

Workshop: Anonymisierung und Pseudonymisierung in Patientenversorgung und Forschung

Protokoll für die Sitzung vom 23. Mai 2016

Protokoll erstellt durch: Dr. Jens Schwanke, Dr. Johannes Drepper, Christof Isele, David Koeppel, Dr. Bernd Schütze

Datum: 23. Mai 2016

Uhrzeit: 10:00 – 17:30 Uhr

Ort: TMF Geschäftsstelle, Charlottenstraße 42/Ecke Dorotheenstraße, 10117 Berlin

Anwesende: siehe Liste

Formalia

- Begrüßung der Teilnehmer
- Darstellung der Zielsetzung: das primäre Ziel des Workshops ist es mögliche Lösungskonzepte für die Anonymisierung und Pseudonymisierung im Zusammenhang mit der EU Datenschutz-Grundverordnung (DS-GVO) zu identifizieren und nachfolgend weiterzuentwickeln

Top 1: Rechtliche Grundlagen

Referent/Moderator: Dr. Bernd Schütze

1.1 Darstellung der rechtlichen Grundlagen

siehe Folien

1.2 Diskussion

- Innerhalb der DSGVO findet sich keine Definition für die Anonymisierung von Daten¹.
- Die bisher in Deutschland verwendete faktische Anonymität existiert in der DS-GVO nicht mehr. Dr. Schütze betont, dass Daten, die bisher „faktisch anonym“ angesehen wurden, nach der DS-GVO als pseudonyme Daten anzusehen sind.
- Ebenso erfordert die Anonymisierung von Daten einen Erlaubnistatbestand. Johannes Drepper merkt an, dass ein Erlaubnistatbestand gemäß Art. 5 Abs. 1 lit. b für die Forschung vorhanden ist. Aus Sicht von Bernd Schütze müsste an dieser Stelle zum einen ein öffentliches Interesse vorhanden sein (und dabei dem zugehörigen Erwägungsgrund entsprochen werden, zum anderen ein entsprechendes europäisches oder nationales Recht als Erlaubnistatbestand gelten.
- Das Bundesministerium des Inneren überarbeitet aktuell das BDSG und will diese Überarbeitung bis 2017 abschließen. In der darauffolgenden Legislaturperiode soll mit der Ausarbeitung der optionalen Öffnungsklauseln bspw. für die Gesundheitsversorgung begonnen werden.
- Bernd Schütze schlägt daher vor, gemeinsam mit weiteren Fachgesellschaften bis Anfang 2017 Anforderungen für einen Gesetzentwurf für die Forschung und Qualitätssicherung in Deutschland zu

¹ Jedoch wird in Erwägungsgrund 26 festgehalten, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten

formulieren. Dabei sollen nicht nur große Verbundprojekte berücksichtigt werden, sondern auch kleinere Projekte, z.B. an einzelnen Universitätskliniken.

- Herr Drepper weist darauf hin, dass die TMF in die vom BMBF einberufene Arbeitsgruppe zur Begleitung des Gesetzgebungsprozesses eingebunden ist und auf diesem Weg Anregungen aus der med. Wissenschaft einbringen kann.

Top 2: Anforderungen der Datenverarbeiter

Moderatoren: Christoph Isele, Prof. Dr. Alfred Winter

2.1 *Vorstellen der Problemstellung aus Sicht der Forschung*

Referent: Prof. Dr. Alfred Winter

siehe Folien

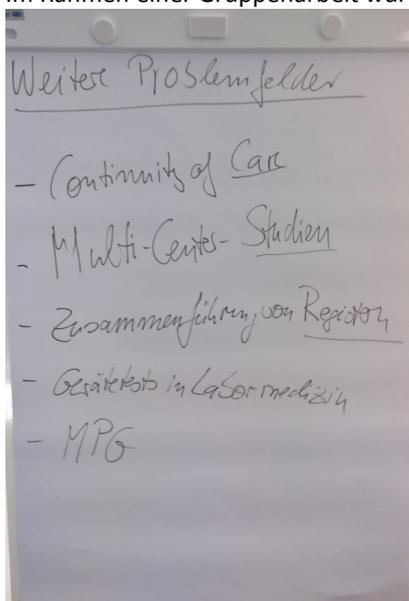
2.2 *Vorstellen der Problemstellung aus Sicht der Versorgung*

Referent: Christoph Isele

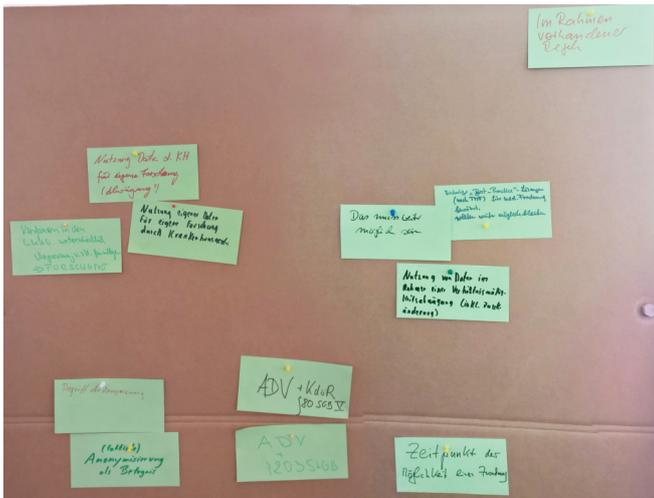
siehe Folien

2.3 *Diskussion*

- Aus Sicht von Alfred Winter muss nicht nur die klinische Forschung berücksichtigt werden, sondern auch die Forschung in der Medizinischen Informatik
- Christoph Isele sieht aus Sicht der Hersteller von Krankenhausinformationssystemen folgende Anforderungen an den Gesetzgeber:
 - Möglichkeiten zur Fehleranalyse auf personenbezogene Daten.
 - Interne Analysen von Datenbeständen bspw. zur Optimierung der Usability oder zur Produktverbesserung
 - die Möglichkeit Daten getriebene Anwendungen entwickeln, z.B. zur klinischen Entscheidungsunterstützung
- Im Rahmen einer Gruppenarbeit wurden folgende Problemfelder identifiziert:



- Aus Sicht der Teilnehmer sollten folgende Aspekte aus der bisherigen Gesetzgebung übernommen werden:



- Aus Sicht der Teilnehmer sollten folgende Anforderungen durch den Gesetzgeber berücksichtigt werden:



Top 3: Wann kann ich Daten als anonym ansehen?

Referent/Moderator: Gerald Spyra

3.1 Vorstellen der Problemstellung

siehe Folien

3.2 Diskussion

- Nur weil anonyme Daten nicht in der DSGVO genannt werden, gibt es diese dennoch (vgl. Erwägungsgrund 26).
- Es existieren zwei Möglichkeiten für anonyme Daten
 - Daten sind von Natur aus anonym
 - Personenbezogene Daten werden so verarbeitet, sodass diese anonym sind. Keiner darf in der Lage sein, eine Person mittels der Daten zu re-identifizieren
- Aus Sicht von Bernd Schütze wird die Verwendung von anonymen Daten für die medizinische Forschung und Qualitätssicherung immer unwahrscheinlicher, da immer mehr Möglichkeiten eine Re-Identifizierung erlauben und somit letztlich nur in wenigen Fällen anonyme Daten vorliegen dürften. Er verweist auf die Ausarbeitung der Artikel-29-Datenschutzgruppe zu Anonymisierungstechniken und deren Interpretation der Anonymität.

- Gerald Spyra sieht dies ebenso wie Bernd Schütze: es sollte nicht geprüft werden, wie anonyme Daten erzeugt werden können, sondern wie pseudonymisierte Daten ohne Einwilligung für die Forschung und Qualitätssicherung verwendet werden können.
- Prof. Dierks weist darauf hin, dass bei einer Einwilligung natürlich immer eine Aufklärung bzgl. des Re-Identifizierungsrisikos erfolgen muss, da ansonsten keine Informiertheit gegeben ist und eine Einwilligung ohne diese nicht rechtswirksam gegeben werden kann
- Es herrscht Konsens, dass idealerweise gesetzliche Erlaubnistatbestände für Forschung und Qualitätssicherung existieren sollten. Forschung und Qualitätssicherung mittels (pseudonymisierten) Daten muss ohne Einwilligung dennoch bestimmten Voraussetzungen genügen:
 - Sichere IT-Infrastruktur
 - Nutzung von Öffnungsklauseln der DSGVO
- Gewährleistung der Sicherheit entsprechend den Vorgaben der DS-GVO, insbesondere den Vorgaben von Artt. 5, 25, 32

Top 4: Umsetzungskonzepte zur Anonymisierung

4.1 Umsetzungskonzepte zur Anonymisierung

Referent: Dr. Johannes Drepper

siehe Folien

4.1.1 Diskussion

- Typische Techniken sind die Generalisierung und die Perturbation zur Anonymisierung von Daten.
- Diese Techniken vermindern das Re-Identifizierungsrisiko
- Die Nützlichkeit der Daten kann bei einer Anonymisierung - je nach Anwendungsfall - bestehen bleiben.
- Bedacht werden muss, dass durch eine Anonymisierung die Varianz verändert werden kann und somit statistische Auswertungen aus anonymisierten Datenbeständen ggfs. nicht mit der Auswertung der nicht-anonymisierten Daten übereinstimmen.

4.2 Umsetzungskonzepte und Möglichkeiten der Pseudonymisierung

Referenten: Martin Bialke

siehe Folien

4.2.1 Diskussion

- Zur Erhöhung der Sicherheit bietet sich die Verwendung von Pseudonymen in mehreren Stufen (bspw. unterschiedliche Pseudonyme je Datentyp: Bioproben, Phänotyp, Bilddaten...) an.
- Ein Datentreuhänder darf in keinem Fall ein Auftragsverarbeiter sein, da sonst die Weisungsfreiheit des Datentreuhänders nicht vorhanden ist.
- Es soll überlegt werden, ob der Begriff und die Aufgaben des Datentreuhänders in einen Vorschlag für ein Forschungsgesetz aufgenommen wird.

4.3 Zusammenfassende Diskussion

Moderation: Prof. Dr. Klaus Pommerening

- Die Anonymisierung von Daten macht diese, je nach Anwendungsfall, unbrauchbar für die Forschung.
- Die Pseudonymisierung dient in der DS-GVO als Maßnahme zur Reduktion des Re-Identifizierungsrisikos.
- Aktuell existieren für Forscher in Deutschland viele Freiräume, jedoch werden diese durch die DS-GVO wahrscheinlich vermindert.
- Bei einer Ausarbeitung muss das gesamte Spektrum von multizentrischer Forschung über klinische Projekte bis hin zur außeruniversitären Forschung in der Industrie und in Instituten betrachtet werden.

Top 5: Zusammenfassung / Diskussion

Referent: Dr. Bernd Schütze

- Die nationalen Öffnungsklauseln sollen möglichst für alle Bundesländer einheitlich gestaltet werden.
- Gemeinsam mit anderen Fachgesellschaften sollten Anforderungen an ein Rahmengesetz bzgl. Forschung und Qualitätssicherung gesammelt und an die Gesetzgeber herangetragen werden:

- Management Summary für die Ministerien
 - White Paper für die Inhalte eines Forschungsrahmengesetzes
- Ziel sollte es sein, dass Management Summary sowie das White Paper im Verlauf des nächsten Jahres zu erstellen.