Personenregistrierung

Die dezentrale Datenhaltung der MII sieht diverse Verantwortlichkeiten bei den Standorten und den zentralen Komponenten, wie der federated Trusted Third Party (fTTP). Die fTTP teilt sich auf in zwei Komponenten: fTTP-Probability für die Personenregistrierung mittels Bloomfilter und fTTP-Clearing (Clearingstelle) für die Dublettenauflösung wenn eine Zuordnung von Bloomfiltern nicht zweifelsfrei erfolgen kann. Da die Personenregistrierung beim Standort beginnt, sind hier einige Voraussetzungen genannt, welche ein Standort adressieren muss. Die Personenregistrierung bei der fTTP ist in den Abschnitten zum Privacy-Preserving Record Linkage und Clearing beschrieben.

Lokale Registrierung

Jeder MII/NUM-Standort hat während der Aufbauphase der MII eine lokale Treuhandstelle (diese kann auch im DIZ verortet sein. Relevant sind die treuhändischen Funktionalitäten, welche bereitgestellt werden müssen) etabliert. Personendaten werden dabei in einem Identitätsmanagement verwaltet. Dabei werden in der Regel für verschiedene Kontexte Pseudonyme vergeben, welche im Pseudonym-Management verwaltet werden. Um die Betroffenenrechte umzusetzen, werden lokal erhobene Einwilligungen und Widerrufe (und Widersprüche) in einem Einwilligungsmanagement verwaltet. Dies ermöglicht ebenfalls das Abrufen aktueller Einwilligungsstände.

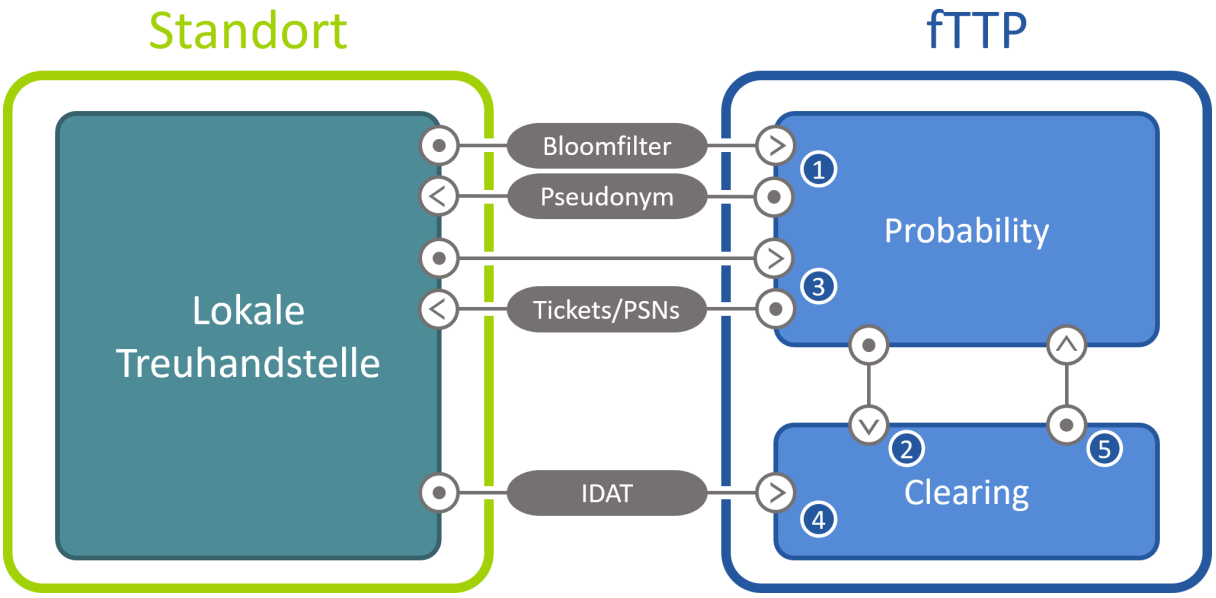
Die identifizierenden Personendaten (IDAT) liegen ausschließlich in der lokalen Treuhandstelle. Um übergreifende Abgleiche mittels Privacy-Preserving Record Linkage durchzuführen, muss anhand einer Teilmenge der identifizierenden Daten ein Bloomfilter erzeugt werden. Dieser muss einmalig bei der fTTP registriert werden. Es kann vorkommen, dass zu einer Person mehrere Ausprägungen von IDAT bekannt sind (z.B. aus unterschiedlichen Systemen, Tippfehler, veränderte Daten wie Namensänderung nach Heirat oder Adressänderungen). Solche möglichen Dubletten sollten beim Standort aufgelöst werden und derselben Person zugeordnet werden. Sollten vor der ersten Registrierung bereits mehrere Ausprägungen vorliegen, so sollte die korrekte Ausprägung (oder als korrekt angesehene Ausprägung) die Grundlage für die Registrierung bei der fTTP sein. Sollten nach erstmaliger Registrierung bei der fTTP Dubletten aufgelöst werden, so ist die Registrierung weiterer Ausprägungen bei der fTTP nicht erforderlich. Es ist jedoch möglich, Änderungen der IDAT (die auch zu einem geänderten Bloomfiltern führen können), der fTTP mitzuteilen, indem der neue Bloomfilter übermittelt wird. Hierbei muss das zuvor erhaltene übergreifende Pseudonym übermittelt werden, sodass der Bloomfilter korrekt zugeordnet werden kann.

Je nach verwendeter Softwarelösung kann der Bloomfilter direkt bei der lokalen Registrierung erzeugt und mitgespeichert werden, oder erst für die Registrierung bei der fTTP ad-hoc generiert werden. Dabei ist zu beachten, dass eine Übertragung von Bloomfiltern (codierten IDAT) und IDAT nur auf Basis einer gültigen Einwilligung (in diesem Fall dem Broad Consent) erfolgen darf. IDAT (auch nicht codierte IDAT) von Personen, zu denen keine gültigen Einwilligungen vorliegen, dürfen nicht an die fTTP übermittelt werden. Die Verantwortung dies sicherzustellen, liegt beim Standort. Die fTTP kann dies nicht prüfen. Sollte eine Person zwischenzeitlich ihre Einwilligung widerrufen, so muss dies der fTTP entsprechend mitgeteilt werden. Die fTTP löscht daraufhin den Datensatz vom Standort.

Das übergreifend gültige Pseudonym, welches durch die fTTP vergeben wird, muss in der lokalen Treuhandstelle der jeweiligen Person zugeordnet werden. Anhand dessen können Personen übergreifend zusammengeführt werden.

Privacy-Preserving Record Linkage

Die initiale Registrierung einer Person je Standort erfolgt immer mittels Bloomfilter. Innerhalb der fTTP werden Personen nur über die Bloomfilter repräsentieren (da anders als in der lokalen Treuhandstelle, liegen keine IDAT vor). Die fTTP führt damit ein Privacy-Preserving Record Linkage (PPRL) durch und vergibt Projekt-spezifisch, Standort-übergreifend gültige Pseudonyme. Bloomfilter können im Vergleich zu anderen Hashing-Verfahren auf Ähnlichkeiten miteinander abgeglichen werden. Ähnlichkeiten in den zugrunde liegenden IDAT zeigen sich auch im Bloomfilter. Die fTTP ordnet identische oder sehr ähnliche Bloomfilter derselben Person zu. Bloomfilter die eine hinreichend hoher Übereinstimmung aufweisen, jedoch nicht zweifelsfrei einer Person zugeordnet werden können, werden als potentielle Dublette angesehen und müssen durch das Clearing aufgelöst werden (siehe „Bei Bedarf: Clearing/Dublettenauflösung“).



Schnittstelle 1 dient zur Registrierung eines Bloomfilters. Die FHIR-Schnittstelle ist unter https://www.ths-greifswald.de/fttp/fhir/requestPsnFromBfWorkflow beschrieben.

Je nach Ergebnis des Record Linkages, werden Pseudonyme vergeben:

1. Ein Bloomfilter wurde erstmalig registriert: Es wird ein neues Pseudonym erzeugt und direkt in der Antwort zurückgeliefert.
2. Ein Bloomfilter ist identisch oder sehr ähnlich zu einem bestehenden Bloomfilter und wird der Person zugeordnet: Das bereits erzeugte Pseudonym zu der Person wird zurückgeliefert.
3. Ein Bloomfilter hat hinreichende Ähnlichkeit zu einem bestehenden Bloomfilter, kann aber nicht zweifelsfrei der Person zugeordnet werden: es wird bis zur Auflösung der möglichen Dublette kein Pseudonym erzeugt. Der Standort der den Bloomfilter geschickt hat bekommt eine entsprechende Rückmeldung, dass nun ein Clearing durchgeführt wird. Standorte, die zuvor ähnliche Bloomfilter übermittelt haben, bekommen eine Mitteilung (über das Ticketsystem, siehe Abschnitt Clearing/Dublettenauflösung), dass nun ein Clearing ausgeführt werden muss. Nach dem zu welchem Ergebnis das Clearing kam, wird ein neues Pseudonym erzeugt oder ein vorhandenes Pseudonym dem Standort mitgeteilt.

Bei Bedarf: Clearing/Dublettenauflösung

Ein Clearing wird immer dann ausgelöst, wenn ein Bloomfilter nicht zweifelsfrei einer Person zugeordnet werden kann. Dies bedingt, dass mindestens ein Standort bereits zuvor einen ähnlichen Bloomfilter registriert hat. Dieser Standort hat für diese Person bereits ein Pseudonym erhalten. Die fTTP stellt ein Ticketsystem bereit, welches automatisiert abgefragt werden kann und die Standorte über erforderliche Clearing-Prozesse informiert. Diese Schnittstelle ist in der fTTP-Probability verortet (Schnittstelle 3). Die FHIR-Schnittstelle ist unter https://www.ths-greifswald.de/fttp/fhir/requestTasks beschrieben. Es wird empfohlen, dieses zumindest einmal täglich abzurufen. Hierrüber erhalten Standorte, welche bereits ein Pseudonym zu einer Person erhalten haben, bei Bedarf eine Mitteilung das zu einer Person die IDAT (eine festgelegte Teilmenge der IDAT) an die Clearingstelle übermittelt werden müssen. Der Standort, welcher einen Bloomfilter registrieren wollte, dieser jedoch nicht eindeutig zugeordnet werden konnte, erhält diese Mitteilung direkt als Antwort auf die Anfrage. Die fTTP-Probability informiert die fTTP-Clearing intern (Schnittstelle 2).

Die Clearingstelle ist zwar Teil der fTTP, jedoch sind die Systeme voneinander getrennt, sodass niemals IDAT und Bloomfilter auf demselben System liegen. Die Standorte übermitteln die angeforderten IDAT mittels einer eindeutigen Kennung (die im Ticket enthalten ist) and die Clearingstelle. Hierbei wird Schnittstelle 4 der fTTP-Clearing verwendet. Die FHIR-Schnittstelle ist unter https://www.ths-greifswald.de/fttp/fhir/providePatientData beschrieben. Die fTTP-Clearing sammelt die IDAT solange, bis alle Standorte die jeweiligen IDAT übermittelt haben, maximal jedoch drei Werktage. Danach werden die IDAT restlos und unwiederbringlich gelöscht. Die jeweiligen Bloomfilter werden dann als separate Personen angesehen. Hierbei können Synonymfehler entstehen, wodurch die Qualität bei späteren Auswertungen negativ beeinflusst werden kann. Haben alle Standorte innerhalb der angegebenen Zeit die IDAT übermittelt, findet ein konventionelles Record Linkage statt. Dabei werden die IDAT automatisiert miteinander verglichen. Sollte es dabei zu einem eindeutigen Ergebnis kommen (Daten sind im Klartext sehr ähnlich oder unterschieden sich deutlich), so wird dieses Ergebnis an die fTTP-Probability übermittelt (Schnittstelle 5). Sollte es auch hier nur hinreichend große Ähnlichkeiten geben, so findet ein zusätzlicher manueller Abgleich statt. Dabei schaut eine Person über die Daten und kann bei Unklarheiten die Standorte befragen oder Rückmeldung zu offensichtlichen Fehlern geben (z.B. Tippfehler). Danach erfolgt die eindeutige Auflösung. Das Ergebnis wird der fTTP mitgeteilt. Die IDAT werden danach unwiederbringlich bei der Clearingstelle gelöscht. Eine Zusammenführung von IDAT und Bloomfiltern findet zu keiner Zeit statt.

Je nach Ergebnis erzeugt die fTTP nun ein neues Pseudonym oder liefert das bestehende Pseudonym einer Person an den Standort, welcher einen Bloomfilter registrieren wollte, der nicht eindeutig zugeordnet werden konnte. Dies geschieht über das Ticketsystem (Schnittstelle 2 der fTTP-Probability).

Grundsätzlich gilt, dieser Vorgang muss nur einmal erfolgen. Ein Bloomfilter, der zunächst nicht eindeutig zugeordnet werden konnte, wird danach in jedem Fall eindeutig zugeordnet, sodass eine spätere Registrierung (z.B. von einem anderen Standort), nie zu einem Clearing-Prozess führt.