



Berlin, 13. März 2019

Stellungnahme zum Datenschutzkonzept für die Clinical Communication Platform (CCP-IT) im Deutschen Konsortium für Translationale Krebsforschung (DKTK)

Das Datenschutzkonzept für die CCP-IT wurde von der TMF-Arbeitsgruppe „Datenschutz“ mehrfach, zuletzt auf der Sitzung am 13. März 2019, beraten. Der AG liegt das Konzept in der Version vom 28. Februar 2019 vor. Es handelt sich um eine Fortschreibung des Konzepts vom 8. Januar 2014, das am 16. Januar 2014 von der Arbeitsgruppe befürwortet wurde.

Das vorliegende Konzept beschreibt eine Plattform, die neben der Bereitstellung von Infrastruktur-Komponenten (wie Datenintegrations-, Pseudonymisierungs- und Authentifizierungsprozessen) vor allem Anfragen nach Fallzahlen und Machbarkeit von Forschungsprojekten ermöglichen soll. Zu diesem Zweck werden medizinische Daten von Krebspatienten (einschließlich Hinweisen auf vorhandene Biomaterialproben) der teilnehmenden Kliniken pseudonymisiert in einer zentralen Datenbank, der „MDS-Datenbank“, gesammelt, in der Regel beruhend auf einer entsprechenden Einwilligung der betroffenen Patienten. Da die Datenbank Pseudonyme verwendet, die ansonsten nur in der Patientenliste bekannt sind, erfüllt das Konzept die Anforderungen an das Klinische Modul des TMF-Datenschutzleitfadens. Im zentralen Identitätsmanagement können auch verschiedene Pseudonyme (im Sinne eines Privacy Preserving Record Linkage) verknüpft werden. Insofern, als

- überhaupt kein Online-Zugriff außer statistischen Abfragen auf die zentrale Datenbank vorgesehen ist,
 - ein zusätzlicher Schutz durch die Umwandlung lokaler in globale Pseudonyme eingerichtet ist,
- ist das Konzept sogar deutlich strenger als das generische TMF-Konzept. Die konkrete Ansiedlung der Datenbanken bei verschiedenen Institutionen unterstützt eine wirksame informationelle Gewaltenteilung. Die Besetzung des Ausschusses Datenschutz ist konkret in Form der beteiligten Rollen beschrieben.

Parallel dazu sollen aber auch Daten von Patienten nutzbar gemacht werden, für die keine explizite (DKTK-) Einwilligung vorliegt. Hierbei handelt es sich um „Altfälle“, auch von Kooperationspartnern, die onkologische Spitzenzentren, aber nicht Mitglieder des DKTK sind. Die Erforderlichkeit, solche Fälle ohne vorliegende explizite Einwilligungserklärung einzubeziehen, ist im Abschnitt 6.2 des Konzepts ausführlich begründet. Zunächst sind dies sehr viele, die Anzahl wird aber im Laufe der Zeit abnehmen, da neue Fälle grundsätzlich nur mit Einwilligung aufgenommen werden, und bei Altfällen die Einwilligung nach Möglichkeit (bei Weiterbehandlung) nachgeholt werden soll. Für die Daten dieser Patienten, als „nicht explizit eingewilligte Patienten“ bezeichnet, sind je nach Rechtslage zwei Optionen vorgesehen:

- Sie werden nur in den behandelnden Einrichtungen in einem sogenannten Brückenkopf gespeichert, der nicht von außerhalb zugänglich ist. Dieser ist nach dem Modell eines klinischen Data-Warehouse konzipiert und muss natürlich den entsprechenden lokal geltenden Datenschutzregeln genügen. Hierfür beherbergt er ein lokales





Identitätsmanagement, das natürlich auch an anderer Stelle (des gleichen Standorts) angesiedelt sein kann. Die Plattform erlaubt keine direkten Abfragen auf die zugehörigen Datenbestände dieser Patienten, sondern dient nur zur Vermittlung von externen Anfragen nach Fallzahlen, die vor Ort außerhalb dieses Systems im Rahmen der rechtlich erlaubten Möglichkeiten bearbeitet werden. Die Bearbeitung solcher Anfragen betrifft nicht die Plattform selbst und ist daher nicht Gegenstand des vorliegenden Datenschutzkonzepts.

- Unter der Voraussetzung, dass die am Ort der Entstehung geltenden Datenschutzregeln einen pseudonymisierten Datenexport erlauben, z. B. aufgrund einer vom DKTK unabhängigen Einwilligung für Forschungszwecke oder Forschungsklauseln in einem Landeskrankengesetz, wird ein reduzierter Datensatz nach expliziter Freigabe in die zentrale Datenbank geladen. Die Prüfung der Zulässigkeit liegt in der Verantwortung der kooperierenden Einrichtung. Da in diesem Fall kein globales Pseudonym erzeugt wird, ist hierbei eine Verknüpfung mit Daten derselben Person aus anderen Quellen nicht möglich.

Neu im Vergleich zum Konzept von 2014 sind im Wesentlichen die Punkte:

- Anpassungen an die DSGVO,
- Einbeziehung zusätzlicher Kooperationspartner in Form von behandelnden Einrichtungen, die nicht Mitglieder des DKTK sind,
- zusätzliche Anwendungsfälle („CCP-Anwendungen“), die die Infrastruktur und auch die Datenbank der Plattform nutzen,
- eventuelle Speicherung von Daten in der zentralen Datenbank ohne explizite Einwilligung,
- Modifikationen in den Pseudonymisierungsprozessen.

Verantwortliche Stelle für die Datenverarbeitung ist das Deutsche Krebsforschungszentrum (DKFZ) in Heidelberg, z. T. in gemeinsamer Verantwortung mit den teilnehmenden Kooperationspartnern.

Die AG Datenschutz sieht in dem Teil des Konzepts, der Patienten mit Einwilligung betrifft, eine Umsetzung einer strengeren Variante des Klinischen Moduls des TMF-Datenschutzleitfadens. Der Teil, der für Patienten ohne Einwilligung nur die Weiterleitung von externen Anfragen vorsieht, wird als unproblematisch bewertet. Nicht Gegenstand dieser Stellungnahme sind

- die Einwilligungserklärungen, die in der jeweiligen Verantwortung der teilnehmenden Einrichtungen liegen,
- die rechtlich bindenden vertraglichen Regelungen mit Kooperationspartnern,
- die rechtliche Würdigung der eventuellen zentralen Speicherung von Daten ohne Einwilligung aufgrund spezieller Rechtsgrundlagen,
- die Datenschutzkonzepte von CCP-Anwendungen, insbesondere die Einschätzung des Reidentifizierungsrisikos durch Speicherung zusätzlicher Daten.

Ansonsten hat die AG keine Einwände gegen das vorgelegte Konzept.

Prof. Dr. Klaus Pommerening
Sprecher der AG Datenschutz
und verantwortlicher Berichterstatter