Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Abteilung Gesundheitsstrategien

21. September 2023

Konzept Identifikatoren Personen

Ergebnisse aus der Arbeitsgruppe Identifikatorenkonzept Personen

Aktenzeichen: 221-169/2/5

Hinweis:
Dieses Konzept gibt das Ergebnis der Diskussionen wieder, die in der *Arbeitsgruppe Identifikatorenkonzept Personen* der *Fachgruppe Datenmanagement im Gesundheitswesen* zwischen dem 13.03.2023 und 18.09.2023 geführt wurden. Die in diesem Konzept dokumentierten Ergebnisse geben nicht die offizielle Haltung der in der AG teilnehmenden Organisationen (inkl. BAG und GDK) wieder.

Inhalt

Abkürzungsverzeichnis

AG IP	Arbeitsgruppe Identifikatorenkonzept Personen
AHV	Alters- und Hinterlassenenversicherung
AHVN	AHV-Nummer
DSG	Bundesgesetz über den Datenschutz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EPD	Elektronisches Patientendossier
EPDG	Bundesgesetz über das elektronische Patientendossier
EPR-SPID	Patientenidentifikationsmerkmal des EPD
FDMG	Fachgruppe Datenmanagement im Gesundheitswesen
GSRN	Global Service Relation Number
IES NG	Informations- und Einsatz-System Next Generation
IVG	Bundesgesetz über die Invalidenversicherung
KIS	Klinikinformationssystem
KVG	Bundesgesetz über die Krankenversicherung
PID	Personenidentifikator
PIS	Praxisinformationssystem
SIK	Schweizerische Informatikkonferenz
UPI	Unique Person Identification (Informatiksystem der ZAS zur Verwaltung von Personenidentifikatoren. Aktuell: AHVN und EPR-SPID)
UVG	Bundesgesetz über die Unfallversicherung
VVG	Versicherungsvertragsgesetz
ZAS	Zentrale Ausgleichstelle

1 Ausgangslage

Die sichere und eindeutige Identifikation von Personen ist für viele Prozesse und Aspekte der Steuerung (inkl. der Forschung) des Gesundheitswesens unabdingbar. Die Identifikation von Personen kann zwar theoretisch in den meisten Fällen über identifizierende Merkmale wie Name, Wohnort und Geburtsdatum etc. erfolgen. Diese Art der Identifikation ist aber abhängig von der Datenqualität. Fehlerquellen sind z.B. komplexe ausländische Namen mit Sonderzeichen oder nicht-lateinischen Buchstaben, Verwechslungen beim Familiennamen und Ledignamen oder Schreibfehler bei phonetisch gleichen Namen mit unterschiedlicher Schreibweise. Im Kontext von IT-Systemen ist die Identifikation über demografische Merkmale komplexer und fehleranfälliger als die Verwendung eines eineindeutigen Personenidentifikators (PID). Bei der Digitalisierung des Gesundheitswesens ist ein PID eine notwendige Voraussetzung, da die Interoperabilität von IT-Systemen nur dann sichergestellt werden kann, wenn Objekte und Personen über Systemgrenzen hinweg eindeutig identifiziert werden können. Darüber hinaus trägt ein eineindeutiger Personenidentifikator auch zur Patientensicherheit bei, indem er das Risiko für eine fälschliche Zuordnung z.B. von Untersuchungsergebnissen oder Medikationen minimiert. Ein PID ist ausserdem immer dann wichtig, wenn Daten aus unterschiedlichen Quellen oder mit unterschiedlichen Erfassungszeitpunkten zweifelsfrei einer Person zugeordnet werden müssen. Beispiele sind

- das Zusammenführen[1] von Daten in einem Klinikinformationssystem (KIS) einer grösseren Institution mit verschiedenen Abteilungen oder Kliniken,
- das Zusammenführen von behandlungsrelevanten Daten aus verschiedenen Primärsystemen (Klinik- bzw. Praxisinformationssystem [KIS, PIS]) im elektronischen Patientendossier (EPD),
- das Zusammenführen der Abrechnungsdaten eines Versicherten durch den Krankenversicherer,
- das Zusammenführen der Daten aus verschiedenen Quellen durch die kantonalen Krebsregister, sowie das Zusammenführen dieser Daten auf nationaler Ebene zu Auswertungszwecken,
- das Zusammenführen von Informationen zu einem bestimmten Fall / zu einer bestimmten Person in den Meldesystemen zur Überwachung von Infektionskrankheiten,
- Das Zusammenführen von Informationen zu Personen in Qualitäts- und Medizinprodukteregistern[2]
- Echtzeitüberwachung der Spitalkapazitäten im Informations- und Einsatz-System Next Generation (IES NG) durch Verknüpfung von Spitalkapazität mit der Zuweisung von einzuliefernden Patienten,
- die Verknüpfung von Datensätzen aus unterschiedlichen Quellen zu Forschungszwecken.

Mit dem *Bericht zur Verbesserung des Datenmanagements im Gesundheitsbereich*, sowie dem *Bericht des Bundesrates in Erfüllung des Postulates 15.4225 Humbel* und der *Motion 21.4373 Einführung eines eindeutigen Patientenidentifikators* liegen drei vom Bundesrat bzw. vom Parlament verabschiedete Aufträge vor, die Einführung eines eineindeutigen Personenidentifikators für das Gesundheitswesen voranzutreiben.

2 Auftrag der AG Identifikatorenkonzept Personen

Die *Fachgruppe Datenmanagement im Gesundheitswesen* (FDMG) hat die AG Identifikatorenkonzept Personen (AG IP) beauftragt, einen Vorschlag für die Einführung eines eineindeutigen Personenidentifikators im Gesundheitswesen zu erarbeiten. Im Rahmen der Umsetzung des Auftrages der AG IP wurde unter Einbezug der Behördenstellen auf Ebene des Bundes und der Kantone, sowie weiteren Akteuren im Gesundheitswesen das vorliegende Konzept erarbeitet, welches für die verschiedenen Anwendungsfälle die bestehenden Personenindikatoren bzw. das Fehlen dieser aufzeigt und eine für alle Anwendungsfälle kohärente Lösung (inkl. Rechtsetzungsbedarf) vorschlägt. Wichtig dabei ist die

[1] Unter «Zusammenführen» wird hier einerseits die Verknüpfung von Daten zu einer Person aus unterschiedlichen Datenquellen verstanden; andererseits auch die Rückführung von Daten auf eine eindeutig identifizierte Person.

[2] Bei medizinischen Registern handelt es sich um «Systematische Sammlung von populations- oder patientenbezogenen, aber auch qualitätsbezogenen, medizinischen und/oder gesundheitsökonomischen Daten in einem vordefinierten Arbeitsbereich, sowie deren Auswertung, die einen definierten Zweck erfüllt, aber Variabilität für unterschiedliche Fragestellungen erlaubt.» (zitiert nach *Medizinische Register in der Schweiz auf einen Blick*, FMH, 2012). In einem Qualitätsregister liegt der Fokus auf Indikatoren, wie z.B. Versorgungsabläufen, Komplikationen oder Mortalitätsraten, die eine Analyse der Qualität von z.B. medizinischen Behandlungen erlauben. In einem Medizinprodukteregister werden Daten zu bestimmten Medizinprodukten gesammelt, die z.B. zu Zwecken der Nachvollziehbarkeit der Verwendung, für die Risikobewertung oder die Forschung verwendet werden können.

gesamtheitliche Betrachtung des Datenökosystems im Gesundheitswesen und die Kontextualität des Verwendungszweckes und der Datenverknüpfung.

Teilnehmende Organisationen:

Bund und Kantone	Bundesamt für Gesundheit BAG
	Bundesamt für Statistik BFS
	Bundeskanzlei BK
	Bundesamt für Sozialversicherungen BSV
	Logistikbasis der Armee (LBA) - Sanität
	Zentrale Ausgleichsstelle ZAS
	Schweizerische Gesundheitsdirektorenkonferenz GDK
	eHealth Suisse
Akteuren im Gesundheitswesen	CARA (EPD-Stammgemeinschaft)
	FMH
	GS1
	H+
	heyPatient AG (Systemhersteller)
	Institut für Sozial- und Präventivmedizin Universität Bern
	refdata
	Swiss Personalized Health Network (SPHN)
	SUVA
	Verein Digitale Gesellschaft

Zusätzlich hat an der zweiten Sitzung der AG IP der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) teilgenommen. Somit ist der EDÖB über die Arbeit der AG IP informiert und wird auch bei der Beurteilung der Ergebnisse der AG IP wieder hinzugezogen werden. Der EDÖB hat insbesondere darauf hingewiesen, dass beim Einsatz der AHVN als eineindeutigem Personenidentifikator der periodischen Risikoanalyse gemäss Artikel 153e AHVG eine entscheidende Rolle zukommt.

Das erarbeitete Konzept soll der FDMG zur Beurteilung vorgelegt werden.

3 Definition von Themenbereichen und Anwendungsfällen

In Anlehnung an die auch für das Programm DigiSanté definierten Themenbereiche fokussieren sich die Überlegungen zu den Personenidentifikatoren auf die folgenden vier Themenbereiche und die zu diesen Themenbereichen gehörenden Anwendungsfälle:

Themenbereich	Anwendungsfälle
Behandlungsprozesse	• **Primärdokumentation** Daten, die zum Zweck der ärztlichen/pflegerischen Dokumentation erhoben werden, sowie Daten zu Abrechnungszwecken. PID für eindeutige Identifikation der Patientin/des Patienten. • **EPD** Austausch behandlungsrelevanter Daten im Kontext des elektronischen Patientendossiers. PID für eindeutige Identifikation der Patientin/des Patienten und die Zusammenführung der Daten verschiedener (Stamm-)Gemeinschaften. • **Gerichtete Kommunikation zwischen Gesundheitseinrichtungen** Z.B. Überweisung, Laborauftrag, Rezept. PID für eindeutige Identifikation der Patientin/des Patienten.

	• **mHealth** (unterstützt durch Apps)[3] Messungen von Vitaldaten über Sensoren. Vom Patienten erfasste Daten, wie z.B. Schlaf- oder Ernährungstagebücher. PID für eindeutige Zuordnung der erfassten Daten zu einer Patientin/einem Patienten. • **Rückruf von Implantaten** Im Falle eines Rückrufes eines bestimmten Implantats können alle betroffenen Implantate-Empfänger gezielt informiert werden. PID für eindeutige Zuordnung der Implantate zu einer Patientin/einem Patienten. • **Qualitäts- und Medizinprodukteregister**
Abrechnungsprozesse	• **Sozialversicherung** (inkl. UV und IV) • Private **Zusatzversicherung**, welche zur sozialen Krankenversicherung angeboten werden (vgl. Art. 47a Versicherungsvertragsgesetz). PID jeweils für eindeutige Zuordnung der Abrechnungsdaten zu einer Patientin/einem Patienten.
Behördenprozesse	• Statistische Erhebungen im Gesundheitsbereich gemäss Statistikerhebungsverordnung (SR 431.012.1) • Krebsregistrierung gemäss Krebsregistrierungsgesetz (SR 818.33) • Epid. Überwachung von übertragbaren Krankheiten gemäss Epidemiengesetz (SR 818.101) • Verknüpfung von Datensätzen zur Berechnung von medizinischen Qualitätsindikatoren gemäss Artikel 59a Krankenversicherungsgesetz (SR 832.10) PID jeweils für eindeutige Zuordnung der erfassten Daten zu einer Person und späteren Verknüpfung der Daten mit Daten aus anderen Quellen, insbesondere zu statistischen Zwecken.
Forschung	• **Nutzung von Daten aus verschiedenen Datenquellen mit Verknüpfung**. PID für eindeutige Zuordnung der erfassten Daten zu einer Person und späteren Verknüpfung der Daten mit Daten aus anderen Quellen. • **Nutzung von Daten ohne Verknüpfung**. PID für eindeutige Zuordnung der erfassten Daten zu einer Person erleichtert den Datenmanagementprozess.

Mit der AHV-Nummer (AHVN) und der Patientenidentifikationsnummer des EPD (EPR-SPID) stehen bereits zwei potentielle, eineindeutige PID zur Verfügung. Aktuell darf die AHVN für die Abrechnungsprozesse der Sozialversicherungen[4] sowie durch die Zusatzversicherer gemäss Artikel 47a Versicherungsvertragsgesetz verwendet werden[5]. Zudem darf sie sowohl von den Behörden zur Erfüllung ihrer Aufgaben, als auch – sofern das anwendbare Recht die systematische Verwendung der AHVN vorsieht – von Organisationen und Personen des öffentlichen oder privaten Rechts, die durch Bundesrecht, kantonales Recht oder kommunales Recht oder durch Vertrag mit Verwaltungsaufgaben betraut sind, verwendet werden[6]. Damit besteht für die oben genannten Themenbereiche Abrechnung und Behördenprozesse bereits eine rechtliche Grundlage zur Verwendung der AHVN. Für den Anwendungsfall *elektronisches Patientendossier* im Themenbereich *Behandlung* besteht mit dem *Bundesgesetz über das elektronische Patientendossier (EPDG)* eine spezialgesetzliche Grundlage zur Verwendung der EPR-SPID.[7]

[3] Die Überlegungen zum mHealth-Apps in diesem Konzept beziehen sich auf Apps, die mit dem EPD oder mit Systemen, die von Leistungserbringern zur Verfügung gestellt werden, verbunden sind. Bei diesen Apps soll die AHVN als PID in der App geführt werden dürfen. Weitere Anwendungsfälle im Kontext mHealth werden im Rahmen des Konzepts nicht betrachtet. Eine Empfehlung für die Verwendung eines PID im Rahmen aller denkbaren mHealth-Anwendungsfälle überschreitet die Möglichkeiten der AG IP im Rahmen des Auftrags der FDMG.

[4] Vgl. Art. 83 KVG, Art. 60*a* UVG, Art. 60 IVG

[5] Vgl. Artikel 47a VVG

[6] Vgl. Artikel 153c AHVG

[7] Bestehende Lösungen für Personenidentifikatoren, wie die EPR-SPID für das EPD, sollen in diesem Konzept nicht in Frage gestellt werden. Der Fokus dieses Dokuments liegt darauf für Anwendungsfälle, für die es noch keinen einheitlichen PID gibt, Lösungen vorzuschlagen.

Es bleiben somit folgende der oben genannten Themenbereiche und Anwendungsfälle bzgl. der Verwendung eines eineindeutigen PID offen:

- Im Themenbereich *Behandlung*:
  - Primärdokumentation/elektronische Krankengeschichte (ohne Bezug zur Abrechnung und ausserhalb des Kontextes EPD)
  - Gerichtete Kommunikation zwischen Leistungserbringern
  - mHealth (unterstützt durch Apps)
  - Qualitäts- und Medizinprodukteregister (z.B. für den Rückruf von Implantaten; von Privaten geführt)
  - Versicherer, die Zusatzversicherungen anbieten, die nicht unter Artikel 47a VVG fallen
  - Echtzeitüberwachung der Spitalkapazitäten im IES NG
- Der Themenbereich *Forschungsdaten* (zum Zwecke einer späteren Verknüpfung)

Aktuell fehlt eine gesetzliche Grundlage, um einen eineindeutigen PID, wie z.B. die AHVN, als Identifikator auch im Behandlungsprozess zu verwenden. Deshalb werden gegenwärtig im Themenbereich *Behandlung*, z.B. bei der Krankengeschichte, lokale/systemspezifische PID verwendet. Dies erschwert, wie oben bereits erwähnt, das Zusammenführen der Daten über verschiedene Systeme hinweg und macht es zudem fehleranfällig. Mit einer gesetzlichen Grundlage für einen eineindeutigen PID, der auch für die Behandlungs- und Forschungsdaten verwendet werden darf, wäre das Verknüpfen dieser Daten – vorbehaltlich der gemäss geltendem Recht notwendigen Einwilligung der betroffenen Personen[8] – problemlos möglich, wodurch der Forschung wertvolle Daten aus dem Behandlungskontext zur Verfügung stehen würden.

[8] Es wäre sinnvoll, wenn das Verfahren zur Erteilung von Einwilligungen bzw. die Verwaltung von Einwilligungen vereinfacht werden würde. Dies geschieht beispielsweise im Vorhaben «Datenraum für die gesundheitsbezogene Forschung» und im Rahmen der Revision des Humanforschungsgesetzes, wo die Möglichkeit einer elektronischen Einwilligung vorgeschlagen wird.

4 PID-Optionen und deren Einschätzung

4.1 PID-Optionen

Folgende Optionen für einen Personenidentifikator im Gesundheitswesen wurden im Rahmen der AG IP betrachtet:

	AHV-Nummer (AHVN)	**Patientenidentifikationsnummer des EPD (EPR-SPID)**	**Neue Gesundheitsnummer**	**Pseudonym AHV-Nummer**
Gesetzliche Grundlage	AHVG	EPDG	-	-
Aktueller Verwendungszweck / Berechtigte	• **Zweck:** Erfüllung gesetzlicher Aufgaben (u.a. Sozialversicherung, behördliche Statistik) • **Berechtigte:** Behörden, Organisationen und Personen gemäss Artikel 153c AHVG	• **Zweck:** Identifikation von Patientinnen und Patienten im Kontext EPD • **Berechtigte:** Gemeinschaften, Stammgemeinschaften und Zugangsportale gemäss Artikel 5 EPDG	-	-
Eigenschaften/ Rahmenbedingungen	• Bestehende Infrastruktur und Schnittstellen zur Verwaltung der AHVN (System UPI der ZAS) • Die Prozesse zur Abfrage der AHV-Nummer sind standardisiert (eCH-Standards) • International standardisiertes Format (EAN-13) • Direkte Verknüpfung mit Daten des BFS ist möglich, da das BFS ebenfalls die AHV-Nummer verwendet.	• Bestehende Infrastruktur und Schnittstellen zur Verwaltung der EPR-SPID (System UPI der ZAS) • Die Prozesse zur Abfrage der EPR-SPID sind standardisiert (eCH-Standards) • International standardisiertes Format (GSRN) • Sektorieller Identifikator → Verknüpfung mit Daten aus anderen Sektoren ist erschwert; aber Verknüpfung zur AHV-Nummer in UPI vorhanden	• Von Grund auf neu zu konzipieren bzgl. Verwendungszweck, Technik, Format • Technische Infrastruktur zur Verwaltung der Nummer muss aufgebaut werden • Rechtliche Verankerung erforderlich	• Generierung von (projektspezifischen) Pseudonymen auf Basis der AHVN, um eine Rückführung auf die AHVN und damit die Verknüpfung von Daten durch Unbefugte zu verhindern. • Aufbau eines Pseudonymisierungsdienstes erforderlich • Rechtliche Verankerung erforderlich

4.2 Übersicht Pro und Contra möglicher Personenidentifikatoren

In der folgenden Tabelle wird eine bewertende Gegenüberstellung der Personenidentifikatoren vorgenommen, die von der AG IP als potentielle Kandidaten für einen PID betrachtet wurden.

AHV-Nummer	EPR-SPID	Neue Gesundheitsnummer	Pseudonym AHV-Nummer
Pro: • Gestützt auf Artikel 153c Absatz 1 AHVG sind bereits verschiedene Stellen berechtigt die AHVN ausserhalb der AHV zu verwenden. Das umfasst u.a. die Leistungserbringer (im Rahmen der ihnen gemäss Bundesgesetz über die Krankenversicherung (KVG) übertragenen Aufgaben) und die Bundesstatistik, deren Daten für die gesundheitsbezogene Forschung von besonderer Bedeutung sind. Rechtliche Grundlagen zur erweiterten Verwendung der AHVN wären aber neu zu schaffen. • Die Qualität der AHVN ist sehr hoch und es bestehen umfangreiche Erfahrungswerte beim Einsatz der AHVN. • Die zentrale technische Infrastruktur ist vorhanden (UPI). • Die eCH-Standards[9] für die Verwaltung und Verwendung der AHVN sind vorhanden • Patientinnen und Patienten kennen die AHVN als Nummer, die bereits	**Pro:** • Die zentrale technische Infrastruktur ist vorhanden (UPI). • Die eCH-Standards für die Verwaltung und Verwendung der EPR-SPID sind vorhanden. • Die missbräuchliche Verknüpfung mit Daten aus anderen Bereichen wird erschwert, da es sich um einen sektoriellen Identifikator handelt. Siehe dazu aber auch Hinweis bei der AHVN bzgl. der Verknüpfung mit Hilfe weiterer personenidentifizierender Merkmale. • International standardisiertes Format (GSRN) • Eine sektorielle Nummer unterstützt die Forderung des DSG nach «Privacy by Design» (Datenschutz durch Technikgestaltung). • Wenn eine Person ihre AHV-Nummer ändert (aus administrativen Gründen oder aufgrund von Fehlerkorrekturen, was in etwa 1% bis 2% der Fälle vorkommt), wird eine neue EPR-SPID erzeugt, die mit der alten	**Pro:** • Die missbräuchliche Verknüpfung mit Daten aus anderen Bereichen wird erschwert, da es sich um einen sektoriellen Identifikator handelt. Siehe dazu aber auch Hinweis bei der AHVN bzgl. der Verknüpfung mit Hilfe weiterer personenidentifizierender Merkmale. • Kann nach internationalem Standard konzipiert werden **Contra:** • Die rechtmässige Verknüpfung mit Daten aus anderen Bereichen wird erschwert • Aufbau einer neuen Infrastruktur zur Verwaltung der Gesundheitsnummer erforderlich (geschätzte Kosten in Höhe von mehreren Dutzend Millionen Franken über einen Zeitraum von zehn Jahren). • Schaffung gesetzlicher Grundlagen nötig und aufwendiger als bei den anderen PID-Optionen	**Pro:** • Die Rückführung auf die Person (über die AHVN) ist zumindest deutlich erschwert. • Die Einführung einer neuen Nummer ist nicht erforderlich→ geringerer Aufwand für Rechtsetzung **Contra:** • Es besteht ein zusätzlicher Aufwand durch die Pseudonymisierung. • Ein Pseudonymisierungsdienst muss aufgebaut werden. (Technik und Organisation) • Bei reger Nutzung kann ein direkter Rückschluss auf die AHVN gezogen werden kann, da viele Institutionen sowohl Zugang zum Pseudonym als auch zur AHVN haben • Bei einem determinierenden Algorithmus kann bei genügend Beispielen das fixe Pseudonym vorhergesagt werden. • Wenn eine Person ihre AHV-Nummer ändert (aus administrativen Gründen oder um Fehler zu korrigieren, was in etwa 1% bis 2% der

[9] Der Verein eCH fördert, entwickelt und verabschiedet Standards im Bereich E-Government. Siehe auch https://www.ech.ch

AHV-Nummer	EPR-SPID	Neue Gesundheitsnummer	Pseudonym AHV-Nummer
heute im Gesundheitswesen eingesetzt wird. • Jeder Einwohner/in der Schweiz verfügt über eine AHVN.[10] **Contra:** • Die grosse Verbreitung der AHVN macht es theoretisch auch für Unbefugte leichter, Daten aus verschiedenen Quellen illegal miteinander zu verknüpfen. Allerdings sind die Datenbanken, in denen die AHVN verwendet wird, dezentral organisiert, sodass man für die Verknüpfung Zugang zu mehreren dieser dezentralen Datenquellen haben müsste. Zudem ist die Wahrscheinlichkeit gross, dass die Daten auch ohne eineindeutigen PID zusammengeführt werden können, sofern die Datensätze über weitere personenidentifizierende Daten verfügen.	verknüpft ist. Die Verbindung zwischen der Person vor und nach der Änderung bleibt erhalten. **Contra:** • Die rechtmässige Verknüpfung mit Daten aus anderen Bereichen wird erschwert. Für eine Verknüpfung z.B. mit der AHVN müsste ein entsprechendes Mapping über die UPI-Services vorgenommen werden. • Rechtliche Verankerung aktuell nur im EPDG → Einsatz aktuell auf das EPD beschränkt • Die EPR-SPID ist in der Bevölkerung weitestgehend unbekannt. • Nur EPD-Inhaber verfügen über eine EPR-SPID (Stand 15. April 2023 wurden 19'481 EPD eröffnet). Mit der Revision des EPDG und dem dort vorgesehenen Opt-Out-Verfahren ist aber davon auszugehen, dass sich die Anzahl der EPD massiv erhöhen wird.	• Qualitätsprobleme in den ersten Jahren nach der Einführung zu erwarten, da die Qualität der Quelldaten vermutlich nicht optimal sein wird. • Eine neue Gesundheitsnummer müsste in der Bevölkerung bekannt gemacht werden. • Alle administrativen Prozesse für die Verwaltung dieser neuen Nummer müssen eingerichtet werden (die sich mit denen der AHV-Nummer überschneiden). Das bedeutet, dass die Aussteller der primären Identität (eidgenössische und kantonale Personenregister) einen zweiten Datenlieferungsprozess (parallel zu demjenigen für die AHV-Nummer) für die neue Struktur einrichten müssen, was der Strategie des Bundes (z.B. Once-only-Prinzip) widerspricht. • Die Problematik von Personen, die nicht über eine AHV-Nummer verfügen (z.B. Touristen), wird durch die Einführung einer neuen Gesundheitsnummer nicht behoben.	Fälle vorkommt), wird das neu erzeugte Pseudonym nicht wieder mit dem alten verknüpft. Die Verbindung zwischen der Person vor der Änderung und der Person nach der Änderung geht verloren. Es ist möglich, dieses Problem zu lösen, indem man eine AHVN-Pseudonym-Verknüpfungstabelle einrichtet, aber das bedeutet, dass man eine neue Sektor Nummer vom Typ EPR-SPID einrichten muss (anstatt diese Lösung direkt zu verwenden).

Hinweis zur Pseudonymisierung von PID: Insbesondere bei der Verwendung der AHVN als PID würde der Pseudonymisierung der AHVN bei den Anwendungsfällen, bei denen die direkte Verwendung der AHVN aus Datenschutzgründen vermieden werden soll, eine wichtige Bedeutung zukommen. Dies betrifft zum Beispiel den Anwendungsfall «Verknüpfung von Daten für die Forschung». Bei der Pseudonymisierung würde ein Trust Center eine wichtige Rolle übernehmen. Dem Trust

[10] Zudem kann eine AHVN falls erforderlich auch für Personen ausgestellt werden, die nicht (offiziell) in der Schweiz ansässig sind oder arbeiten, sofern diese mit einer Behörde in Kontakt kommen, die berechtigt ist, die AHVN systematisch zu verwenden. Dies betrifft z.B. Sans-Papiers, für die der Arbeitgeber Sozialversicherungsbeiträge bezahlt.

Center könnte u.a. die Aufgabe zukommen die Pseudonyme zu generieren und in den Datensätzen gegen die AHVN zu ersetzen. Zudem würde das Trust Center die Schlüssel zur Codierung bzw. De-Codierung von Pseudonymen verwalten und die Verknüpfung der Daten bzw. die Bereitstellung der verknüpften Daten zu übernehmen. (vgl. auch Kapitel 5, Abschnitt *Besondere Massnahmen zur Gewährleistung des Datenschutzes in Forschungsprojekten*)

4.3 Einschätzung der PID-Optionen

Bei Gesundheitsdaten handelt es sich gemäss Artikel 5 Buchstabe c DSG um besonders schützenswerte Personendaten. Deshalb muss dem Datenschutz beim Entscheid für einen PID im Gesundheitswesen besondere Beachtung geschenkt werden. Das blosse Führen eines eineindeutigen PID erhöht das Datenschutzrisiko dabei nur geringfügig. Risiken entstehen, sobald sensible Daten mit Daten verknüpft werden, die eine Person identifizieren können. Der PID ist zwar eine Möglichkeit zur Identifikation einer Person, aber auch das Tripel *Nachname/Vorname/Geburtsdatum* ist ein Quasi-Identifikator.

Ein zusätzliches Risiko für den Datenschutz entsteht aber durch die Möglichkeiten zur Verknüpfung von Datensätzen mit Hilfe eines PID und die damit entstehenden Datensammlungen bzw. Profilbildungen zu einer bestimmten Person. Es ist allerdings festzuhalten, dass – wie in den in Kapitel 1 referenzierten Aufträgen von Bundesrat und Parlament vorgeschlagen – die **rechtmässige** Verknüpfung von gesundheitsbezogenen Daten eine wesentliche Motivation für die Einführung eines einheitlichen PID im Gesundheitswesen darstellt, z.B. um dadurch mehr Daten in besserer Qualität für die gesundheitsbezogene Forschung zur Verfügung stellen zu können.

Die Verknüpfung von Datensätzen kann aber auch missbräuchlich erfolgen – egal welcher Identifikator bzw. welches Set an Identifikatoren eingesetzt wird. Es gilt also aus Datenschutzperspektive zu beurteilen, welche der in Kapitel 4 beschriebenen PID-Optionen den Datenschutz am besten gewährleistet, bzw. die Wahrscheinlichkeit für das missbräuchliche Zusammenführen von Datensätzen durch Unbefugte reduziert. Es muss aber auch darauf hingewiesen werden, dass die Wahrscheinlichkeit gross ist, dass Daten aus verschiedenen Datensätzen auch ohne eineindeutigen PID zusammengeführt werden können, sofern die Datensätze über weitere personenidentifizierende Daten verfügen. Werden z.B. Vorname, Name und Geburtsdatum fehlerfrei (!) in den distinkten Datensammlungen erfasst, können gemäss Schätzungen der Schweizerischen Informatikkonferenz (SIK) die Daten von 99,98 % der Schweizer Bevölkerung eindeutig zusammengeführt werden[11].

Ein weiterer Vorteil der Verwendung eines eineindeutigen PID ist, dass die Identifikation mittels PID sicherer ist als die Identifikation mit Hilfe anderer identifizierender Merkmale. Werden z.B. Namen als identifizierende Merkmale verwendet kann es bei komplexen ausländischen Namen mit Sonderzeichen oder nicht-lateinischen Buchstaben, bei der Verwechslungen von Familiennamen und Ledignamen oder bei phonetisch gleichen Namen mit unterschiedlicher Schreibweise zu Fehlidentifikationen kommen.

Die verschiedenen betrachteten eineindeutigen PID unterscheiden sich im Wesentlichen in ihrem aktuellen Verbreitungsgrad, den vorhandenen bzw. nicht-vorhandenen technisch-organisatorischen Infrastrukturen und den vorhandenen bzw. nicht-vorhandenen rechtlichen Grundlagen.

Je stärker der Anwendungsbereich des eineindeutigen Identifikators eingeschränkt ist (z.B. limitiert auf das EPD oder den Gesundheitsbereich), desto geringer ist der Nutzen für die Anwendungsfälle, bei denen die Verknüpfung von Daten entscheidend ist (wie z.B. bei Forschungsprojekten, wenn eine Verknüpfung von Daten aus der Krankengeschichte mit sozioökonomischen Daten oder anderen Daten der öffentlichen Statistik, etc. stattfinden soll). Sofern in vielen verschiedenen Datensätzen derselbe PID verwendet wird, ist das Zusammenführen der Datensätze – auch durch Unbefugte – insofern vereinfacht, als dass man eben nur diesen einen Identifikator kennen muss, um die Datensätze zusammenzuführen.

Bei der Verwendung verschiedener, sektorieller Identifikatoren, muss eine Person, die die Datensätze zusammenführen möchte, neben den einzelnen Identifikatoren auch über Informationen zum Mapping

[11] Vgl. *AHV-Versichertennummer als eindeutiger behördlicher Personenidentifikator*, S. 4, Herausgeber: Schweizerische Informatikkonferenz

dieser Identifikatoren verfügen, was das Zusammenführen der Datensätze erschwert. Aus der Perspektive des Datenschutzes bringen sektorielle Identifikatoren theoretisch einleuchtende allerdings in der Praxis nur geringe Vorteile, da – wie oben bereits erwähnt – in den meisten Fällen auch eine Verknüpfung der Daten über weitere identifizierende Merkmale möglich ist. Insbesondere beim Zusammenführen der Daten aus kriminellen Motiven kann davon ausgegangen werden, dass es für die handelnden Personen irrelevant ist, ob – eine gute Qualität der Ausgangsdaten vorausgesetzt – ein geringer Bruchteil der Daten (im obigen Beispiel der SIK 0.02%) nicht zusammengeführt werden kann.

Eine effizientere Massnahme, um das unbefugte Zusammenführen von Daten zu verhindern, ist die Verteilung der Datensammlungen auf getrennte Datenbanken. Dadurch ist es erforderlich Zugriff zu mehreren Datenbanken zu haben, um Daten verknüpfen zu können, was das unbefugte Verknüpfen wesentlich erschwert. Zudem sind hohe Mindestanforderungen an die Datensicherheit für IT-Systeme zu stellen, welche die AHVN bzw. einen anderen PID führen.

Bei einer Abwägung zwischen der Verwendung der AHVN und einer neuen Gesundheitsnummer ist bei der Betrachtung möglicher Risiken für den Datenschutz ausserdem zu berücksichtigen, dass bei der Verwendung der AHVN ein Risiko besteht, dass unbefugt Persönlichkeitsprofile erstellt werden. Bei einer neu eingeführten Gesundheitsnummer bestehen insbesondere in der ersten Phase der Nutzung allerdings Qualitätsrisiken (wie z.B. die falsche Zuordnung einer Nummer zu einer Person), die möglicherweise sogar zu unerwünschten gesundheitlichen Folgen führen können, die es zu vermeiden gilt.

Unter diesen Voraussetzungen lässt sich die Aussage treffen, dass im Kontext des Gesundheitswesens nicht der verwendete PID der aus Datenschutzperspektive entscheidende Faktor ist, sondern die begleitenden risikominimierenden Massnahmen, die bei der Bearbeitung von personenbezogenen gesundheitsrelevanten Daten angewendet werden. Diese Massnahmen müssen darauf fokussiert sein die personenbezogenen Gesundheitsdaten vor unberechtigtem und möglicherweise auch kriminell-motiviertem Zugriff zu schützen.

5 Fazit und Empfehlung der AG IP

Die AG IP spricht sich bei den Anwendungsfällen, bei denen eine Rückführung von Daten auf eine bestimmte Person erforderlich ist, für die AHVN als eineindeutigem Personenidentifikator aus.

Dies betrifft die Anwendungsfälle

- Primärdokumentation/elektronische Krankengeschichten (ausserhalb des EPD)
- gerichtete Kommunikation (z.B. zwischen Leistungserbringern beim eRezept (ausserhalb des EPD) oder zwischen mHealth-Apps und KIS, PIS oder EPD)
- Datenerhebung im Rahmen von Forschungsprojekten, bei denen die spätere Rückführung auf eine Person, z.B. für Verknüpfungszwecke, notwendig ist[12]
- Register, in den Daten über einen längeren Zeitraum zu einer Person erhoben werden
- Echtzeitüberwachung der Spitalkapazitäten im IES NG

Um die Verwendung der AHVN in den oben genannten Anwendungsfällen zu ermöglichen, muss der Kreis der systematischen Nutzer der AHVN gemäss Artikel 153c AHVG bei bestimmten Anwendungsfällen auf private Institutionen ausgeweitet werden (z. B. universitäre Forschungseinrichtungen).

Die bereits bestehenden rechtlichen Grundlagen, die weite Verbreitung und die vorhandenen technischen Infrastrukturen sind gute Voraussetzungen für die Ausweitung der Verwendung der AHVN.

[12] Sofern die Verwendung der AHVN im Rahmen eines Forschungsprojekts als nicht notwendig erachtet wird, kann selbstverständlich auch ein beliebiger anderer lokaler Identifikator verwendet werden. Die Verwendung der AHVN wird dann als sinnvoll erachtet, wenn die Daten entweder zu einem späteren Zeitpunkt mit weiteren Daten verknüpft werden sollen oder wenn die Identifizierung der Person zu der ein Datensatz gehört notwendig ist (z.B. bei Forschungsergebnissen, die potentielle Gefährdungen für eine Person aufdecken).

Eine dezentrale Datenhaltung bei den Datensammlungen, welche die AHVN verwenden, wird als notwendig erachtet, da dies das Zusammenführen der Daten erschwert und somit ein höherer Datenschutz gewährleistet ist. Zudem sollen – gemäß den Empfehlungen der ZAS – in den Datensammlungen Privater, die die AHVN verwenden, die Gesundheitsdaten und Personendaten getrennt bearbeitet werden.

Bei Verwendung der AHVN sind die bestehenden rechtlichen Grundlagen strikt einzuhalten. Besondere Relevanz für die Gewährleistung des Datenschutzes haben hier Artikel 153d *Technische und organisatorische Massnahmen* und Artikel 153e *Risikoanalyse* des AHVG.

Für Anwendungsfälle, bei denen eine Rückführung von Daten auf eine bestimmte Person oder die Verknüpfung von Datensätzen unwahrscheinlich aber nicht ausgeschlossen ist, empfiehlt die AG IP die Verwendung eines projektspezifischen Pseudonyms der AHVN, um eine weitestgehende De-Identifizierung der Datensätze zu ermöglichen. Beispiele für solche Anwendungsfälle sind die Mehrzahl der Forschungsprojekte bei denen Daten bereits vorgängig (z.B. mit Hilfe der AHVN) verknüpft wurden, oder Register, die zur Qualitätssicherung, z.B. im Bereich Implantate dienen (vgl. auch Szenarien 5 und 6 im Kapitel 7.1.).

Wenn die Notwendigkeit der Rückführung der Daten auf eine Person oder die Verknüpfung mit weiteren Daten ausgeschlossen werden kann, kann statt des Pseudonyms der AHVN ein beliebiger lokaler Identifikator verwendet werden.

Die Verwendung eines sektoriellen PID für das Gesundheitswesen wird von den meisten Mitgliedern der AG IP aus folgenden Gründen als nicht sinnvoll erachtet: Bei der Einführung eines sektoriellen Personenidentifikators stehen einem relativ geringen Nutzen für den Datenschutz relativ hohe Kosten bei der Einführung des sektoriellen Identifikators gegenüber. Zudem kann durch die Verwendung eines projektspezifischen Pseudonyms der AHVN ein höheres Datenschutz-Level erreicht werden als durch einen sektoriellen PID.

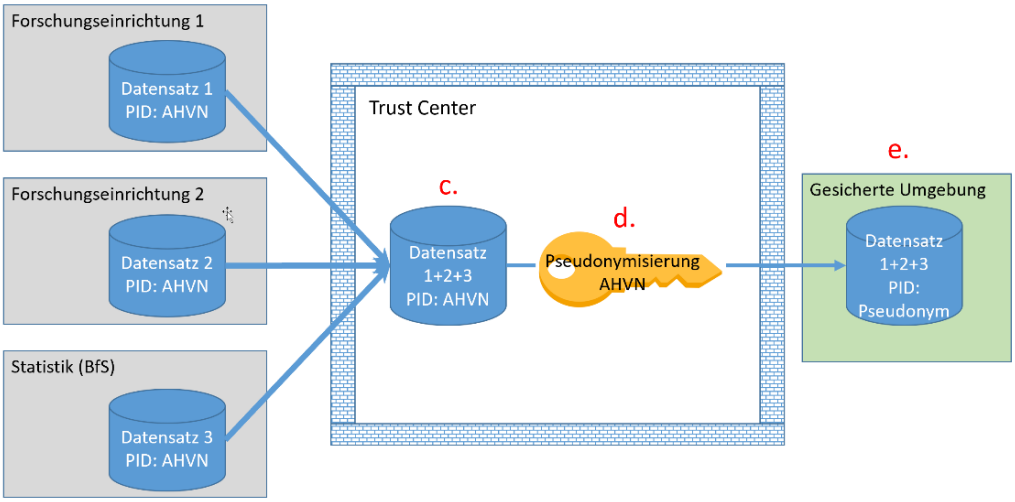
Zusammenfassung des Lösungsvorschlages zur Verwendung der AHVN

Themenbereich	Anwendungsfall	Verwendung AHVN	Fallspezifische Bewilligung zur Verwendung der AHVN erforderlich?
Behandlung	Primärdokumentation/elektronische Krankengeschichte (ohne Bezug zur Abrechnung und ausserhalb des Kontextes EPD)	Ja	Nein
	Gerichtete Kommunikation zwischen Leistungserbringern (ausserhalb des Kontextes EPD)	Ja	Nein
	mHealth (bei Integration mit Systemen der Leistungserbringer)	Ja	Ja
	Qualitäts- und Medizinprodukteregister, sofern Rückbezug auf Person erforderlich ist (z.B. für den Rückruf von Implantaten; von Privaten geführt; bundesrechtlicher Auftrag vorhanden)	Ja	Nein
	Qualitäts- und Medizinprodukteregister, sofern Rückbezug auf Person nicht erforderlich ist	Nein	-
	Versicherer, die Zusatzversicherungen anbieten, die nicht unter Artikel 47a VVG fallen	Ja	Nein

Forschung	Forschungsprojekte mit Verknüpfung von Daten	Ja	Ja
	Forschungsprojekte ohne Verknüpfung von Daten	Nein	-
	Register ohne bundesrechtlichen Auftrag	Ja	Ja

Besondere Massnahmen zur Gewährleistung des Datenschutzes in Forschungsprojekten
Im Unterschied zu den meisten anderen der oben genannten Anwendungsfälle, dient die AHVN im Kontext Forschung nicht primär dazu die konkrete Person zu identifizieren, zu der Daten vorliegen, sondern in Forschungsprojekten wird die AHVN in der Regel als Verknüpfungsvariable für die Verknüpfung von Daten aus unterschiedlichen Datenquellen verwendet. In den verknüpften Datensätzen kann die AHVN deshalb in den meisten Fällen durch ein Pseudonym ersetzt werden.
Bei der Verwendung der AHVN zur Verknüpfung von Daten zu Forschungszwecken sind deshalb – zusätzlich zu den oben genannten Massnahmen und den Vorgaben nach Artikel 153d und 153e AHVG – folgende Sicherungsmassnahmen erforderlich:

1. Folgende Aufgaben müssen **von einem Trust Center wahrgenommen** werden (die folgende Liste ist nicht abschliessend):
    a. Bewertung der Anfragen der Forschenden für das Führen der AHVN in ihren Datensätzen in Bezug auf Notwendigkeit, Datenschutz und Ethik.
    b. Bewertung der Anfragen der Forschenden für die Verknüpfung von Datensätzen in Bezug auf Notwendigkeit, Datenschutz und Ethik.
    c. Verknüpfung der Datensätze
    d. Ersetzen der AHVN im verknüpften Datensatz mit einem Pseudonym der AHVN. Die genaue Methode der Pseudonymisierung wird nicht definiert. Es muss aber gewährleistet sein, dass das Pseudonym auf die AHVN zurückgeführt werden kann, falls eine Rückführung der Daten auf eine Person oder eine spätere Verknüpfung mit weiteren Datensätzen erfolgen soll. Die Informationen für die Rückführung vom Pseudonym auf die AHVN sind nur dem Trust Center bekannt (vgl. auch Buchstabe f)
    e. Bereitstellung der verknüpften Datensätze zur Bearbeitung durch die Forschenden in einer gesicherten Umgebung.



    f. Sichere Archivierung der verknüpften Datensätze und Mappinginformationen, nachdem die Datenbearbeitung durch die Forschenden abgeschlossen ist.[13]

[13] Die Archivierung der Daten dient einerseits gemäss dem *Kodex zur wissenschaftlichen Integrität* der *Akademien der Wissenschaften Schweiz* der Sicherstellung ihrer Reproduzierbarkeit und/oder Überprüfbarkeit (je nach Disziplin), ihrer Verlässlichkeit und Genauigkeit (vgl. *Kodex zur wissenschaftlichen Integrität* Kapitel 4.5). Andererseits erscheint es auch sinnvoll einmal verknüpfte Daten für folgende Forschungsprojekte, die auf dieselben verknüpften Daten zurückgreifen möchten, vorzuhalten, um den Aufwand für die Verknüpfung zu reduzieren.

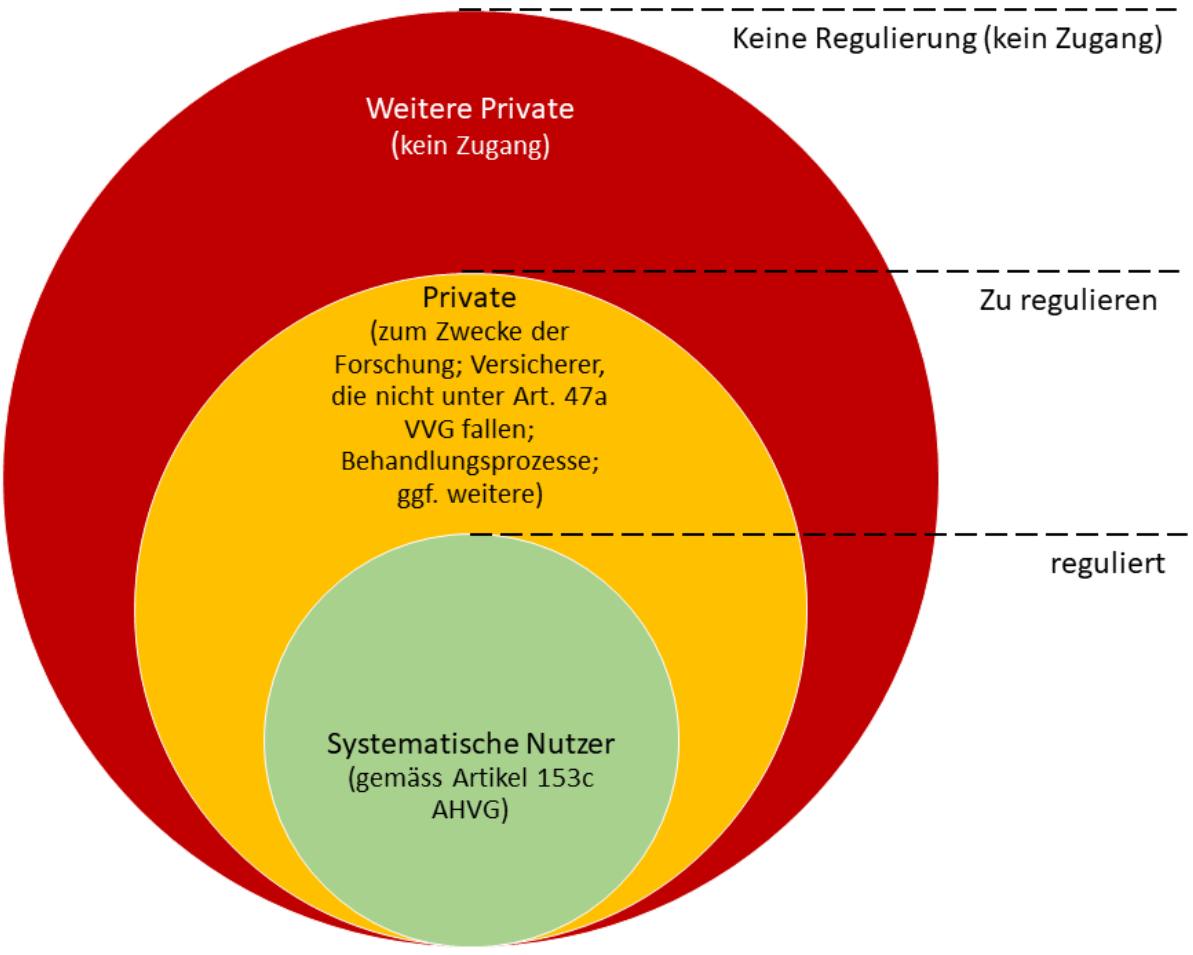
g. Sicherstellen, dass die verknüpften Daten nur den Forschenden und den verantwortlichen Mitarbeitern des Trust Centers zugänglich gemacht werden.
h. Datengebern, d.h. den einzelnen Personen, deren Daten verwendet werden, Auskunft über die Verwendung ihrer Daten erteilen.

2. Die folgenden Auflagen zur Verwendung der AHVN in Forschungsprojekten müssen rechtlich verankert werden:
    a. Für das Führen der AHVN in einem Forschungsprojekt muss eine Bewilligung des Trust Centers und/oder der zuständigen Ethikkommission eingeholt werden. Dabei sind bestehende rechtliche Regelungen zu beachten. Weitere notwendige rechtliche Regelungen sind ggf. zu schaffen.
    b. Für die Verknüpfung von Daten zu Forschungszwecken mit Hilfe der AHVN muss eine Bewilligung des Trust Centers eingeholt werden.
3. Die Verknüpfung der Datensätze darf nur durch das Trust Center erfolgen.
4. Die Daten aus den verknüpften Datensätzen dürfen von den Forschenden nicht in ihren eigenen Datenbestand integriert werden.

6 Hinweis zum Rechtsetzungsbedarf

Der Rechtsetzungsbedarf wird erst nach der Freigabe des Konzepts durch die FDMG abschliessend eruiert.

Die aktuelle Verwendung und der zu regulierende Bereich wird in der folgenden Grafik schematisch dargestellt:



Im Zuge der Diskussionen in der AG IP wurde bereits folgender Rechtsetzungsbedarf identifiziert:

- Der Kreis der systematischen Nutzer der AHVN ausserhalb der AHV (Art. 153c AHVG) soll erweitert werden. Dies betrifft z.B. Institutionen, die Daten zu Forschungszwecken bearbeiten, Leistungserbringer, die die Primärdokumentation führen, Institutionen, die etwa mit bundesrechtlichem Auftrag schweizweit vereinbarte Qualitätsregister führen, oder Krankenversicherer, die Zusatzversicherungen anbieten, die nicht unter Artikel 47a VVG fallen.
- Rechtliche Verankerung der Bewilligung zum Führen der AHVN in Datensätzen im Kontext der (gesundheitsbezogenen) Forschung, inkl. Register, die ohne bundesrechtlichen Auftrag geführt werden. Die Bewilligung zur Verwendung der AHVN im Rahmen von Forschungsprojekten soll im Einzelfall von einem Trust Center oder einer Ethikkommission erteilt werden.
- Ein Trust Center mit den in Kapitel 5 definierten Aufgaben muss rechtlich verankert werden.
- Die Verknüpfung von Daten für Forschungszwecke darf nur durch das Trust Center erfolgen.
- Falls für einen Anwendungsfall erforderlich, muss die Verwendung der AHVN durch Organisationen und Personen des öffentlichen oder privaten Rechts gemäss Artikel 153c Absatz 1 Buchstabe a Ziffer 4 AHVG in den entsprechenden spezialgesetzlichen Regelungen verankert werden.
- Rechtliche Verankerung der Anforderungen an mHealth-Apps, die die AHVN Führen wollen.

7 Anhang

7.1 Anhang 1: Szenarien Verwendung AHVN / Pseudonym

7.1.1 Szenario 1: Primärdokumentation / Führen von Daten in der elektronischen Krankengeschichte

Eine Gesundheitsfachperson (GFP) dokumentiert medizinische Daten wie die Anamnese, Diagnosen, Untersuchungsergebnisse, Röntgenaufnahmen, Medikationen etc. in der elektronischen Krankenakte einer Patientin/eines Patienten. Wenn eine weitere Behandlung erforderlich ist, muss die GFP in der Lage sein, die Daten direkt der betreffenden Person zuzuordnen und diese auch zu identifizieren. In diesem Fall soll die AHVN als Personenidentifikator verwendet werden, über die die konkrete Person eineindeutig identifiziert werden kann.

7.1.2 Szenario 2: Gerichtete Kommunikation zwischen Leistungserbringern

GFP A überweist die Patientin M an GFP B. GFP B muss in der Lage sein, die Überweisung und die zur Verfügung gestellten Unterlagen und medizinischen Daten eindeutig einer Person zuzuordnen, um die richtige Person aufbieten zu können und die Behandlung fortzusetzen. In diesem Fall soll die AHVN als Personenidentifikator verwendet werden, mit deren Hilfe die konkrete Person eineindeutig identifiziert werden kann.

7.1.3 Szenario 3: Forschungsprojekt mit Rückführung der Forschungsdaten auf eine Person

Im Rahmen eines Forschungsprojekts sollen Analysen durchgeführt werden, bei denen die Wahrscheinlichkeit hoch ist, dass die Ergebnisse für die betroffenen Personen potentiell schwerwiegende gesundheitliche Risiken offenlegen kann. In diesem Fall soll die betroffene Person über diese Risiken informiert werden können, damit entsprechende Massnahmen eingeleitet werden können, um gesundheitliche Schäden für die Person zu verhindern. In diesem Fall soll die AHVN als PID verwendet werden, über die die konkrete Person eineindeutig identifiziert werden kann.

7.1.4 Szenario 4: Forschungsprojekt bei dem Daten aus verschiedenen Quellen verknüpft werden sollen

Bei einem Forschungsprojekt werden personenbezogene Daten erhoben, deren Aussagekraft sich durch die Verknüpfung mit Daten aus anderen Quellen erhöht, bzw. deren Aussagekraft sich erst durch die Verknüpfung mit Daten aus anderen Quellen ergibt. Für die Verknüpfung der Daten braucht es über die zu verknüpfenden Datensammlungen hinweg einen einheitlichen PID. In diesem Fall soll die

AHVN als PID verwendet werden, da die AHVN als PID bereits in vielen Datensammlungen geführt wird und die entsprechenden Infrastrukturen zur Verwendung der AHVN vorhanden sind.

Im verknüpften Datensatz wird die AHVN durch ein Pseudonym ersetzt, dass, falls eine spätere Verknüpfung mit weiteren Daten erfolgen soll, oder die Rückführung von Daten auf eine bestimmte Person erforderlich wird, wieder auf die AHVN zurückgeführt werden können muss.

7.1.5 Szenario 5: Forschungsprojekte bei denen mit Daten gearbeitet werden soll, die nicht auf eine zu identifizierende Person zurückgeführt werden müssen

In einem Forschungsprojekt werden Daten verwendet, die zwar eindeutig einer Person zugeordnet werden müssen (Individualisierung des Datensatzes). Die konkrete Person muss für den Forschungszweck aber nicht bekannt sein (Personalisierung des Datensatzes). In diesem Fall soll ein Pseudonym der AHVN oder ein beliebiger anderer lokaler Identifikator verwendet werden, um die Daten eindeutig einem Individuum zuzuordnen. Die Identifikation der realen Person hinter dem Pseudonym kann bei Verwendung eines Pseudonyms der AHVN nur mittels eines Schlüssels erfolgen, der von einer Dritten vertrauenswürdigen Partei verwaltet wird.

7.1.6 Szenario 6: Implantateregister

In einem Implantateregister wird registriert, welche Person welches Implantat erhalten hat. In der Regel muss der Impantatträger nicht identifiziert werden können. Im Fall eines Produktfehlers, bzw. bei erst im Nachhinein festgestellten Risiken mit einem Implantat, kann es notwendig sein, die Implantatträger z.B. über Risiken oder über einen allfälligen Ersatz der Implantate zu informieren. In diesem Fall soll ein Pseudonym der AHVN verwendet werden, um die Daten im Implantateregister eindeutig einer Person zuzuordnen. Die Identifikation der realen Person hinter dem Pseudonym kann, wenn erforderlich, mittels eines Schlüssels erfolgen, der von einer Dritten vertrauenswürdigen Partei verwaltet wird.

7.2 Anhang 2: Stellungnahmen zu den Aussagen im Dokument

7.2.1 Stellungnahme der FMH

Die FMH bedankt sich für die Möglichkeit ihre von der AG PI abweichende Position zum Konzept Identifikatoren Personen darzulegen.

Aus datenschutzrechtlichen Gründen setzt sich die FMH für einen sektoriellen PID ein, da dieser insbesondere das Zweckbindungsgebot stärkt und gewährleistet, dass die Daten im Kontext des Gesundheitswesens verbleiben. Mit der EPR-SPID wird bereits ein sektorieller PID im Gesundheitsbereich eingesetzt und genutzt. Eine neue Gesundheitsnummer ist nicht notwendig und die Verwendung der AHV-Nummer als universeller Patientenidentifikator bringt zusätzliche Risiken.

Bei der AHVN als PID geht es nicht in erster Linie um das Risiko der Verknüpfung von Datenbanken. Vielmehr führt die breite Verwendung der AHVN dazu, dass es sich nicht mehr um einen "nicht-sprechenden" Personenidentifikator handelt, sondern um ein Personendatum, welches sich mit geringem Aufwand auf eine bestimmte oder bestimmbare Person zurückführen lässt. Die AHVN wird auf öffentlichen Dokumenten zusammen mit dem vollen Namen geführt (z.B. Versichertenkarte). Zudem besteht das hohe Risiko, dass möglichen Verknüpfungen von Gesundheitsdaten mit personenbezogenen Datenbeständen aus anderen Lebensbereichen (z.B. Steuerdaten, Strafregisterdaten) erfolgen können (Botschaft EPDG 2013, S. 5360.)

Auch braucht die gesundheitsbezogene Forschung keine personenbezogenen Daten (AHVN), sondern individualisierte Daten. Die Weitergabe von Personendaten für die Forschung gemäss HFG braucht eine Einwilligung, die Weitergabe von individualisierten, nicht personenbezogenen Daten aber nicht. Die AHVN ist deshalb ungeeignet resp. erschwert die Bekanntgabe (vgl. auch Vernehmlassung Revision EPDG Art. 19f und 19g.)

Der Nutzen für die im Konzept genannten Anwendungsfälle ist bei allen PID der gleiche. Unterschiedlich sind jedoch die technisch-organisatorischen Massnahmen zum Schutz und der Sicherheit der

Daten. Die Aussage, dass im Kontext des Gesundheitswesens nicht der verwendete PID der aus Datenschutzperspektive entscheidende Faktor ist, trifft nicht zu. Vielmehr ist es aus datenschutzrechtlicher Sicht nach Art. 7 Abs. 1 DSG verpflichtend, eine technische Lösung zu wählen, die insbesondere die Grundsätze nach Art. 6 DSG (u.a. Zweckbindungsgebot) gewährleistet. Das erfüllt nur ein sektorieller PID.

Position / Fazit der FMH

Die Argumente, welche gemäss Konzept für die AHVN sprechen, sind für die FMH nicht überzeugend, und viele Argumente, die im Konzept für die Verwendung der AHVN aufgeführt werden, sprechen auch oder sogar eher für einen sektoriellen PIN, wie EPR-SPID. Aus Sicht der FMH ist eindeutig der EPR-SPID zu verwenden, der bereits als sektorieller PID für den Gesundheitsbereich angelegt ist und gemäss Vernehmlassung zur Revision des EPDG im Gesundheitswesen auch weiterverbreitet werden soll, so insbesondere durch Schnittstellen für die Verwendung der Daten für die Forschung. Die Verwendung der AHVN als universeller Patientenidentifikator lehnt die FMH ab.

7.2.2 Stellungnahme der Digitalen Gesellschaft

Die Digitale Gesellschaft bedankt sich für die Möglichkeit, ihre von der AG abweichende Position zum Konzept Identifikatoren Personen darzulegen.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, sieht sich als Interessensvertreterin der Zivilgesellschaft und setzt sich ein für Datenschutz und die Verteidigung der Grund- und Menschenrechte im digitalen Raum.

Mit diesem Ziel teilt die Digitale Gesellschaft grundsätzlich die Datenschutzbedenken der FMH bezüglich des Konzepts Identifikatoren Personen im Gesundheitswesen, und lehnt deswegen eine Erweiterung des Verwendungszwecks der AHVN als Personenidentifikator ab.

Grundsätzlich fordern wir auch für die Identifikatoren Personen im Gesundheitswesen die Gewährleistung der informationellen Selbstbestimmung mit Vorgaben zu:

- einer Protokollierung der Zugriffe auf persönliche Gesundheitsdaten und der definierten Aufbewahrungsdauer der Protokollierung;
- das Auskunftsrecht gemäss Datenschutzrecht auch betreffend Datenzugriffe auf persönliche Gesundheitsdaten;
- Meldepflicht und konsequente Rechts-Durchsetzung bei missbräuchlichen Verwendung (zB. der AHVN).

Spezifische Vorschläge:

- Das Konzept schlägt als einzige Lösung einen, in breiten Bereichen verwendeten (‘universellen’) PID vor, der für die beschriebenen Anwendungsfälle die eindeutige Identifizierung von Objekten und Personen über Systemgrenzen hinweg ermöglichen soll. Die Verwendung verschiedener, sektorieller Identifikatoren (gemäss Standards wie IHE) wird zwar als vorteilhaft aus der Perspektive des Datenschutzes anerkannt, aber als zu aufwändig angesehen. Schwer nachvollziehbar erscheint hier, warum die international von Herstellern und Anwendern getriebenen Standards zu Datenstrukturen und Schnittstellen für Datenverarbeitungssysteme des Gesundheitswesens, welche am Markt eingeführt sind, als "zu aufwändig" angesehen werden.
- Das Konzept beschreibt ein “nur geringfügig erhöhtes Datenschutzrisiko” für die persönlichen Gesundheitsdaten durch einen "zusätzlichen PID" wie die AHVN. Etwas widersprüchlich ”sollen – gemäss den Empfehlungen der ZAS – in den Datensammlungen privatwirtschaftlicher Stellen, welche die AHVN verwenden, die Gesundheitsdaten und Personendaten getrennt bearbeitet werden."

=> "sollen" und "Empfehlung" sind in diesem Zusammenhang klar zu schwache Anforderungen, welche auch der Argumentation von "bereits vorhandenen weiteren personenidentifizierenden Daten" gegenlaufen. Herausgestellt seien beispielsweise Anwendungsfälle "impliziter Identifikation" durch individualisierte Datenerfassung mithilfe von mHealth Anwendungen auf persönlichen Smartdevices: Alle Identifkatoren des Smartdevices könnten aufgrund dieser schwachen Anforderungen mit der AHVN zusammengefasst werden. Es ist nicht verständlich, wie eine missbräuchliche Verwendung, etwa Profilierung, nachgewiesen und wirksam unterbunden werden könnte.

Deshalb **müssen** Personen-identifizierende nicht-medizinische Daten von Gesundheitsdaten getrennt gespeichert werden. Sie dürfen zweckgebunden zur Bearbeitung in konkreten Anwendungsfällen innerhalb angemessen gesicherter Umgebungen (zB Klinik- bzw. Praxisinformationssysteme) zusammengeführt werden. Über den Umfang und die Natur konkreter Anwendungsfälle geben die IHE Standards im Kontext "Identifkation von Patienten" erprobte Beispiele.

- Das vorliegende Konzept will auf Anwendungsfälle fokussieren, für die es noch keinen einheitlichen PID gibt. Dabei soll die AHVN laut dem vorliegenden Vorschlag für eine eindeutige (Selbst-)Identifikation der Patientin/des Patienten im Direktkontakt mit dem Leistungserbringer verwendet werden. Gleichzeitig soll ihre Verwendung in der Primärdokumentation erlaubt werden im Kontext von "medizinischen Behandlungen ohne Bezug zur Abrechnung und ausserhalb des Kontextes EPD".

Durch die laufenden Arbeiten an einer neuen Version des EPD und der Revision des EPDG (in Vernehmlassung) sind Umfang, Schnittstelle und die Wirkungsweise des zukünftigen "Kontextes EPD" noch nicht endgültig definiert. Zumindest ist unter dem Begriff 'Identifikationsmittel' (Art. 7 VE-EPDG) eine zukünftige Version einer E-ID vorgesehen für die Patienten-Identifikation und den Zugriff auf das EPD.
Die Anzahl der "medizinischen Behandlungen ohne Bezug zur Abrechnung und ausserhalb des Kontextes EPD" wird somit bei einer erfolgreichen Einführung eines EPD voraussichtlich vernachlässigbar klein. Damit bleibt der Nutzen der vorgeschlagenen Erweiterung der AHVN für weitere Spezialanwendungen (z.B. Kommunikation zwischen eRezept, mHealth-Apps, KIS, PIS oder EPD), welche ebenfalls von der endgültigen Ausgestaltung eines zukünftigen EPD abhängen, fraglich.

Speziell für mHealth Anwendungen wird im vorliegenden Konzept die Notwendigkeit einer fallspezifischen Bewilligung zur Verwendung der AHVN erkannt, ohne weitere Beschreibung der Kriterien der Bewilligung, wie etwa medizinische Wirksamkeit oder auch alternative (generische) Anwendungen. Eine Erfassung z.B. von Vitaldaten über Sensoren und Apps mit Integration in Systeme der Leistungserbringer nach heutigem Stand der Technik erzeugt weitere Metadaten mit impliziter Identifkation (siehe oben). Die konsequente Anwendung von sektoriellen IDs macht die systematische Zusammenführung und Auswertung durch berechtigte und unberechtigte Dritte transparent und ermöglicht den Patienten so erst die informationelle Selbstbestimmung.

Fazit und Empfehlung:

Ein Konzept 'Identifikatoren Personen im Gesundheitswesen' sollte die aufgeführten grundsätzlichen Forderungen berücksichtigen und darüber hinaus inhaltlich mit der laufenden Entwicklung beim Elektronischen Patienten Dossier (EPD) koordiniert erstellt werden, mit dem Ziel eines gesamtheitlichen Systems aus abgestimmten Bausteinen nach den datenschutzrechtlichen Prinzipien von «Privacy-by-Design».