20Cyber-Organisation.pdf

Swissmedic - Schweizerisches Heilmittelinstitut. (o. J.-a). *Bezeichnete Stellen*. Abgerufen 24. November 2023, von https://www.swissmedic.ch/swissmedic/de/home/medizinprodukte/regulierung-medizinprodukte/konformitaetsbewertungsstellen.html

Swissmedic - Schweizerisches Heilmittelinstitut. (o. J.-b). *Swissmedic—Schweizerisches Heilmittelinstitut*. Abgerufen 1. November 2023, von https://www.swissmedic.ch/swissmedic/de/home/ueber-uns/swissmedic--schweizerisches-heilmittelinstitut.html

Swissmedic - Schweizerisches Heilmittelinstitut. (2021). *Merkblatt Medizinprodukte-Software*.

Swissmedic - Schweizerisches Heilmittelinstitut. (2023, Juli). *Nachgeforscht. Wenn eine App ein MEP ist. Eine Sache der Hersteller.* https://www.swissmedic.ch/swissmedic/de/home/ueber-uns/publikationen/visible/visible-single-page.spa.v7.app/de/nachgeforscht.html

TÜV Süd. (o. J.). *EU-Medizinprodukteverordnung (MDR)*. Abgerufen 1. November 2023, von https://www.tuvsud.com/de-de/branchen/gesundheit-und-medizintechnik/marktzulassung-und-zertifizierung-von-medizinprodukten/mdr-medizinprodukteverordnung-eu

Vollebregt, E. (2020, März 16). *The MDCG cybersecurity guidance – a helpful rush job*. https://www.axonlawyers.com/the-mdcg-cybersecurity-guidance-a-helpful-rush-job-2/

Wenner, H. (2023, Juli 28). *Cybersecurity von Medizinprodukten als Teil der IT-Sicherheit im Gesundheitswesen*. https://www.vde.com/topics-de/health/beratung/cybersecurity-medizinprodukte-it-sicherheit-gesundheitswesen

6 Anhang

6.1 Interviewleitfaden

Administratives

Projekt:	Digitale Gesundheitswendungen Standortbestimmung und Datenschutzvorgaben/Cybersicherheit
Template:	Interview-Guide
Zielgruppe:	_____
Expert/in:	_____
Organisation:	_____
Durchgeführt von:	_____
Datum:	_____
Filename Ton-Datei:	_____

Einleitung

- ☐ Vorstellung Interviewer (Rolle im Projekt etc.):
- ☐ Dies ist ein Projekt des KPM/Institut für öffentliches Recht im Auftrag des Bundesamtes für Gesundheit (BAG)
- ☐ Zweck des Interviews
- ☐ Aufzeichnung? Ja/nein (entsprechendes unterstreichen/einkreisen) – Interview wird nach Projektende wieder gelöscht.
- ☐ Dank im Voraus (für Zeit, Teilnahme und offene und möglichst ehrliche Antworten)
- ☐ Check, ob Mikrofon/Aufnahmegerät läuft
- ☐ Können Sie sich bitte kurz vorstellen? (heutige Rolle, sonstige Tätigkeiten, Ausbildung, o. ä.)

Datenschutz/Cybersicherheit

Fragen	Validierung/ Explorativ	Interviewpartner
1.1 Recht Schweiz: Was sind die rechtlichen Grundlagen in der Schweiz?		
1.1.1 Welche Unterlagen zu Datenschutz/Cybersicherheit sind öffentlich verfügbar, welche kann das BAG von den Herstellern einfordern? *Verwaltung (Swissmedic/Kantone): Sind Informationen aus Marktüberwachung von Swissmedic/Kantonen verfügbar? Können gegebenenfalls auch weitere Unterlagen unabhängig vom Antragssteller eingeholt werden?* *Leistungsanbieter: Was für Unterlagen können angeboten werden?*	Validierung	Swissmedic/Kantone/Swiss Medtech/SVDI/Interpharma
1.1.2 Wer hat in der Schweiz welche Aufsichtspflichten (Kantone, Bund, etc.)?		
1.1.3 Haben das BAG oder die vergütenden Versicherer in der Überprüfung der entsprechenden Erfüllung der Anforderungen bezüglich Datenschutzes/Cybersicherheit gesetzliche Verpflichtungen? *--> s. Ordnungsmodell.*	Validierung	erweitertes Projektteam/ Verbände (Zahler)
1.1.4 Hat das anwendende Fachpersonal in der Überprüfung der entsprechenden Erfüllung der Anforderungen bezüglich Datenschutzes/Cybersicherheit gesetzliche Verpflichtungen? *=> Basierend auf rechtlicher Analyse => Validierung* *=> Umsetzung*	Validierung	SBK/Spitex/FMH/H+/ Patientenorganisation
1.2 Technik: Wie könnten die nach kantonalem Recht zugelassenen Abgabestellen einen sicheren Download gewährleisten? *Technische Lösungen? Was sind die speziellen Herausforderungen?*	Explorativ	Nach kantonalem Recht zugelassene Abgabestellen/Swiss Medtech/SVDI/ Interpharma/Swiss Network for Digital Medical Regulation
1.2.1 Wer leistet Support bei allfälligen technischen Problemen? Wie sind sie hierzu *organisiert? (interne wie externe Perspektive)* *Technischer Erstsupport? Fachlicher Support? Weitere Unterstützung?* *Braucht es für dGAs noch andere Formen an Support als bei nicht-dGA-Produkten?*	Explorativ	erweitertes Projektteam Swiss Medtech/SVDI/Interpharma Verbände (Zahler) SBK/Spitex/FMH/H+/ Patientenorganisation
1.3 Recht MedTech: Was muss bei der Entwicklung von MedTech-SW bezüglich Datenschutzes/Cybersicherheit erfüllt, respektive berücksichtigt werden? Inwieweit sehen Sie die Anforderungen des neuen schweizerischen Datenschutzrechts (insbesondere Privacy-by-Design/Default, Datenbearbeitungsverzeichnis, etc.) durch die Europäische Zertifizierung abgedeckt? Gibt es hier einen Mehraufwand?	Validierung	NCSC Swiss Medtech/ SVDI/Interpharma
1.3.1 Was gilt spezifisch bezüglich Datenschutzes/Cybersicherheit für Apps im Bereich der digitalen Gesundheitsanwendungen?	Validierung	NCSC, Swiss Medtech/ SVDI/Interpharma
1.3.2 Was ist die Rolle der Konformitätsbewertungsstellen?	Validierung	Swiss Medtech/Experten/ SVDI

Fragen	Validierung/ Explorativ	Interviewpartner
1.4 Synthese: Was sind die aktuellen Herausforderungen für den Gesetzgeber?	Explorativ	erweitertes Projektteam/ Kantone/NCSC/Swissmedic/Swiss Medtech/SVDI/ Interpharma/Verbände (Zahler)

Schluss

☐ Haben Sie noch etwas zu ergänzen? Oder haben Sie noch Fragen an mich/uns?

☐ Dank (für die Teilnahme/Zeit und konstruktiven und wertvollen Aussagen)

☐ Ziel und Zweck des Projektes in mehr Details

☐ Feedback/Fragen/Unklarheiten im Nachgang