



Berlin, 17. September 2014

Stellungnahme zu den Schablonen zur Erstellung eines Datenschutzkonzepts für ein OSSE-Register und zur Ergänzung eines Datenschutzkonzepts bei Einsatz eines OSSE-Brückenkopfs

Die Schablonen wurden von der TMF-Arbeitsgruppe „Datenschutz“, zuletzt auf der Sitzung am 16. September 2014, beraten. Der AG lagen sie in der Version vom 16. August 2014 vor.

Hierbei handelt es sich nicht um Datenschutzkonzepte für konkrete Projekte, sondern um Vorlagen, die für ein jeweils konkretes Projekt ergänzt werden müssen. Bei den betroffenen Projekten handelt es sich um Register für seltene Krankheiten, die mit Hilfe der OSSE-Register-Software aufgesetzt werden oder mit Hilfe eines Brückenkopfs in das OSSE-System eingebunden werden.

Für ein OSSE-Register wird ein offener Ansatz verfolgt, der verschiedene Varianten unterstützt. Durch den Einsatz der OSSE-Software werden bereits datenschutzgerechte Prozesse definiert, die z. B. eine angemessene informationelle Gewaltenteilung berücksichtigen und die Kontrolle von Datenexporten unterstützen.

Bei dem Brückenkopf handelt es sich um eine Schnittstelle für Register, die mit anderer Software aufgesetzt sind. Hierbei wird vorausgesetzt, dass ein solches Register bereits sein eigenes Datenschutzkonzept hat; es werden nur die zusätzlichen Maßnahmen für die Einbindung beschrieben. Die Einbindung bedeutet dabei nur, dass dezentrale Machbarkeitsanfragen für Studien unterstützt werden, die dann register-intern „manuell“ gemäß dem dort gültigen Datenschutzkonzept bearbeitet werden; ein automatischer Datenexport findet nicht statt. Insofern wird das Konstrukt eines OSSE-Brückenkopfs in dieser generischen Version von der AG als unkritisch und bei geeignetem Gesamtkonzept als zustimmungsfähig angesehen.

Die Varianten für ein OSSE-Register unterscheiden sich durch die unterschiedliche Position des Identitätsmanagements. In Variante 1 wird ein gemeinsames zentrales Identitätsmanagement für mehrere gleichartige Register genutzt, in Variante 2 ein zentrales Identitätsmanagement nur für dieses eine Register. Variante 3 schließlich sieht eine lokale Pseudonymisierung an der jeweiligen Datenquelle vor. Bei den Varianten 2 und 3 wird dabei auf die Zusammenführbarkeit von Daten aus verschiedenen Registern bzw. Datenquellen verzichtet.

Das zentrale Identitätsmanagement verwaltet IDAT (außer bei Variante 3) und zwei Stufen von Pseudonymen, PID und PSN. Ein getrennt angesiedelter Pseudonymisierungsdienst zum Übergang zwischen diesen beiden Pseudonymen ist nicht vorgesehen. Das ist im Sinne des TMF-Datenschutzleitfadens verhältnismäßig, da ein OSSE-Register im Wesentlichen einem klinischen Modul entspricht, wo der zweite Pseudonymisierungsschritt gar nicht erforderlich wäre. Er ist hier aber





sinnvoll, damit der bei Variante 3 an der Datenquelle bekannte PID nicht im Register bekannt werden muss.

Für die Einbindung von Proben werden zwei Varianten angeboten: einmal eine Biobank, die Proben zentral sammelt und verschlüsselte Verweise darauf ins Register übermittelt, zum anderen eine dezentrale Aufbewahrung der Proben mit ebenfalls verschlüsselten Verweisen darauf im Register. Beides ist mit dem TMF-Datenschutzleitfaden, insbesondere mit dem Datenschutzkonzept für Biomaterialbanken im Einklang.

Während technische Details eines konkreten Datenschutzkonzepts gemäß diesen Schablonen durch den Einsatz des OSSE-Systems schon weitgehend vorgegeben sind, können organisatorische Details naturgemäß auf einer generischen Ebene noch nicht festgelegt werden. Insbesondere müssen die rechtlichen Verantwortlichkeiten für jedes Projekt spezifisch definiert werden. Die Schablonen sehen solche Definitionen auch vor. Für die Rolle des Ausschusses Datenschutz ist ein „Registerausschuss“ vorgesehen.

Die AG Datenschutz sieht in den vorgelegten Schablonen eine wirksame Hilfe zur Erstellung eines Datenschutzkonzepts für ein Register im Sinne eines klinischen Moduls, das den Anforderungen des TMF-Datenschutzleitfadens genügt. Daher empfiehlt die AG die vorgelegten Schablonen in passenden Fällen anzuwenden.

Univ.-Prof. Dr. K. Pommerening
Sprecher der Arbeitsgruppe Datenschutz