

Anwenderhandbuch



Version 2.13.0 vom 15.08.2021

Herausgeber:

Unabhängige Treuhandstelle der Universitätsmedizin
Greifswald K.d.ö.R.

Ersteller:

Christopher Hampf, M.Sc.

Ellernholzstr. 1-2
17475 Greifswald

Tel. 03834 / 86-7851, Fax: 03834 / 86-6843

E-Mail: christopher.hampf@uni-greifswald.de

Versionierung

Version	Datum	Bearbeitungsart / Betroffene Abschnitte	Bearbeiter
1.0	08.02.2019	Update und Erweiterung der Doku von mosaic-greifswald.de	Christopher Hampf
2.10	18.12.2019	Erweiterung und Anpassung für gICS 2.10.0	Christopher Hampf und Martin Bialke
2.11	06.02.2020	Erweiterung und Anpassung für gICS 2.11.0	Christopher Hampf und Martin Bialke
2.12.0	03.03.2021	Aktualisierung der Bilder zu Benutzeroberflächen Ergänzungen zu neuen Funktionalitäten Autorisierung/Authentifizierung überarbeitet FHIR Gateway ergänzt Logging ergänzt Upgrade ergänzt	Christopher Hampf und Martin Bialke
2.12.1	11.03.2021	Erweiterung und Anpassung für gICS 2.12.1	Christopher Hampf und Martin Bialke
2.13.0	15.06.2021	Erweiterung und Anpassung für gICS 2.13.0	Martin Bialke
2.13.0	15.08.2021	Textmarkenfehler bereinigt, neue Downloadlinks	Martin Bialke

Inhalt

Versionierung	2
Inhalt	3
Abbildungsverzeichnis	4
Tabellenverzeichnis	6
1 Hintergrund	7
2 Der generische Informed Consent Service (gICS)	7
3 Begriffsbestimmungen	9
4 Symbolverzeichnis	10
5 Funktionalitäten	11
5.1 Was leistet der Dienst (Auszug).....	11
5.2 Was leistet der Dienst nicht.....	11
6 Installation	11
6.1 Systemanforderungen	11
6.2 Download und Starten des Dienstes	12
7 Die grafische Oberfläche des gICS	14
7.1 Anlegen von Domänen	15
7.2 Erstellung einer Vorlage für Einwilligungen.....	18
7.3 Erstellung einer Vorlage für Widerrufe bzw. Verweigerungen	22
7.4 Erfassung von Einwilligungen, Widerrufen und Verweigerungen	22
7.5 Abfragen von Einwilligungsdetails.....	25
7.6 Bearbeiten, Duplizieren und Finalisieren.....	26
7.7 Gültigkeit von Einwilligungen und Modulen automatisch ablaufen lassen	27
7.8 Dokumenten-Suche (Ermittlung des zeitlichen Verlaufs).....	30
7.9 Durchführung von Analysen	31
7.10 Export und Import von Domänenkonfigurationen und Vorlagen	32
7.11 Vorlagendruck und automatische Erkennung von Einwilligungsinhalten	34
8 Qualitätsstatus	36
9 Logging	37
10 FHIR-Unterstützung für gICS per TTP FHIR-Gateway	37
Festlegung des SAFE_SIGNERID_TYPE	39
Individualisierung von FHIR Ressourcen	39
Absicherung des FHIR-Gateway-API per Keycloak.....	41

11	Authentifizierungs- und Autorisierung	41
11.1	Verwendung von KeyCloak	42
11.2	Verwendung von gRAS.....	42
12	Empfehlungen zur Absicherung des Anwendungsservers	45
13	Health Check	45
13.1	Abfrage	46
13.2	Konfiguration	47
14	Upgrade	47
15	Nutzung der Soap-Schnittstelle	48
15.1	Abruf von Consent Informationen.....	48
15.2	Abruf eines Consent Policy Status	50
16	Publikationen und Vorträge	53
17	Weiterführende Informationen	54

Abbildungsverzeichnis

Abbildung 1-1: Ablauf der Consent Verwaltung von der Erstellung der Einwilligung über die Ausfüllung durch den Patienten bis zum Import in den gICS.....	7
Abbildung 2-1: Die Einwilligungen und Widerrufe der Studien werden in modularer Form mittels des gICS verwaltet.	8
Abbildung 6-1: Aktuelle Architektur des gICS Docker Containers am Beispiel der Version 2.13.0.....	12
Abbildung 7-1: Überblick der Attribute, welche bei den jeweiligen Bausteinen gesetzt werden können. Attribute mit gestrichelten Rand sind optional, alle anderen sind Pflichtattribute und müssen (zumindest leer) gesetzt werden.	15
Abbildung 7-2: Oberfläche zum Anlegen einer neuen Domäne.	16
Abbildung 7-3: Auflistung aller erstellten Domänen. Eine Domäne wurde angewählt und das entsprechende Kontextmenü wird dargestellt.	17
Abbildung 7-4: Oberfläche zum Anlegen einer neuen Policy.....	19
Abbildung 7-5: Oberfläche zum Anlegen eines neuen Moduls.....	20
Abbildung 7-6: Oberfläche zum Erstellen einer neuen Vorlage.....	21
Abbildung 7-7: Oberfläche zur Erfassung einer neuen Einwilligung.	23
Abbildung 7-8: Kontextmenü zu einer Einwilligung.	24

Abbildung 7-9: Überblick der Attribute einer im gICS abgebildeten Einwilligung. Attribute mit gestrichelten Rand sind optional, alle anderen sind Pflichtattribute und müssen (zumindest leer) gesetzt werden.	25
Abbildung 7-10: Detailansicht einer Einwilligung. Hierbei kann der Einwilligungsstatus jedes Moduls eingesehen werden. Dabei ist auch ersichtlich, wann ein Modul abläuft, sofern ein Ablaufdatum oder -zeitraum definiert wurde (siehe Abschnitt 7.7).	26
Abbildung 7-11: Kontextmenü mit den Aktionen Bearbeiten, Duplizieren und Löschen am Beispiel von Policies.	27
Abbildung 7-12: Definition eines Ablaufs einer Einwilligung, hier am Beispiel eines Ablaufzeitraums.	28
Abbildung 7-13: Definition eines Ablaufdatums eines Moduls.	29
Abbildung 7-14: Oberfläche zur exemplarischen Suche von Dokumenten.	30
Abbildung 7-15: Oberfläche beim exemplarischen Finden von Einwilligungen und Widerrufen.	31
Abbildung 7-16: Ermittlung des Einwilligungsstatus einer Policy für eine gegebene Liste von Teilnehmern.	32
Abbildung 7-17: Oberfläche beim exemplarischen Export der Vorlage „Patienteneinwilligung MII [Allgemein]“	33
Abbildung 7-18: Import von Vorlagen und weiteren Inhalten: das Vorschau-Fenster zeigt, welche Inhalte bereits im gICS vorhanden sind und ggf. ob auf Wunsch diese überschrieben werden sollen. Hierzu wird das Kontrollkästchen <i>Aktualisierung vorhandener Elemente erlauben</i> angewählt.	34
Abbildung 7-19: Es können mehrere Exemplare von Einwilligungsvorlagen auf einmal gedruckt / als PDF exportiert werden. Dabei können für jedes Exemplar Signer-IDs vorgeben werden.	35
Abbildung 7-20: Automatische Erkennung der Einwilligungsinhalten bei Import einer gescannten Einwilligung im PDF-Format.	35
Abbildung 7-21: Automatische Erkennung der Einwilligungsinhalten bei Import einer gescannten Einwilligung im PDF-Format.	36
Abbildung 8-1: Dialog zum Setzen oder Ändern des Qualitätsstatus einer Einwilligung, eines Widerrufs oder einer Verweigerung.	37
Abbildung 8-2: Option (beim Erstellen einer neuen Domäne) um ungeprüfte Dokumente zu erlauben/nicht zu erlauben. Hier werden exemplarisch auch ungeprüfte Dokumente mit dem Status gültig zugelassen.	37
Abbildung 15-1: XML-Repräsentation einer beispielhaften Anfrage von Einwilligungsinformationen über die SOAP-Schnittstelle des gICS.	49
Abbildung 15-2: XML-Repräsentation einer beispielhaften Einwilligung (in Auszügen) nach Abruf über die SOAP-Schnittstelle des gICS.	50

Abbildung 15-3: XML-Repräsentation einer beispielhaften Anfrage „Hat Patient ABC in die Policy XYZ eingewilligt?“ zur Ermittlung des Status einer Consent Policy für eine ausgewählte Signer-ID (z.B. ein Studien-Pseudonym) über die SOAP-Schnittstelle des gICS..... 51

Abbildung 15-4: XML-Repräsentation einer Antwort auf die Anfrage „Hat Patient ABC in die Policy XYZ eingewilligt?“ über die SOAP-Schnittstelle des gICS. 52

Tabellenverzeichnis

Tabelle 2-1: Mögliche Ausprägungen, welche den Status der Zustimmung (in Bezug auf eine Policy) repräsentieren.	8
Tabelle 7-1: Beispiel zur Konfiguration des Formats und der Version.	16
Tabelle 7-2: Unterstützte Domänen-Eigenschaften.....	17
Tabelle 7-3: Übersicht der verwendeten Datumsangaben.	29
Tabelle 10-1: Individualisierung von FHIR Consent.Provision.Coding durch ausgewählte External Properties.	40
Tabelle 10-2: Individualisierung von FHIR Questionnaire.Item.linkId durch ausgewählte External Properties.	40
Tabelle 10-3: Individualisierung von Antworten und Antwort-Optionen bei FHIR Questionnaire und FHIR QuestionnaireResponse durch ausgewählte External Properties.	40
Tabelle 11-1: Nutzer der Gruppe Admin und User haben unterschiedliche Zugriffsrechte in der Web-Oberfläche.	41
Tabelle 14-1: Qualitätsstatus die bei einem Upgrade gesetzt werden können.	48
Tabelle 15-1: idMatchingTypes	51

1 Hintergrund

Die Erhebung, Verarbeitung und Nutzung von medizinischen Forschungsdaten erfordert im Regelfall eine zweckbezogene informierte Einwilligung des Betroffenen, den sogenannten Informed Consent (IC) (vgl. Art. 6-11 DSGVO).

Im Kontext stetig wachsender nationaler und internationaler Forschungsinitiativen ist ein zuverlässiges und effizientes Verfahren zur digitalen Verwaltung von Einwilligungen und Widerrufen unabdingbar. Zu diesem Zweck wurde am Institut für Community Medicine das Einwilligungsmanagement generic Informed Consent Service (gICS) entwickelt. Dieser gICS ist sowohl in papierbasierte als auch rein digitale Arbeitsabläufe integrierbar und dient der Verarbeitung modular abgebildeter Einwilligungen und Widerrufen im Studienkontext. In der Praxis hat es sich bewährt, inhaltlich oder logisch zusammenhängende Prozessschritte der Datenverarbeitung (Policies) zu Modulen zusammenzufassen (z.B. Modul „Umgang mit Daten“).

Im gICS stellen Vorlagen (Templates) die digitale Umsetzung eines unausgefüllten und strukturierten Einwilligungsdokuments dar. Es besteht aus durch den Teilnehmer zustimmbaren Modulen und ergänzenden Informationen des Original-Einwilligungsdokumentes (Header, Footer, Pflichtmodulen, Festlegung von Antwortoptionen, Freitexten, etc.). Der gICS ist als Open Source Software lizenziert (AGPLv3) und kostenfrei für kommerzielle und nicht-kommerzielle Zwecke einsetzbar.

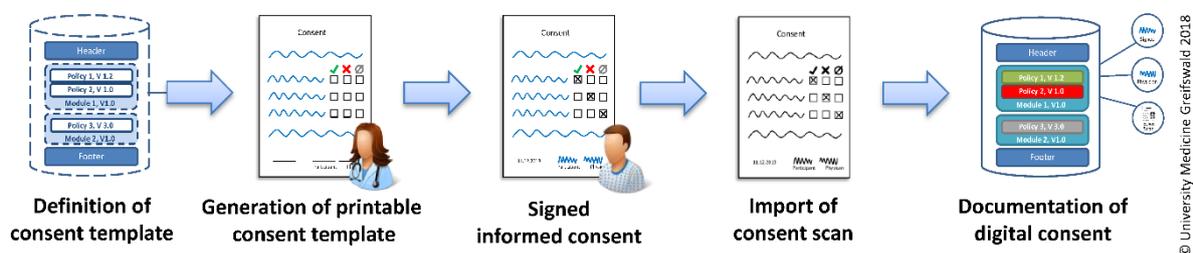


Abbildung 1-1: Ablauf der Consent Verwaltung von der Erstellung der Einwilligung über die Ausfüllung durch den Patienten bis zum Import in den gICS.

2 Der generische Informed Consent Service (gICS)

Der generische Informed Consent Service (kurz: "gICS") fokussiert Einwilligungen und Widerrufe im Studienkontext. Der bereitgestellte Webservice bildet die Anbindung zur Verarbeitung modular abgebildeter Einwilligung. Auf diese Weise hat der Patient/Proband die Möglichkeit, seine Einwilligung zu einzelnen Punkten (z.B. Datenspeicherung, Wiederkontaktierung) zu geben. Jeder dieser Punkte wird als Policy bezeichnet, zu der der Status der Zustimmung in derzeit neun möglichen Ausprägungen (vgl. **Tabelle 2-1**) erfasst wird. Da sich Inhalte einer Policy im Laufe der Zeit ändern können, sind diese versioniert. In Anlehnung an die papiergestützte Einwilligungserfassung werden eine oder mehrere Policies zu einer Vorlage zusammengefasst. Diese wird genutzt, um Einverständniserklärungen für den Probanden zu generieren. Die Unterschriften von Patient und Arzt vervollständigen das Informed Consent Dokument (vgl. **Abbildung 2-1**).

Tabelle 2-1: Mögliche Ausprägungen, welche den Status der Zustimmung (in Bezug auf eine Policy) repräsentieren.

Status-Bezeichnung	Status-Wert	Status-Wert, wenn „unknownStatels-ConsideredAsDecline=TRUE“
Akzeptiert	ACCEPTED	ACCEPTED
Abgelehnt	DECLINED	DECLINED
Unbekannt	UNKNOWN	DECLINED
Nicht gefragt	NOT_ASKED	DECLINED
Nicht gewählt	NOT_CHOSEN	DECLINED
Widerrufen	WITHDRAWN	DECLINED
Invalidiert	INVALIDATED	DECLINED
Verweigert	REFUSED	DECLINED
Ausgelaufen	EXPIRED	DECLINED

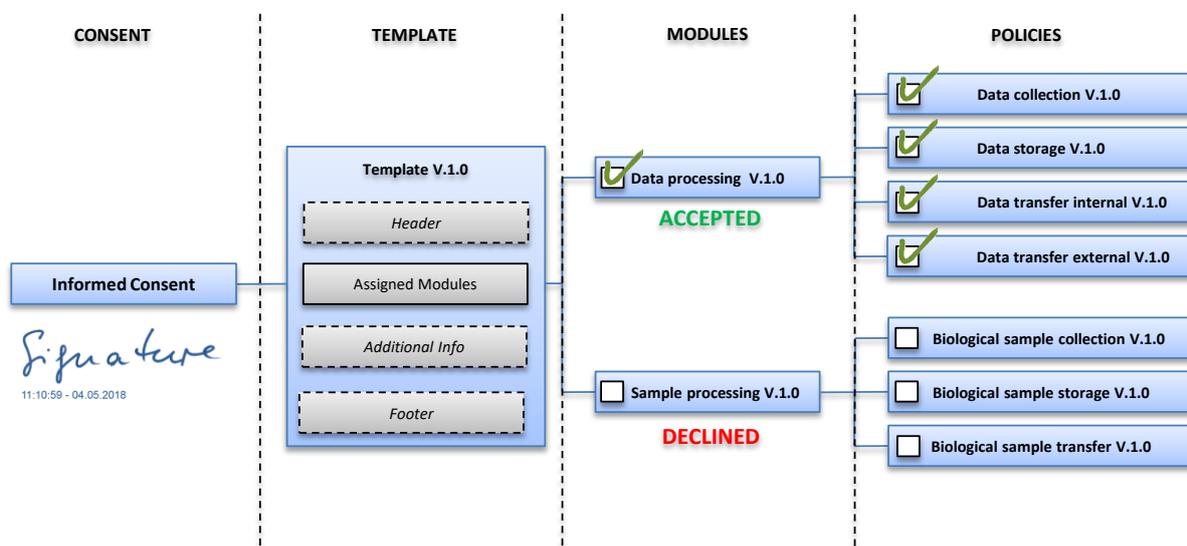


Abbildung 2-1: Die Einwilligungen und Widerrufe der Studien werden in modularer Form mittels des GICS verwaltet.

3 Begriffsbestimmungen

Domäne (Domain)

Eine Domäne ist eine organisatorische Einheit (Mandant), z.B. eine Studie, ein Projekt oder ein Institut.

Policy

Eine Policy ist eine atomare Einheit, zu der eine Einwilligung erteilt werden kann, z.B. Speichern von Bioproben. Jede Policy kann einzeln abgefragt werden.

Modul (Module)

Aus verschiedenen Gründen (z.B. thematische Nähe oder Abhängigkeit der Policies) können mehrere Policies zu einem Modul zusammengefasst werden. Das führt dazu, dass ein Proband dieser Zusammenstellung von Policies nur komplett zustimmen kann.

(Einwilligungs-)Vorlage (Template)

Eine Einwilligungsvorlage enthält einen einleitenden Text (Header), mindestens ein Modul und eine Abschlussbemerkung (Footer). Die Vorlage stellt den inhaltlichen Rahmen einer Einwilligung dar.

Teilnehmer-ID (Identifikator der betroffenen Person/Signer-ID)

Die Einwilligung enthält typischerweise keine personenbezogenen Informationen, wie Adresse oder Geburtstag der betroffenen Person (Teilnehmer, Patient, Behandlungsfall, ...). Um den Bezug zwischen Person und Einwilligung herzustellen, wird die Einwilligung mit mindestens einer eindeutigen Signer-ID versehen. Dies kann je nach Anforderungen die Fallnummer, ein Patientenidentifikator oder ein Studienpseudonym, o.ä. sein.

Einwilligung (Consent)

Eine Einwilligung ist eine ausgefüllte und unterzeichnete Einwilligungsvorlage mit Datumsangabe und Personenbezug (im Fall von glCS typischerweise eine Signer-ID, wie zum Beispiel ein Pseudonym).

Ablaufeigenschaften (Expiration Properties)

Eigenschaften in einem definierten Format zur Beschreibung der Gültigkeit (Dauer und/oder Zeitpunkt) von Policies, Modulen, Vorlagen und Einwilligungsdokumenten. Diese werden in Echtzeit durch den glCS bei der Abfrage von gültigen Einwilligungen ausgewertet.

Externe Eigenschaften (External Properties)

Diese externen Eigenschaften sind vollkommen frei nutzbar und Software-Entwicklern vorbehalten. Diese Eigenschaften können von externen Werkzeugen, wie zum Beispiel dem THS-Dispatcher ausgelesen werden und so beispielsweise für die bedingte Anzeige von Unter-Modulen,

Textformatierungen u.v.m. verwendet werden. Die Angabe erfolgt dabei im Schema *ATTRIBUT=VALUE*. Mehrere Eigenschaften werden durch Semikolons getrennt.

Informierte Einwilligung (Informed Consent)

Eine informierte Einwilligung (IC) setzt voraus, dass speziell geschultes Personal den Patienten/Studienteilnehmer umfassend über Inhalte und Auswirkungen seiner Einwilligung aufgeklärt hat. Der Patient/Studienteilnehmer hatte zudem die Möglichkeit Fragen zu stellen und wurde über die Möglichkeiten des Widerrufs der Einwilligung informiert.

Verweigerung/Ablehnung (Refusal)

Eine Verweigerung ist die Aussage eines Teilnehmers, an einer Studie/Register nicht teilnehmen zu wollen. Der Status entspricht einer Person, die nie gefragt wurde. Lag zuvor bereits eine Einwilligung vor, muss ein Widerruf ausgefüllt werden.

Widerruf (Withdrawal)

Der Widerruf ist die Rücknahme einer zuvor gegebenen Einwilligung. Im Gegensatz zur Verweigerung hat der Teilnehmer also bereits an der Studie/Register teilgenommen.

4 Symbolverzeichnis

Viele Informationen werden in der gICS-Oberfläche mit Symbolen geliefert. Dabei werden diese entweder auf der jeweiligen Seite in Form einer Legende erklärt. Andernfalls wird die Bedeutung zumindest dann angezeigt, wenn der Maus-Cursor über das jeweilige Symbol gefahren wird. Für einen Überblick sind hier einige Symbole erläutert.



Das Dokument ist gültig.



Das Dokument ist ganz abgelaufen.



Das Dokument ist teilweise abgelaufen.



Das Dokument hat kein Ablaufdatum (läuft nicht automatisch ab).



Das Dokument besitzt einen Scan (Herunterladen mit einem Klick).



Das Dokument besitzt keinen Scan.



Das Dokument wurde auf Papier unterschrieben.



Das Dokument wurde digital unterschrieben.

5 Funktionalitäten

5.1 Was leistet der Dienst (Auszug)

- Erstellung und Verwaltung von Policies und Vorlagen
- Erfassung modular aufgebauter Einwilligungen
- Abbildung von Widerrufen
- Unterstützung von Versionierung
- automatisierbare Abfrage des Einwilligungsstatus frei konfigurierbar
- Festlegung von Pflichtpolicies
- Optionale Freitextfelder
- Suche nach individuellen, konsentierten Kennungen, wie zum Beispiel Fallnummern
- Integration papierbasierter Verfahren

5.2 Was leistet der Dienst nicht

- Definition von Abläufen im Umgang mit Einwilligungen und Widerrufen
- Entwurf der benötigten Inhalte der Konsentierungsdokumente, dies muss innerhalb der jeweiligen Studie selbst erfolgen (Der TMF Consent Wizard kann an dieser Stelle jedoch behilflich sein.)
- Ethische Prüfung der Konsentierungsdokumente, dies muss durch eine entsprechende Ethik-Kommission im Rahmen der Studie erfolgen

6 Installation

6.1 Systemanforderungen

Technisch

- Windows oder Ubuntu Server (oder vergleichbar)
- Mindestens 8 GB Arbeitsspeicher
- Mindestens 5 GB Festplattenspeicher (100.000 Datensätze inklusive Dokumentenscan (300 dpi, 3 seitig) entsprechen rund 5 GB)

- Installierte aktuelle Version von *Docker* und *Docker Compose*
- Administrative Rechte
- Keine Nutzungsbeschränkungen auf die bereitgestellten Service- und Client-URLs
- Personell
- Verantwortlicher mit grundlegenden IT-Kenntnissen zur Administration des Servers und zur Einrichtung des gICS-Dienstes (zuzüglich der Wartung und regelmäßiger Sicherungen der gICS-Datenbank)
- Verantwortlicher zur Administration und Pflege der gICS-Inhalte

⚠ Hinweis: Bei einem Upgrade von einer bestehenden Instanz zu einer neuen Version sind ggf. die Hinweise im **Kapitel 8** zu beachten.

6.2 Download und Starten des Dienstes

Um den gICS als Docker-Container zu starten, werden die Programme *Docker* und *Docker Compose* benötigt. Beide Programme müssen hierfür installiert sein. Da zwischen beiden Programmen Inkompatibilitäten auftreten können, wird empfohlen die jeweils aktuellsten Versionen zu installieren.

Der gICS benötigt zur Ausführung mehrere Container (vgl. **Abbildung 6-1**). Damit diese nicht einzeln gestartet werden müssen und entsprechend zusammengeschaltet werden müssen, wird der Dienst mit Docker-Compose gestartet. Alle hierzu benötigten Ressourcen werden im öffentlichen Repository des MOSAIC-Projekts bereitgestellt¹.

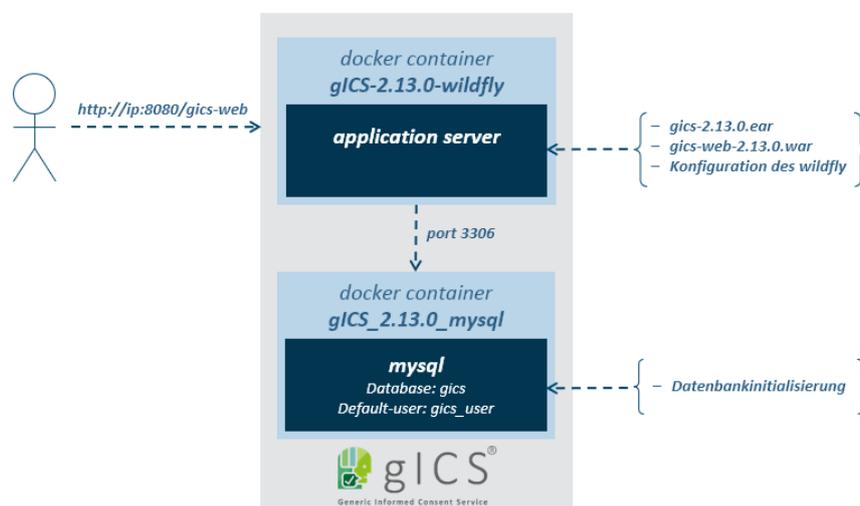


Abbildung 6-1: Aktuelle Architektur des gICS Docker Containers am Beispiel der Version 2.13.0.

Das entstehende Docker-System besteht aus getrennten Containern für die erforderliche Datenbankinstanz (MySQL) und den benötigten Anwendungsserver (Wildfly inkl. Datenbank-Konnektoren) zur Verfügbarmachung der Programmdateien. Beide Container kommunizieren intern

¹ Weitere Informationen unter <https://www.ths-greifswald.de/forscher/gics/#download>

über den MySQL-Port 3306. Der Zugriff auf das System von „außen“ erfolgt über den Web-Browser. Die Inhalte werden über den Port 8080 (gICS) für den Anwender bereitgestellt.

Die Konfiguration erfolgt mittels Docker Compose. Der Installationsvorgang nimmt rund 3 Minuten in Anspruch und erfordern rund 1.4 GByte an Speicherplatz.

Um die folgenden Schritte problemlos durchführen zu können, wird ein Account mit administrativen Rechten benötigt. Exemplarisch werden die folgenden Befehle mit **sudo** ausgeführt.

Download der benötigten Dateien

Laden Sie die aktuellste Version von <https://www.ths-greifswald.de/forscher/e-pix/#download> herunter und entpacken Sie die ZIP-Datei. Diese enthält alle relevanten Docker-Compose-Dateien.

Vergabe Schreibrechten

```
sudo chmod -R 755 [name des gICS-Ordners]/compose-wildfly/  
chown -R 1000:1000 [name des gICS-Ordners]/compose-wildfly/logs/ [name des  
gICS-Ordners]/compose-wildfly/deployments/
```

Wechseln in das gICS-Verzeichnis für die Standard-Version

```
cd [name des gICS-Ordners]/compose-wildfly/
```

Sollte der MySQL-Dienst auf der Maschine ausgeführt werden, dann stoppen des Dienstes

```
sudo service mysql stop
```

Prüfen der Docker-Version (vorausgesetzt ist Version 1.13.1 oder höher)

```
sudo docker -v
```

Prüfen der Docker Compose-Version (vorausgesetzt ist Version 1.8.0 oder höher)

```
sudo docker-compose -v
```

Starten des gICS mithilfe von Docker Compose

```
sudo docker-compose up
```

Damit werden die benötigten Komponenten heruntergeladen und die Konfiguration von MySQL und Wildfly gestartet. Danach wird die aktuelle Version des gICS bereitgestellt. Der Installationsvorgang kann in Abhängigkeit der vorhandenen Internetverbindung etwa 7 Minuten dauern. Der erfolgreiche Start des Dienstes wird mit der folgenden Ausgabe abgeschlossen.

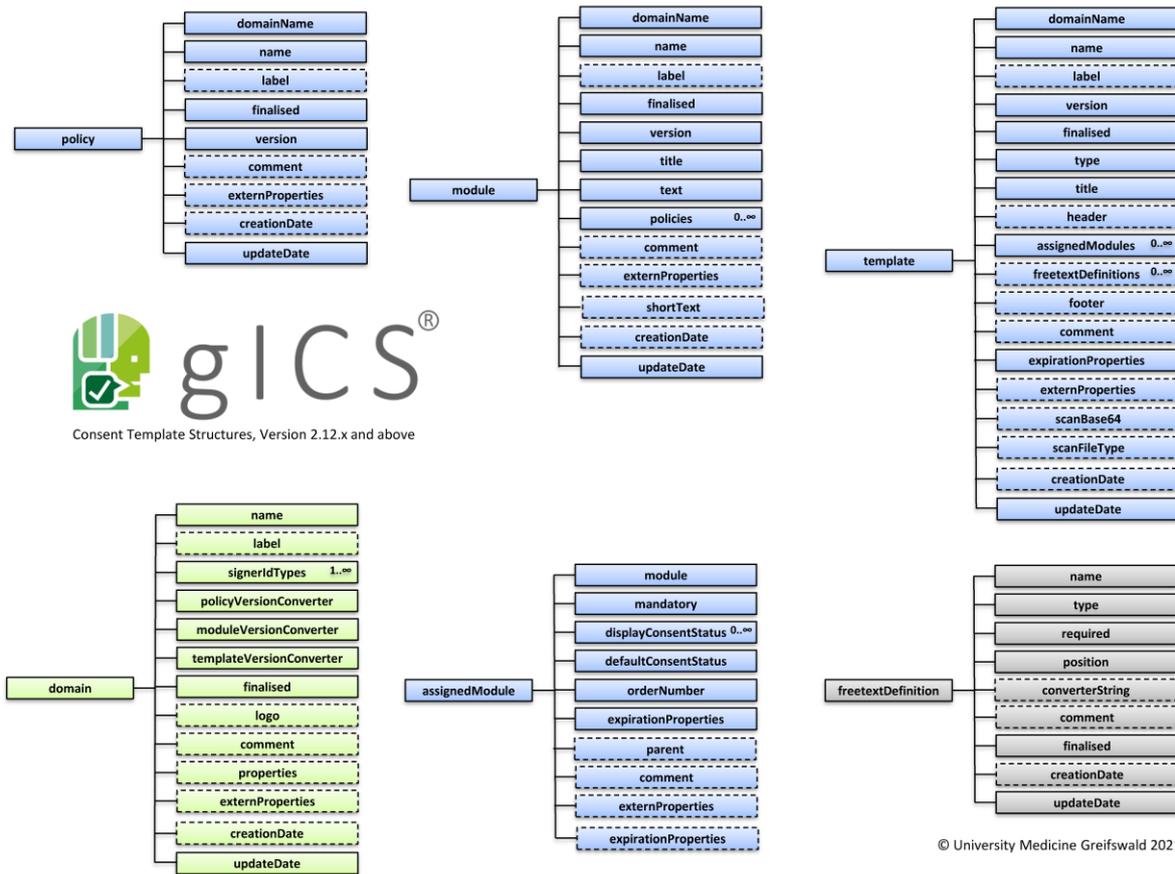
```
Wildfly 18.0.0.Final (Wildfly Core 5.0.0.Final) started in 63373ms -  
Started 824 of 1024 services (324 services are lazy, passive or on-demand)
```

7 Die grafische Oberfläche des gICS

Um dem Datentreuhänder die Verwaltung von Einwilligungen und Widerrufern zu ermöglichen, verfügt der gICS über eine grafische Benutzeroberfläche die speziell für den Einsatz im Web-Browser entwickelt wurde.

Der Aufbau der Oberfläche orientiert sich an typischen Arbeitsabläufen eines Datentreuhänders. Die daraus resultierenden Anwendungsfälle umfassen die

1. Anlegen von Domänen
2. Erstellung einer Vorlage für Einwilligungen
3. Erstellung einer Vorlage für Widerrufe bzw. Verweigerungen
4. Erfassung von Einwilligungen, Widerrufen und Verweigerungen
5. Abfragen von Einwilligungsdetails
6. Bearbeiten, Duplizieren und Finalisieren
7. Gültigkeit von Einwilligungen und Modulen automatisch ablaufen lassen
8. Dokumenten-Suche (Ermittlung des zeitlichen Verlaufs)
9. Durchführung von Analysen
10. Export und Import von Domänenkonfigurationen und Vorlagen
11. Vorlagendruck und -erkennung



© University Medicine Greifswald 2021

Abbildung 7-1: Überblick der Attribute, welche bei den jeweiligen Bausteinen gesetzt werden können. Attribute mit gestrichelten Rand sind optional, alle anderen sind Pflichtattribute und müssen (zumindest leer) gesetzt werden.

Als Teil der Erstellung der ersten Einwilligungsvorlage (siehe Anwendungsfall 1) wird eine Domäne, zumindest eine Policy und mindestens ein Modul angelegt. Die entsprechenden Bausteine können jeweils unterschiedliche Attribute gesetzt werden. Eine Auflistung der jeweiligen Attribute ist in Abbildung 2-1 zu finden.

7.1 Anlegen von Domänen

Innerhalb einer Domäne werden die Einwilligungen und Widerrufe zum Beispiel zu einem Projekt oder Studie verwaltet. Das Anlegen von domänenspezifischen Vorlagen, Modulen und Policies für Einwilligungen, Widerrufe und Verweigerungen wird im **Abschnitt 7.2** gezeigt.

Unter dem Menüpunkt *Domänen* werden alle bereits angelegten Domänen aufgelistet. Um eine neue Domäne zu erstellen, muss die Schaltfläche *Erstellen* angewählt werden. Daraufhin öffnet sich ein Fenster mit den auszufüllenden Feldern. In **Abbildung 7-2** wird die entsprechende Oberfläche dargestellt. Wenn mit dem Cursor über das „?“-Symbol gefahren wird, werden weitere Hilfestellungen gegeben zu den entsprechenden Optionen geliefert.

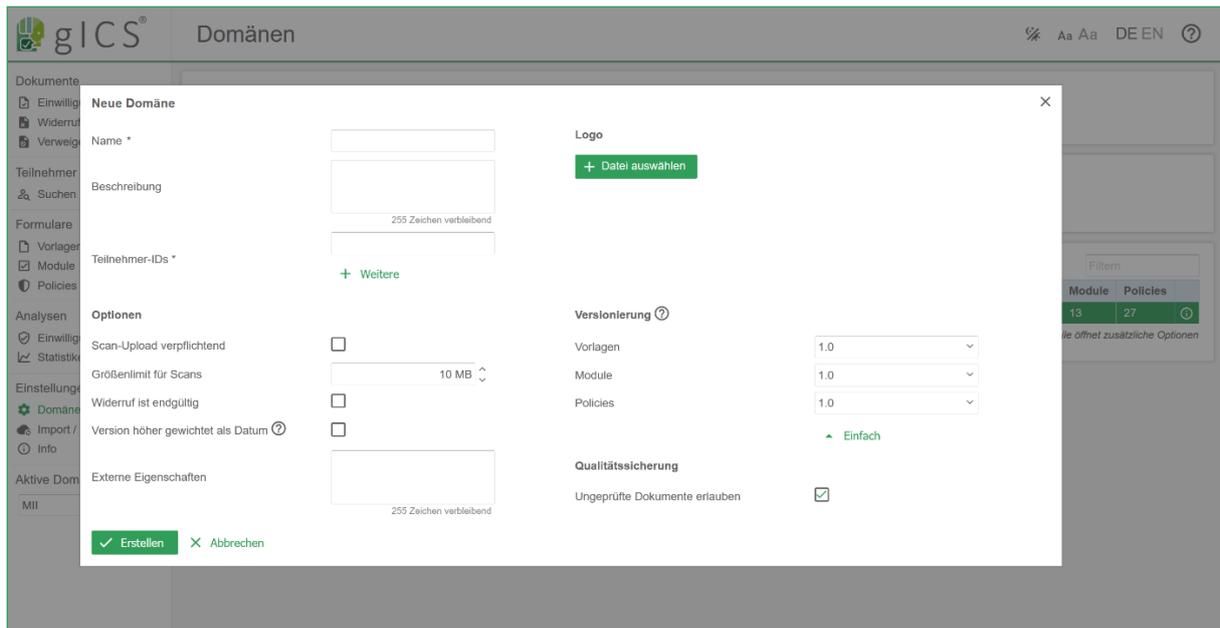


Abbildung 7-2: Oberfläche zum Anlegen einer neuen Domäne.

Beim Anlegen einer neuen Domäne muss ein eindeutiger Name festgelegt werden. Des Weiteren können eine kurze Beschreibung und ein Logo der Domäne hinzugefügt werden. Das Logo wird auf allen Einwilligungen und Widerrufen der Domäne in der Kopfzeile dargestellt.

Es ist möglich individuelle Kennungen auf dem jeweiligen Informed Consent zu vermerken, wie zum Beispiel Fallnummern. Diese werden in Form von Teilnehmer-IDs (Signer-ID Typen) je Domäne festgelegt und können direkt im Anschluss bei der Erstellung des Informed Consent als ergänzende Information zum Patienten angegeben werden. Damit können später beispielsweise einem Patienten Fälle zugewiesen werden. Es können mehrere Teilnehmer-IDs dem Patienten zugewiesen werden.

Vorlagen, Module und Policies werden versioniert. Das jeweilige Format wird in der Domäne festgelegt und gilt dann jeweils für die darin enthaltenen Vorlagen, Module und Policies. In **Tabelle 7-1** sind die möglichen Formate dargestellt.

Tabelle 7-1: Beispiel zur Konfiguration des Formats und der Version.

Versionierungs-Ebene	Format	Beispiel
1	major	Version 1, Version 2, ...
2	major.minor	Version 1.0, Version 1.1, Version 2.0, ...
3	major.minor.maintenance	Version 1.0.1, Version 2.1.0, Version 2.1.c, ... (lässt in der letzten Ebene Zahlen und Buchstaben zu)

Jeder Domäne können weitere Eigenschaften hinzugefügt werden, welche für eine projektspezifische Konfiguration der Domäne verwendet werden können. Die derzeit unterstützten Eigenschaften mit der jeweiligen Beschreibung sind in **Tabelle 7-2** dargestellt.

Tabelle 7-2: Unterstützte Domänen-Eigenschaften

Option	Bedeutung
Version höher gewichtet als Datum	Bei der Abfrage einer Einwilligung wird standardmäßig der Status der Policy mit dem jüngsten Datum verwendet. Wird diese Option gewählt, wird stattdessen immer nur der Status der Policy mit der neusten Version verwendet.
Widerruf ist endgültig	Standardmäßig kann ein Widerruf mit einer erneuten Einwilligung aufgehoben werden. Ist diese Option gewählt, so kann ein Widerruf auch bei erneuter Einwilligung nicht wieder aufgehoben werden.
Scan-Upload verpflichtend	Ist diese Option gewählt, so kann eine Einwilligung, Widerruf oder Verweigerung nur angelegt werden, wenn ein Scan der jeweiligen Einwilligung/Widerruf direkt mit hochgeladen wird.
Größenlimit für Scans	Mit dieser Option kann die Größe von Scans limitiert werden. Standardmäßig darf pro Scan eine 10 MB große Datei beigefügt werden.

Mit einem Klick auf *Erstellen* wird die Domäne angelegt und ist in der Auflistung der verfügbaren Domänen enthalten. Mit einem Rechtsklick auf eine Domäne kann ein Kontextmenü für weitere Optionen geöffnet werden. Die Oberfläche mit der Auflistung aller verfügbaren Domänen und dem geöffneten Kontextmenü ist in **Abbildung 7-3** dargestellt.

The screenshot shows the 'gICS' interface for managing domains. The main content area displays a table with the following data:

Name	Beschreibung	Einwilligungen	Widerrufe	Verweigerungen	Vorlagen	Module	Policies
MI (aktiv)	Medizininformatik Initiative	-	-	-	1	13	27

The context menu for the selected domain includes the following options:

- Details der Domäne
- Aktivieren
- Bearbeiten (eingeschränkt)
- Löschen

Abbildung 7-3: Auflistung aller erstellten Domänen. Eine Domäne wurde ausgewählt und das entsprechende Kontextmenü wird dargestellt.

Im Kontextmenü kann über den Menüpunkt *Details der Domäne* die eingestellten Einstellungen eingesehen werden. Über den Menüpunkt *Aktivieren* kann die angewählte Domäne aktiviert werden. Alternativ kann hierzu auch das Auswahlmeneü im linken Menü verwendet werden. Mit dem Menüpunkt *Bearbeiten* können die Einstellungen einer Domäne verändert werden. Dabei ist zu beachten, dass sobald in der Domäne Einwilligungen und Widerrufe erfasst wurden, nicht mehr alle Optionen bearbeitet werden können. Mit dem letzten Menüpunkt *Löschen*, kann die Domäne

entfernt werden. Dies ist jedoch nur möglich, wenn keine Einwilligungen und Widerrufe in der entsprechenden Domäne enthalten sind.

⚠ Hinweis: Sind innerhalb einer Einwilligungsdomäne mehr als ein SignerIdType konfiguriert (z.B. Pseudonym, Fallnummern, PatientenID), wird in **FHIR Consent** Exporten per Default der erste SignerIdType als Personenidentifikator im FHIR Consent verwendet.

Dies kann im Bedarfsfall angepasst werden durch Definition eines **External Property** **SAFE_SIGNERID_TYPE** für die jeweilige Domain (z.B. „SAFE_SIGNERID_TYPE = Pseudonym“).

7.2 Erstellung einer Vorlage für Einwilligungen

Um eine neue Vorlage zu erstellen, müssen eine Domäne und mindestens ein Modul mit einer Policy vorhanden sein. Wie in **Abbildung 7-1** gezeigt, wird zumindest eine Policy einem Modul beigelegt, welches zusätzlich mit Titel und Texten versehen werden kann. Mehrere Module werden einer Vorlage zugeordnet und können später in der Einwilligung, dem Widerruf oder der Verweigerung ausgefüllt werden.

Anlegen von Policies

Um Policies anlegen zu können, muss zunächst die zugehörige Domäne ausgewählt werden. Dies geschieht über das untere Auswahlmü mit der Überschrift „Aktive Domäne“ im linken Seitenmenü.

Beim Hinzufügen einer Policy muss ein sprechender, eindeutiger Name festgelegt und manuell eine Versionsnummer vergeben werden, entsprechend dem für die Domäne festgelegten Versionsformat (siehe **Tabelle 7-1**). Die Beschreibung darf 255 Zeichen enthalten und ist optional. Zusätzlich können *Externe Eigenschaften* definiert werden. Diese sind frei nutzbar und können beispielsweise von externen Werkzeugen ausgewertet werden.

Die Oberfläche zum Anlegen einer Policy ist in **Abbildung 7-4** dargestellt.

The screenshot shows the 'Neue Policy' form in the gICS system. The form is titled 'Neue Policy' and contains the following fields:

- Name ***: MDAT_nutzen (89 Zeichen verbleibend)
- Version ***: 1.0
- Beschreibung**: (255 Zeichen verbleibend)
- Externe Eigenschaften**: (255 Zeichen verbleibend)

At the bottom of the form, there are two buttons: 'Hinzufügen' (with a green checkmark) and 'Abbrechen' (with a red X). The footer of the form indicates 'Treuhandstelle der Universitätsmedizin Greifswald - gICS 2.12.0'.

The left sidebar contains the following navigation options:

- Dokumente**: Einwilligungen, Widerrufe, Verweigerungen
- Teilnehmer**: Suchen
- Formulare**: Vorlagen, Module, Policies
- Analysen**: Einwilligungsstatus, Statistiken
- Einstellungen**: Domänen, Import / Export, Info
- Aktive Domäne**: MII

Abbildung 7-4: Oberfläche zum Anlegen einer neuen Policy.

Anlegen von Modulen

Um Module anlegen zu können, muss wieder zunächst die gewünschte Domäne ausgewählt werden. Anschließend sind ein eindeutiger Name und eine Versionsnummer festzulegen. Zusätzlich können ein Titel und ein Modultext vergeben werden. Die Versionsnummer orientiert sich dabei an dem ausgewählten Versionsformat, dass in der Domäne gesetzt wurde (vgl. **Tabelle 7-1**). Der Modultext kann dabei mithilfe des WYSIWYG²-Textfeldes formatiert werden.

Jedem Modul ist eine Auswahl von Policies in beliebiger Reihenfolge zuzuordnen. Ein Modul kann dabei nur die Policy in einer Version beinhalten. Es ist demnach nicht erlaubt, beispielsweise die Policy „Re-Kontaktierung“ in den Versionen 1.0 und 1.1 demselben Modul zuzuordnen.

⚠ Hinweis: Die Reihenfolge der Policies kann nur beim Anlegen des Moduls bestimmt werden. Bei einer nachträglichen Änderung ist dies nicht mehr möglich.

Die folgenden Angaben sind optional und sind unter dem Punkt *Sonstiges* gruppiert. Darunter enthalten ist ein Kommentar, welcher gesetzt werden kann. Außerdem erlauben Module die Vergabe von *Externen Eigenschaften*. Diese sind vollkommen frei nutzbar und können beispielsweise für die bedingte Anzeige von Unter-Modulen, Textformatierungen u.v.m. verwendet werden. Für Module steht die Eigenschaft `CONTAINS_HTML=TRUE` zur Verfügung. Damit kann einem externen Werkzeug mitgeteilt werden, dass durch die Formatierung von Modultitel und -text eine Ausgabe in HTML erfolgen muss, damit diese korrekt dargestellt werden. Hierzu muss das entsprechende Werkzeug diese Eigenschaften auswerten.

Die Oberfläche zum Anlegen eines Moduls ist in **Abbildung 7-5** dargestellt.

² What You See Is What You Get (Was du siehst, ist das was du bekommst)

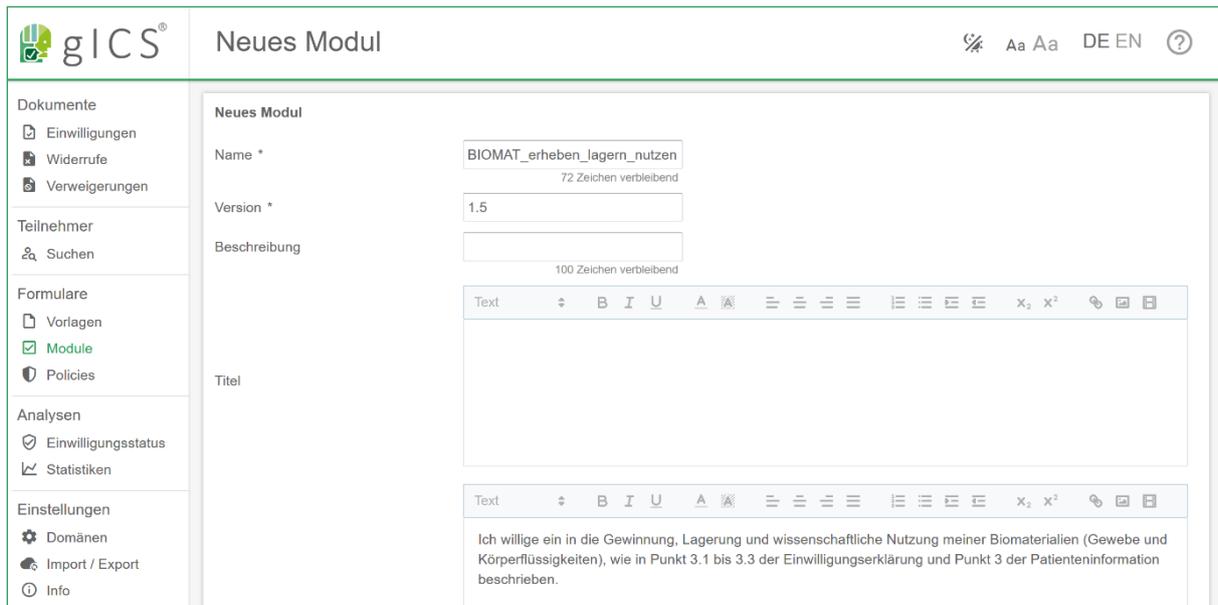


Abbildung 7-5: Oberfläche zum Anlegen eines neuen Moduls.

Solange ein Modul nicht finalisiert wurde, kann dieses ohne Veränderung der Version bearbeitet werden. Ein Modul wird automatisch finalisiert, wenn eine Vorlage mit diesem Modul finalisiert wird. Ein manuelles finalisieren erfolgt über die Modul-Übersicht, indem beim entsprechenden Eintrag die Aktion *Entwurf finalisieren* angewählt wird.

Anlegen von Vorlagen

Die Vorlage stellt die Arbeitsgrundlage für die zukünftig erfassten Einwilligungen und Widerrufe dar. Zunächst wird die gewünschte Domäne ausgewählt. Beim Anlegen einer Vorlage kann zwischen den drei Typen *Einwilligung*, *Widerruf* und *Verweigerung* unterschieden. Je nach Vorlage muss der gewünschte Typ ausgewählt werden. Danach müssen ein eindeutiger Name der Vorlage und eine Versionsnummer (siehe **Tabelle 7-1**) angegeben werden. Der Titel, eine einleitende Kopfzeile, sowie eine abschließende Fußzeile können bei Wunsch definiert und formatiert werden.

Die Auswahl und Reihenfolge der benötigten Module können beliebig aus dem Pool der in dieser Domäne verfügbaren Module definiert werden. Es können Pflicht-Module, Vorauswahl der Antworten und die anzuzeigenden Antwortmöglichkeiten festgelegt werden. Die möglichen Antwortmöglichkeiten sind in **Tabelle 2-1** dargestellt. Die Auswahl als Pflichtmodul begrenzt den Umfang der möglichen Antworten auf *Akzeptiert*, *Abgelehnt*, *Widerrufen* und *Invalidiert*. Ein Pflichtmodul legt fest, dass beim Erfassen der Einwilligung dieses Modul stets akzeptiert werden muss.

Um weitere Daten bei der Erfassung einer Einwilligung zu erfassen, können *Benutzerdefinierte Felder* ergänzt werden. Diese besitzen einen Namen, welcher auf der Einwilligung dargestellt wird. Ein Feld kann als Pflichtfeld definiert werden und je nach erfassten Daten muss der entsprechende Datentyp angegeben werden (Text, Datum, Zahl, Zahl (Fließkomma) oder Kontrollkästchen). Im Fall eines

Datums muss zudem das Datumsformat angegeben werden (siehe Liste gängiger Datumsformate³). Damit kann beispielsweise mithilfe eines *Benutzerdefinierten Feldes* des Typs Text, eine Adresse abgefragt werden.

Unter dem Punkt *Sonstiges* können weitere optionale Eigenschaften definiert werden. Neben einem Kommentar kann der automatische Ablauf für die entsprechenden Einwilligungen und *Extern Properties* definiert werden. Bei Letzterem wird die Eigenschaft semikolon-separiert im Schema *ATTRIBUT=VALUE* definiert. Die Einrichtung eines Ablaufdatums wird im **Abschnitt 7.7** erläutert. Für die *Extern Properties* steht die Eigenschaft `containsHTML=true` zur Verfügung. Damit kann einem externen Werkzeug mitgeteilt werden, dass durch die Formatierung von Titel, Kopf- und Fußzeile eine Ausgabe in HTML erfolgen muss, damit diese korrekt dargestellt werden.

Die Oberfläche zum Anlegen einer Vorlage ist in **Abbildung 7-6** dargestellt.

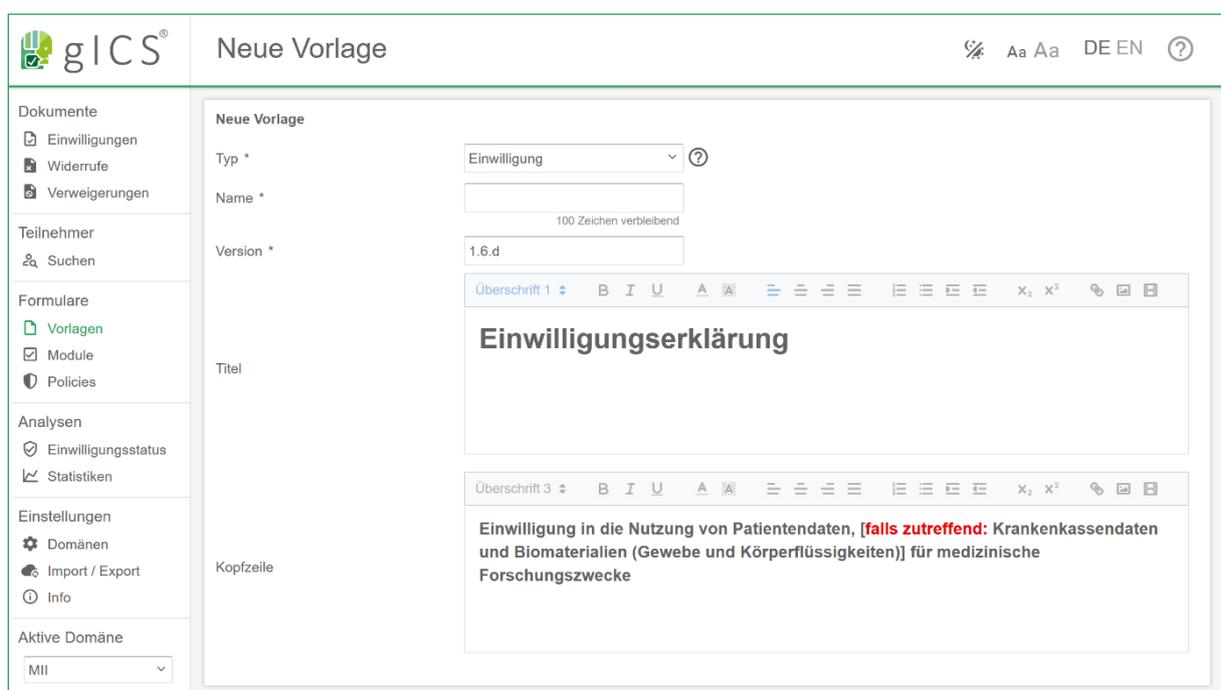


Abbildung 7-6: Oberfläche zum Erstellen einer neuen Vorlage.

Bevor Einwilligungen mittels der erzeugten Vorlage erfasst werden, sollte die Vorlage finalisiert werden. Solange eine Vorlage nicht finalisiert ist, gilt diese als Entwurf und kann beliebig verändert werden ohne eine Versionsänderung vorzunehmen. Eine Vorlage wird finalisiert, indem in der Vorlagenübersicht die Aktion *Entwurf Finalisieren* ausgeführt wird. Dies hat zur Folge, dass alle in dieser Vorlage verwendeten Module ebenfalls finalisiert werden. Solange eine Vorlage nicht finalisiert wurde, wird beim Ausdruck der Vorlage ein Wasserzeichen mit dem Text „nicht final“ auf der Seite angezeigt.

Wenn eine Vorlage auf Grundlage einer bereits existenten Vorlage angelegt werden soll, so kann die bereits vorhandene Vorlage dupliziert werden. Dies wird in **Abschnitt 7.6.2** erläutert.

³ Weitere Informationen unter <https://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html>

7.3 Erstellung einer Vorlage für Widerrufe bzw. Verweigerungen

⚠ Hinweis: Für die Abbildung von Einwilligungen, Widerrufen und Verweigerungen sollten zwingend unterschiedliche Vorlagen genutzt werden. Den Patienten können auf diese Weise unterschiedliche Botschaften mitgegeben werden und die Folgen seines Handelns besser deutlich gemacht werden. Die innerhalb der Widerrufe und Verweigerungen zugeordneten Policies sollten indes die gleichen sein, die bereits in der Einwilligungsvorlage genutzt wurden.

Beim Anlegen von Vorlagen für Widerrufe oder Verweigerungen wird grundsätzlich so vorgegangen wie beim Anlegen von Einwilligungsvorlage (vgl. **Abschnitt 7.2**). Abweichend davon wird beim Anlegen der Vorlage der Typ Widerruf (bzw. Verweigerung) gewählt.

Bei einem Widerruf sollten dieselben Policies verwendet werden, wie bei der dazugehörigen Einwilligung. Hierzu kann ein entsprechendes Modul mit den jeweiligen Policies zusammengestellt werden (vgl. **Abschnitt 7.2**). Für das entsprechende Modul mit den jeweiligen Policies wird die Antwortmöglichkeit WIHTDRAWN (vgl. Tabelle 2-1) gesetzt.

7.4 Erfassung von Einwilligungen, Widerrufen und Verweigerungen

Einwilligungen, Widerrufe und Verweigerungen werden grundsätzlich auf die gleiche Art erfasst. Die Art des Dokuments ergibt sich aus dem in der Vorlage definierten Dokumententyps. Exemplarisch wird nachfolgend nur die Erfassung einer Einwilligung (Consent) dargestellt.

Es gibt zwei mögliche Vorgehensweisen zur Erfassung einer Einwilligung. Zum einen kann über die Oberfläche eine Einwilligung ausgefüllt werden und im Nachgang ein entsprechender Scan der papierbasierten Einwilligung angefügt werden. Zum anderen kann ein Scan hochgeladen werden und die darin gewählten Antwortmöglichkeiten in die digitale Einwilligung übertragen werden. Hierbei ermöglicht der gICS auch die automatische Erfassung der gesetzten Kreuze, sodass diese nicht manuell in die digitale Einwilligung eingetragen werden müssen. Es findet lediglich eine manuelle Prüfung statt. Bei einer papierbasierten Erfassung wird die jeweilige Vorlage ausgedruckt (s. **Abschnitt 7.11**) und analog ausgefüllt. Der Ausdruck muss anschließend eingescannt und als Scan bei der digitalen Erfassung hochgeladen werden. Zum Ausdrucken wird die Vorlagenübersicht aufgerufen und die jeweilige Vorlage ausgewählt und über das Kontextmenü der Eintrag *Drucken* gewählt.

Für die erste Variante muss zur Erfassung einer Einwilligung zunächst, je nach Typ, das zu erfassende Dokument (Einwilligungen, Widerrufe, Verweigerungen), der Button *Ausfüllen* und die entsprechende Vorlage ausgewählt werden. Im Anschluss wird die Einwilligung des Patienten zu den einzelnen Modulen festgehalten und es sind die ggf. vorhandenen Freitextfelder auszufüllen. Zusätzlich sind die spezifischen IDs/Pseudonyme des Patienten und des unterzeichnenden Arztes als auch das entsprechende Datum zu erfassen. Wurden für diese Domäne sogenannte Signer-ID Typen definiert, wie zum Beispiel Fallnummern, sind diese beim Patienten mit anzugeben. Das Anhängen der gescannten Unterschrift von Arzt und Patient ist aus datenschutzrechtlichen Gründen erforderlich. Ob für das Erfassen einer Einwilligung ein entsprechender Scan obligatorisch

hochgeladen werden muss, kann in der Domänenkonfiguration (siehe **Abschnitt 7.1**) mithilfe der Eigenschaft `SCANS_ARE_NOT_MANDATORY_FOR_ACCEPTED_CONSENTS` bzw. Scan-Upload verpflichtend definiert werden.

Optional kann ein Scan der (papierbasierten) Einwilligung dem digitalen Informed Consent angehängen werden. Dies ist auch im Nachhinein problemlos möglich.

Die Oberfläche zur Erfassung einer Einwilligung ist in **Abbildung 7-7** dargestellt.

The screenshot shows the gICS 'Einwilligungen' (Consents) interface. The main content area displays a consent form for 'miracum Medical Informatics in Research and Care in University Medicine'. The form is titled 'Einwilligungserklärung' (Version 1.6.d) and is for the 'MII' domain. The form content includes:

Einwilligung in die Nutzung von Patientendaten, [falls zutreffend: Krankenkassendaten und Biomaterialien (Gewebe und Körperflüssigkeiten)] für medizinische Forschungszwecke

1. Erhebung, Verarbeitung und wissenschaftliche Nutzung meiner Patientendaten, wie in der Patienteninformation beschrieben; dies umfasst

1.1 die Verarbeitung und Nutzung meiner Patientendaten für die medizinische Forschung ausschließlich wie in der Patienteninformation beschrieben und mit getrennter Verwaltung des Namens und anderer direkt identifizierender Daten (Codierung). Unter der Adresse <http://www.medizinformatik-initiative.de/datenutzung> kann ich mich für einen E-Mail-Verteiler registrieren, der per E-Mail über alle neuen Studien, die mit den Patientendaten durchgeführt werden, vor deren Durchführung informiert (siehe Punkte 1.1, 1.2 und 1.3 der Patienteninformation).

1.2 die wissenschaftliche Analyse und Nutzung meiner codierten Patientendaten durch Dritte wie z.B. durch andere Universitäten/Institute/forschende Unternehmen; dies kann auch eine Weitergabe für Forschungsprojekte im Ausland umfassen, wenn in diesem europäischen Datenschutzrecht gilt oder die Europäische Kommission ein angemessenes Datenschutzniveau bestätigt hat. An einem etwaigen kommerziellen Nutzen aus der Forschung werde ich nicht beteiligt. Vor einer Weitergabe an Forscher außerhalb meiner behandelnden Einrichtung erfolgt zudem eine weitere Ersetzung des internen Kennzeichens durch eine neue Zeichenkombination.

1.3 die Möglichkeit einer Zusammenführung meiner Patientendaten mit Daten in Datenbanken anderer Forschungspartner. Voraussetzung ist, dass ich dieser Nutzung bei den entsprechenden Forschungspartnern auch zugestimmt habe.

Ich willige ein in die Erhebung, Verarbeitung, Speicherung und wissenschaftliche Nutzung meiner Patientendaten wie in Punkt 1.1 bis 1.3 der Einwilligungserklärung und Punkt 1 der Patienteninformation beschrieben.

Ja Nein

Abbildung 7-7: Oberfläche zur Erfassung einer neuen Einwilligung.

Bei der zweiten Variante muss zunächst die entsprechende Vorlage ausgedruckt und durch den Patienten ausgefüllt werden. Zum Drucken wird unter dem Menüpunkt *Vorlagen* die zu druckende Vorlage ausgewählt und über die dazugehörige Aktion gedruckt. Dabei kann gewählt werden, ob eine leere Vorlage gedruckt werden soll oder bereits die Signer-ID ausgefüllt sein soll. Dabei können auch Vorlagen für mehrere Patienten gedruckt werden. Zudem besteht die Möglichkeit die entsprechenden Signer-IDs (auch mehrere bei mehreren Patienten) anzugeben und die entsprechenden Einwilligungen zu erzeugen. Jede Vorlage besitzt dabei einen sogenannten QR-Code, in dem die Informationen zur Vorlage kodiert sind. Zum Einlesen der ausgefüllten Einwilligung, muss diese eingescannt werden. Danach wird im gICS, wie in der Variante zuvor, das entsprechende Dokument gewählt und der Button *Hochladen und einlesen* angeklickt. Das eingescannte Dokument wird danach ausgewählt und kann nun hochgeladen werden. Der gICS sucht dabei automatisiert den abgebildeten QR-Code und generiert die entsprechende digitale Einwilligung. Gesetzte Kreuze werden dabei automatisch erkannt und entsprechend hinterlegt. Ggf. nicht erkannte Einwilligungen, die Signer-IDs und Datumsangaben können danach manuell übertragen werden. Je nach Konfiguration (vgl. **Abschnitt 7.1**, Parameter "REVOKE_IS_PERMANENT") kann ein einmaliger Widerruf zur Folge haben, dass ein Patient keine erneute Einwilligung geben kann. Ein Widerruf eines Widerrufs wäre in diesem Fall nicht möglich.

Alle erfassten Einwilligungen sind unter dem Menüpunkt Einwilligungen aufgelistet (analog dazu: Widerrufe und Verweigerungen). Zusätzliche Optionen zu jeder Einwilligung können im Kontextmenü eingesehen bzw. aufgerufen werden. Dies ermöglicht unter anderem das Kopieren oder Hinzufügen einer Teilnehmer-ID, das Herunterladen, Anhängen oder Drucken von Scans, dem Setzen des Qualitätsstatus (Details siehe **Kapitel 8**), eines Kommentars oder der Externen Eigenschaften. In **Abbildung 7-8** ist das Kontextmenü mit allen Optionen dargestellt.

The screenshot shows the gICS interface for 'Einwilligungen'. On the left is a navigation menu with categories like 'Dokumente', 'Teilnehmer', 'Formulare', 'Analysen', and 'Einstellungen'. The main area shows a table with 4 entries. The first entry is highlighted, and a context menu is open over it. The table columns are: Datum, Teilnehmer-IDs, Vorlage, Version, Qualitätsstatus, Details, and Eigenschaften. The context menu options are: Details, Teilnehmer-ID kopieren, Teilnehmer-ID hinzufügen, Scan herunterladen, Scan ersetzen, Qualitätsstatus setzen, Kommentar, Externe Eigenschaften, Invalidieren, and Drucken.

Datum	Teilnehmer-IDs	Vorlage	Version	Qualitätsstatus	Details	Eigenschaften
02.02.2021 10:36:52		Inteneinwilligung MII [Allgemein]	1.6.d	Automatisch		
01.02.2021 15:04:45		Inteneinwilligung MII [Allgemein]	1.6.d	Nicht geprüft		
01.02.2021 10:20:03		Inteneinwilligung MII [Allgemein]	1.6.d	Nicht geprüft		
01.02.2021 10:16:54		Inteneinwilligung MII [Allgemein]	1.6.d	Geprüft, keine Fehler		

Abbildung 7-8: Kontextmenü zu einer Einwilligung.

Auf der rechten Seite befindet sich ein Filterfeld, mithilfe dessen die Einträge nach Teilnehmer-ID, Vorlage oder Version gefiltert werden können. Alternativ kann nach Qualitätsstatus gefiltert werden. Hierzu wird in der Kopfzeile der Tabelle das Feld *Qualitätsstatus* angewählt. Danach können ein oder mehrere Status ausgewählt werden.

⚠ Hinweis: Wenn nach Qualitätsstatus gefiltert wird, bleibt das Filterfeld (für Teilnehmer-ID, Vorlage und Version) unberücksichtigt. Soll der Qualitätsstatus nur für eine Teilnehmer-ID beispielsweise gefiltert werden, kann die Suche unter dem Menüpunkt *Teilnehmer* verwendet werden (vgl. **Abschnitt 7.8**).

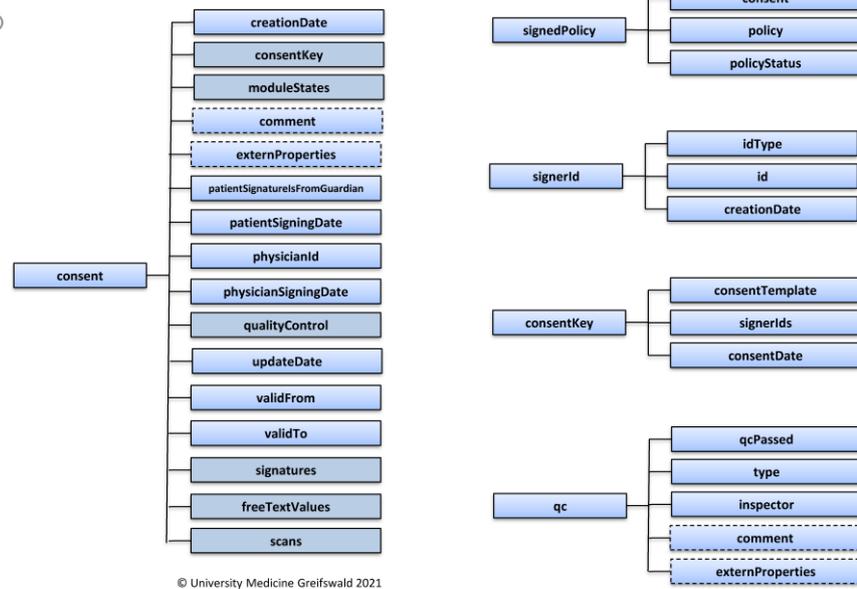


Abbildung 7-9: Überblick der Attribute einer im gICS abgebildeten Einwilligung. Attribute mit gestricheltem Rand sind optional, alle anderen sind Pflichtattribute und müssen (zumindest leer) gesetzt werden.

7.5 Abfragen von Einwilligungsdetails

Das Abfragen einer Einwilligung erfolgt primär automatisiert über die bereitgestellte Webschnittstelle (vgl. Entwicklerdokumentation⁴ und **Kapitel 12**) und ermöglicht gezielt den Einwilligungsstatus von Policies für einen definierten Patienten zu ermitteln (Beispiele mittels SOAP-Schnittstelle in **Kapitel 12**). Je nach Konfiguration (vgl. **Abschnitt 7.1**) bezieht sich diese Abfrage stets auf die neuesten Policies bzw. die Policies mit der höchsten Versionsnummer (abhängig von der Domänenkonfiguration, siehe **Abschnitt 7.1**).

Wie für mehrere Teilnehmer der Einwilligungsstatus zu einer bestimmten Policy abgefragt werden kann, wird in **Abschnitt 7.9** detailliert erklärt.

Alternativ kann die Web-Oberfläche zur Anzeige vorhandener Einwilligungen oder die Suchfunktion (siehe **Abschnitt 7.8**) genutzt werden. Eine Filterfunktion erlaubt die Anzahl der angezeigten Datensätze entsprechend den Filterparametern (Datum, Vorlagenname, Teilnehmer-ID) zu reduzieren. Sofern vorhanden können einer Einwilligung zugeordnete Dokumentenscans direkt eingesehen oder heruntergeladen werden.

Jede Einwilligung kann zudem über die Detailansicht genauer betrachtet werden. In **Abbildung 7-10** ist die Detailansicht zu einer Einwilligung abgebildet.

⁴ <https://www.ths-greifswald.de/wp-content/uploads/tools/gics/doc/2-10-0/>

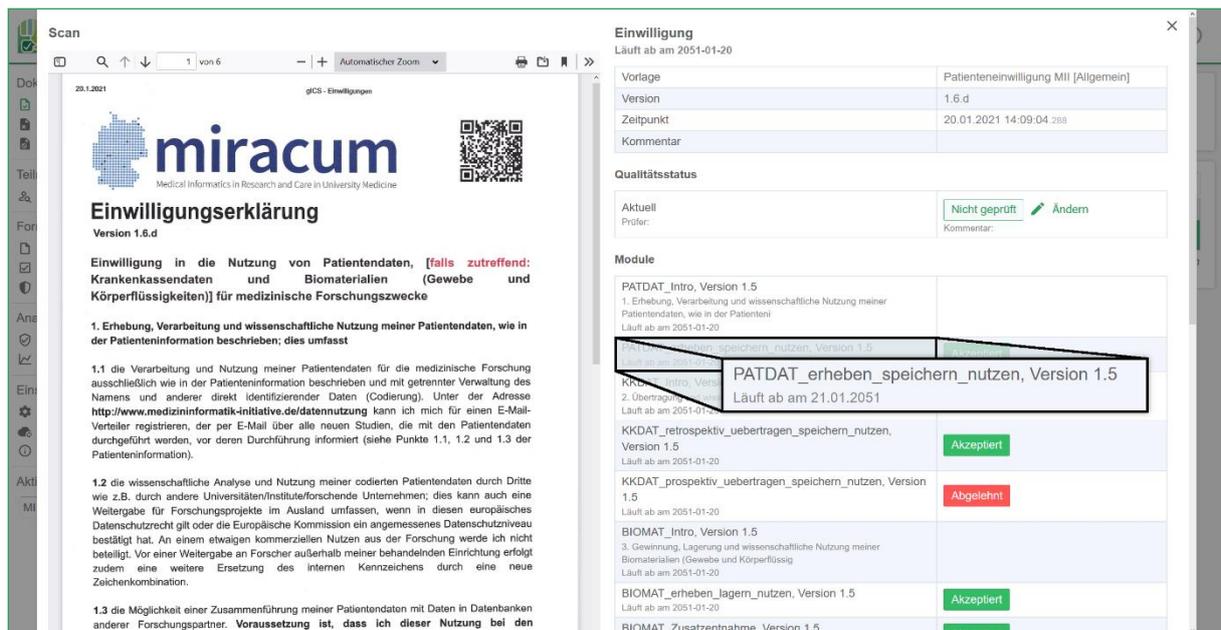


Abbildung 7-10: Detailansicht einer Einwilligung. Hierbei kann der Einwilligungsstatus jedes Moduls eingesehen werden. Dabei ist auch ersichtlich, wann ein Modul abläuft, sofern ein Ablaufdatum oder -zeitraum definiert wurde (siehe Abschnitt 7.7).

Zu jeder Einwilligung kann ein Kommentar mit maximal 255 Zeichen gesetzt werden. Dieser kann ebenfalls in den Einwilligungsdetails eingesehen werden.

7.6 Bearbeiten, Duplizieren und Finalisieren

7.6.1 Bearbeiten

Manchmal ist es nötig eine Vorlage oder ein Modul zu bearbeiten. Wenn das entsprechende Element noch nicht finalisiert wurde, kann dies ohne Einschränkungen getan werden. Ist beispielsweise eine Vorlage bereits finalisiert und im produktiven Einsatz, dann darf die Semantik der Vorlage nicht mehr verändert werden. Es ist dann nicht mehr möglich alle Felder zu bearbeiten. Bei einer Vorlage kann so beispielsweise nur der Name, der Kommentar und die externen Eigenschaften bearbeitet werden. Soll auf Basis einer finalisierten Vorlage eine neue Version angelegt werden, dann muss diese zuvor dupliziert werden. Die dadurch entstehende Kopie kann wiederum frei bearbeitet werden, bis diese finalisiert wird. Hierbei muss dann die Versionsnummer entsprechend angepasst werden.

7.6.2 Duplizieren

Soll auf Basis einer bestehenden Vorlage, Modul oder Policy eine Kopie angelegt werden um die Eigenschaften zu übernehmen, können die entsprechenden Elemente dupliziert werden. Eine Vorlage, Modul oder Policy kann in der jeweiligen Übersichtsseite mithilfe des Kontextmenüs und der Aktion *Duplizieren* kopiert werden. In **Abbildung 7-11** wird das entsprechende Kontextmenü exemplarisch an Policies gezeigt.

The screenshot shows the gICS Policies interface. On the left is a navigation sidebar with categories like 'Dokumente', 'Teilnehmer', 'Formulare', 'Analysen', and 'Einstellungen'. The main area displays a table of 27 policies. A context menu is open over the first row, showing options: 'Bearbeiten', 'Duplizieren', and 'Löschen'.

Name	Version	Beschreibung	Erstellung	Letzte Bearbeitung	Aktionen
BIOMAT_Analysedaten_zusammenfuehren_Dritte	1.0	zusammenführen von biomat analysedaten m...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
BIOMAT_bereitstellen_EU_C	1.0	Herausgabe von Biomaterialien (BIOMAT) an ...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
BIOMAT_Eigentum_uebertra	1.0	Eigentumsübertragung der BIOMAT an den T...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
BIOMAT_erheben	1.1	Gewinnung von Biomaterialien (BIOMAT)	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
BIOMAT_lagern	1.0	Lagern bzw Speichern von Biomaterialien (Bl...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
BIOMAT_nutzen	1.0	Wissenschaftliche Nutzung und Analyse von ...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
BIOMAT_Zusatzmengen_entnehmen	1.0	neue policy in mil consent 1.6.d zur entnahme...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
IDAT_bereitstellen_EU_DSGVO_konform	1.0	Herausgabe identifizierender Daten (IDAT) an...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
IDAT_erheben	1.0	Erfassung neuer identifizierender Daten (IDAT)	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]
IDAT_nutzen	1.0	Wissenschaftliche Nutzung identifizierender D...	20.01.2021 13:42:44	20.01.2021 14:05:47	[Bearbeiten] [Löschen]

Abbildung 7-11: Kontextmenü mit den Aktionen Bearbeiten, Duplizieren und Löschen am Beispiel von Policies.

Unabhängig davon, ob ein finalisiertes Element dupliziert wird, kann die Kopie frei bearbeitet werden und separat finalisiert werden. Eine Kopie ist immer dann nötig, wenn ein bereits finalisiertes Element bearbeitet werden soll und die Änderungen eine semantische Veränderung bedeuten. In diesem Fall wird die Kopie entsprechend bearbeitet und die Versionsnummer gemäß den Festlegungen (vgl. **Abschnitt 7.1**, vgl. **Tabelle 7-1**) erhöht.

7.6.3 Finalisieren

Vorlagen und Module sollten vor dem produktiven Einsatz finalisiert werden. Dies stellt sicher, dass keine semantischen Änderungen mehr an den jeweiligen Elementen vorgenommen werden können. Eine Vorlage oder ein Modul gilt solange sie oder es nicht finalisiert wurde als Entwurf. Beim Ausdruck (s. **Abschnitt 7.11**) einer Vorlage wird der Hinweis „nicht final“ als Wasserzeichen über den Ausdruck gelegt. Eine Vorlage kann finalisiert werden, indem in der Vorlagenübersicht die Aktion *Entwurf Finalisieren* ausgeführt wird. Dies hat zur Folge, dass alle in dieser Vorlage verwendeten Module ebenfalls finalisiert werden. Analog dazu kann ein Modul in der Modulübersicht finalisiert werden. Nicht finalisierte Module oder Vorlagen sind in der jeweiligen Übersicht als *Entwurf* markiert.

⚠ Hinweis: Die direkte Aktualisierung eines Informed Consent ist aufgrund der notwendigen Nachverfolgbarkeit und Nachvollziehbarkeit der Einwilligungsprozesse nicht angedacht. Es ist jedoch möglich eine erneute Einwilligung mit entsprechend aktualisierten Angaben anzulegen (vgl. **Abschnitt 7.3**).

7.7 Gültigkeit von Einwilligungen und Modulen automatisch ablaufen lassen

In manchen Fällen kann es nötig sein, dass eine Einwilligung automatisch nach einer gewissen Zeit abläuft. Manchmal sollen aber nur einzelne Module ablaufen. Beides kann bei der Erstellung einer Einwilligungsvorlage definiert werden.

Ein automatisches Ablauf einer Einwilligung kann auf zwei Weisen stattfinden. Entweder es wird ein fixes Datum festgelegt. Danach laufen alle Einwilligungen, unabhängig des Zeitpunkts der Erfassung, automatisch ab. Zum anderen kann eine Zeitspanne definiert werden. Eine Einwilligung läuft dann erst nach Erreichen dieser Zeitspanne nach Zeitpunkt der Unterzeichnung ab.

Gleiches kann ebenso für Module und Policies eingerichtet werden. Hierbei laufen aber nur einzelne Module ab, die Einwilligung und alle anderen Module bleiben dabei weiterhin gültig. Damit kann eine Vorlage modelliert werden, bei der beispielsweise das Modul für die Erhebung von weiteren Daten nach 5 Jahren automatisch abläuft, jedoch andere Module zum Beispiel zum Verarbeiten bestehender Daten weiterhin gültig ist.

Die Einstellung zum Eintragen des Ablaufdatums oder -zeitraums ist unter dem Punkt *Sonstiges* zu finden. In **Abbildung 7-12** wird die entsprechende Oberfläche dargestellt.

▼ Sonstiges

Kommentar 255 Zeichen verbleibend

Ablauf der Vorlage

Nie An Datum Nach Zeitraum

Jahre 5

Monate 0

Tage 0

Externe Eigenschaften 255 Zeichen verbleibend

Abbildung 7-12: Definition eines Ablaufs einer Einwilligung, hier am Beispiel eines Ablaufzeitraums.

Um ein Ablaufdatum für ein Modul zu definieren, kann in der Vorlage das entsprechende Modul bearbeitet werden. Mit Klick auf den Button *Ablauf dieses Modules* kann die entsprechende Option hinterlegt werden. In **Abbildung 7-13** ist die entsprechende Oberfläche dargestellt.

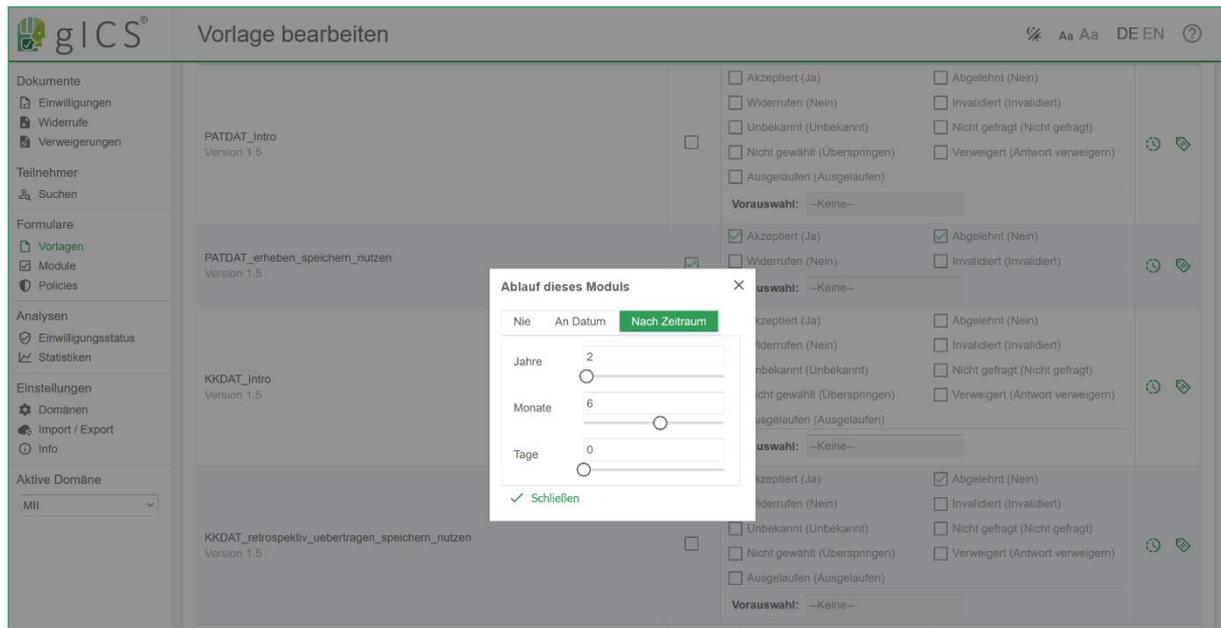


Abbildung 7-13: Definition eines Ablaufdatums eines Moduls.

Bei der Verwaltung von Einwilligungen sind unterschiedlichste Datumsangaben zu berücksichtigen. Nachfolgende Tabelle zeigt eine Übersicht der erhobenen und errechneten Datumsangaben, die bei der Auswertung von Einwilligungsangaben eine wesentliche Rolle spielen.

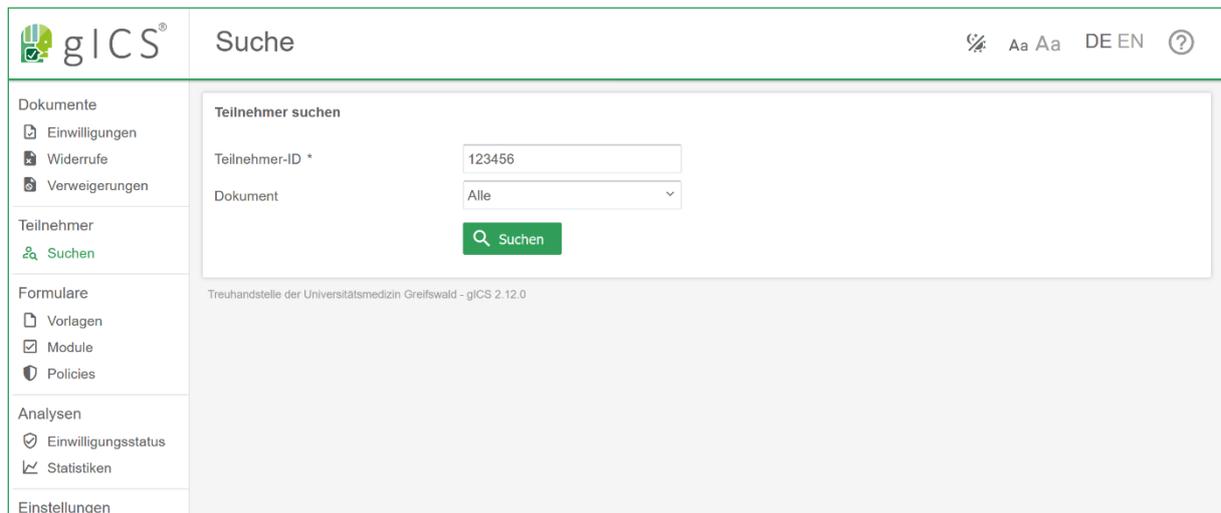
Tabelle 7-3: Übersicht der verwendeten Datumsangaben.

Art des Datums	Interne Bezeichnung (DTO)	Automatischer Wert	Bemerkung
„ausgefüllt am“	Consent:Key:ConsentDate	Nein	Extern vorgegeben beim Ausfüllen der Einwilligung
„erstellt am“	Consent:CreationDate	Ja	
„aktualisiert am“	Consent:UpdateDate	Ja	
„gültig von“	Consent:ValidFrom	Nein	Extern vorgegeben beim Ausfüllen der Einwilligung
Datum der Unterschrift	Signature:SignatureDate	Nein	Extern vorgegeben beim Ausfüllen der Einwilligung
Beginn Gültigkeit der Einwilligung	Consent:LegalConsentDate	Ja	Max von (CreationDate, SignatureDate, ValidFrom)
Ende der Gültigkeit (SignedPolicy)	SignedPolicy:ExpirationDate	Ja	Das kleinste Ablaufdatum, das sich aus den ExpirationProperties aller übergeordneten Elemente ergibt
Ende der Gültigkeit (Consent)	maxExpirationPolicyDate	Ja	Infocfeld: Max von ExpirationDate der zugeordneten SignedPolicies

⚠ Hinweis: Das **ConsentDate** wird extern vorgegeben und **Datenbank-intern** ausschließlich als Identifikator verwendet. Es wird **nicht** bei der Gültigkeitsberechnung von Einwilligungsinhalten berücksichtigt.

7.8 Dokumenten-Suche (Ermittlung des zeitlichen Verlaufs)

Mithilfe der Suche können alle gespeicherten Einwilligungen, Widerrufe und Verweigerungen durchsucht und nach Teilnehmer-ID aufgelistet werden. Dabei kann zusätzlich der Typ des Dokuments gefiltert werden. Alle aufgelisteten Einträge können eingesehen und bearbeitet werden. Zusätzlich können die jeweiligen Scans heruntergeladen werden. Außerdem besteht die Möglichkeit die Einträge weiter zu filtern. Hierfür ist ein Suchfeld vorhanden, womit über alle Felder der Auflistung hinweg gefiltert werden kann. In **Abbildung 7-14** ist die Oberfläche beim exemplarischen Suchen von Einwilligungen abgebildet und in **Abbildung 7-15** die daraus resultierende Liste von gefundenen Einwilligungen, Widerrufe und Verweigerungen. Je nach Dokumentenart, werden die gefundenen Einwilligungen, Widerrufe und Verweigerungen durch unterschiedliche Icons dargestellt.



The screenshot shows the 'gICS' search interface. The title bar includes the logo, the word 'Suche', and utility icons for search, font size, language (DE/EN), and help. A left sidebar contains a navigation menu with categories: Dokumente (Einwilligungen, Widerrufe, Verweigerungen), Teilnehmer (Suchen), Formulare (Vorlagen, Module, Policies), Analysen (Einwilligungsstatus, Statistiken), and Einstellungen. The main content area is titled 'Teilnehmer suchen' and features two input fields: 'Teilnehmer-ID *' with the value '123456' and 'Dokument' with a dropdown menu set to 'Alle'. A green 'Suchen' button is positioned below the fields. At the bottom of the main area, the text 'Treuhandstelle der Universitätsmedizin Greifswald - gICS 2.12.0' is visible.

Abbildung 7-14: Oberfläche zur exemplarischen Suche von Dokumenten.

The screenshot shows the gICS search results page. On the left is a navigation sidebar with categories like 'Dokumente', 'Teilnehmer', 'Formulare', 'Analysen', 'Einstellungen', and 'Aktive Domäne'. The main content area is titled 'Suchergebnisse' and contains a search bar, a list of document types, and a detailed view for a specific participant, 'Teilnehmer 123456'. This view shows that 24 policies are accepted, 3 are rejected, and 0 are not set. Below this is a table with one document entry, showing its type, date, participant ID, template, version, and quality status ('Geprüft, keine Fehler').

Abbildung 7-15: Oberfläche beim exemplarischen Finden von Einwilligungen und Widerrufen.

Zu dem gefundenen Teilnehmer kann direkt die Anzahl von akzeptierten, abgelehnten und nicht gesetzten Policies eingesehen werden. Außerdem können weitere Aktionen durchgeführt werden: *Einwilligung erfassen*, *Widerruf erfassen* und *Teilnehmer zusammenführen*. Bei den ersten beiden Aktionen wird im jeweiligen Einwilligungs- oder Widerrufsformular automatisch die Teilnehmer-ID eingetragen. Wurde die teilnehmende Person mit unterschiedlichen IDs erfasst, kann diese Person mittels der zwei erfassten IDs zusammengeführt werden. Hierzu wird die Schaltfläche Teilnehmer zusammenführen gewählt und die zwei IDs entsprechend angegeben. Je nach Domäne kann dabei der ID-Typ und die jeweilige ID angegeben werden.

7.9 Durchführung von Analysen

Einwilligungsstatus von Teilnehmern ermitteln und exportieren

Im Regelfall sind zwei Arten von Auskünften erforderlich, die sich über den Menüpunkt *Einwilligungsstatus* auf einfache Weise beantworten lassen:

- Wie genau haben **ausgewählte Teilnehmer** in eine bestimmte Policy (z.B. Herausgabe von Forschungsdaten an Dritte) eingewilligt?
- Wie haben **alle Teilnehmer** eines Projektes in eine bestimmte Policy eingewilligt?

Für Fall a) ist eine Liste von Teilnehmer-IDs (Signer-IDs) im CSV-Format erforderlich. Nach dem Hochladen der entsprechenden Datei („Liste mit Teilnehmer-IDs hochladen“) in Schritt 1, wird das Encoding automatisch erkannt. Sollte die Import-Datei mehr als eine Spalte enthalten, kann die Spalte mit Signer-IDs in Schritt 2 gewählt werden. In Schritt 3 wird spezifiziert, welche Policy genau analysiert werden soll, ob ein detailliertes Resultat angezeigt werden soll (konkreter Policy-Status anstelle eines vereinfachten True/False) und auf welche Art von Signer-ID sich die Analyse fokussiert (im Fall von mehreren konsentierten Signer-IDs). Details dazu sind in der nachstehenden **Abbildung 7-16** dargestellt. Das gesamte Analyseergebnis kann anschließend als CSV gespeichert werden.

Im Fall b) wird auf die Eingrenzung der Analyse in Bezug auf ausgewählte Teilnehmer verzichtet. Der Rest erfolgt analog.

⚠ Hinweis: Schritt 3 kann in beiden Modi beliebig oft mit unterschiedlichen Policies durchgeführt werden. Das angezeigte Ergebnis wird jeweils um eine neue Spalte erweitert.

Abbildung 7-16: Ermittlung des Einwilligungsstatus einer Policy für eine gegebene Liste von Teilnehmern.

Kennzahlenermittlung und Abruf allgemeiner Statistiken

Die Statistik-Übersicht ist erreichbar über den Menüpunkt *Statistiken* und bietet eine tabellarische Zusammenfassung der aktuellen Elemente in der gICS Datenbank zum Zeitpunkt des Aufrufs (Kennzahlen des gICS) der Statistik-Seite. Sowohl die aktuellen Kennzahlendaten, als auch die Kennzahlendaten seit Initialisierung der gICS Datenbank können als CSV-Datei heruntergeladen werden.

Diagrammdarstellungen geben Aufschluss über zeitliche Verläufe (z.B. Anzahl von Einwilligungen und Widerrufen über die Zeit) und können als PNG-Dateien gespeichert werden.

⚠ Hinweis: Die Generierung der gICS Kennzahlen wird täglich und automatisch innerhalb der gICS Datenbank ausgelöst, um zeitliche Verläufe darstellen zu können.

7.10 Export und Import von Domänenkonfigurationen und Vorlagen

Vorhandene Konfigurationen von Vorlagen, Modulen und Policies und Domänen können im JSON- und/oder XML-Format exportiert werden.

Export

Beim Export kann gewählt werden, welche Elemente exportiert werden sollen. Hierbei kann gewählt werden zwischen einem Export aller Elemente, nur der Domäne, sowie nur Vorlagen, Modulen und Policies. Bei den letzten dreien besteht zudem die Möglichkeit die entsprechend vorhandenen Vorlagen, Modulen oder Policies auszuwählen, welche exportiert werden sollen. Die Export-Funktion ist erreichbar in den Einstellungen mittels Klick auf den Button *Import/Export*. Um beispielsweise eine Vorlage und alle dafür notwendigen Module, Policies und Konfigurationen zu exportieren (vgl. **Abbildung 7-17**) muss zunächst die gewünschte Domäne ausgewählt werden. Soll ein eventuell vorhandenes Logo mitexportiert werden, ist das entsprechende Häkchen zu setzen. Um ein oder mehrere Vorlagen zu exportieren, muss unter Inhalte *Vorlagen auswählen* und im Anschluss die gewünschten Vorlagen per Drag & Drop ausgewählt werden. Je nach Wunsch können die Exporte als eine XML- oder JSON-Datei erzeugt werden.

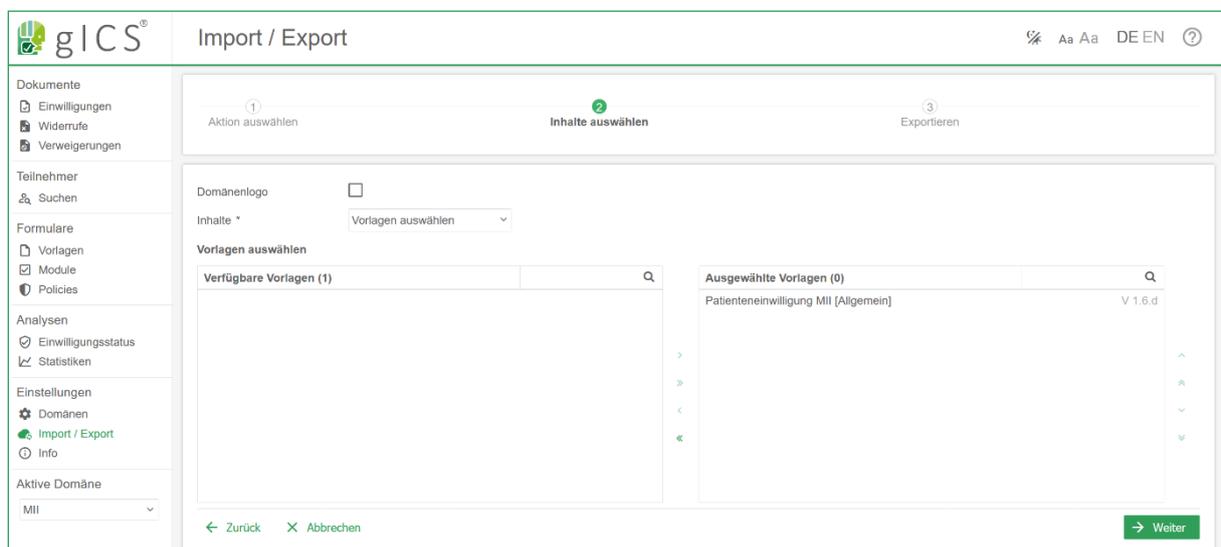


Abbildung 7-17: Oberfläche beim exemplarischen Export der Vorlage „Patienteneinwilligung MII [Allgemein]“.

Import

Die Import Funktion arbeitet entsprechend analog. Nach Auswahl der zu importierenden Datei zeigt ein Vorschau-Fenster (**Abbildung 7-18**) welche neuen Inhalte importiert werden und welche Import-Inhalte übersprungen werden, da sie in gICS bereits vorhanden sind. Sollen vorhandene Inhalte in gICS beim Import-Prozess überschrieben werden, muss die *Aktualisierung von vorhandenen Elementen erlaubt* werden. Der Import-Prozess startet durch Klick auf *Import starten*. Eine sprechende Meldung im Nachgang fasst die Import-Vorgänge kurz zusammen.

gICS® Import / Export

1 Aktion auswählen 2 Datei hochladen 3 **Vorschau** 4 Ergebnis

Vorschau der 42 zu importierenden Elemente

Aktualisierung vorhandener Elemente erlauben

Typ	Name	Version	Aktion bei Import
Domäne	MII		Überspringen
Modul	BIOMAT_erheben_lagern_nutzen	1.5	Überspringen
Modul	BIOMAT_Intro	1.5	Überspringen
Modul	BIOMAT_Zusatzentnahme	1.5	Überspringen
Modul	Geltungsdauer	1.5	Überspringen
Modul	KKDAT_Intro	1.5	Überspringen
Modul	KKDAT_prospektiv_uebertragen_speichern_nutzen	1.5	Überspringen
Modul	KKDAT_retrospektiv_uebertragen_speichern_nutzen	1.5	Überspringen
Modul	PATDAT_erheben_speichern_nutzen	1.5	Überspringen
Modul	PATDAT_Intro	1.5	Überspringen

1-10 von 42

← Zurück × Abbrechen ✔ Importieren

Abbildung 7-18: Import von Vorlagen und weiteren Inhalten: das Vorschau-Fenster zeigt, welche Inhalte bereits im gICS vorhanden sind und ggf. ob auf Wunsch diese überschrieben werden sollen. Hierzu wird das Kontrollkästchen *Aktualisierung vorhandener Elemente erlauben* angewählt.

7.11 Vorlagendruck und automatische Erkennung von Einwilligungsinhalten

Drucken von Vorlagen

Die in gICS verwalteten Vorlagen für Einwilligungen, Widerrufe und Verweigerungen können direkt aus der jeweiligen Vorlagenübersicht über das Kontext-Menü (Rechtsklick auf die gewünschte Vorlage, Drucken) gedruckt werden. Dabei wird eine druckfähige HTML-Seite erzeugt, die entweder direkt gedruckt oder aber per PDF-Printer als PDF gespeichert werden kann.

⚠ Hinweis: Wenn der Einwilligungsprozess die automatische Erkennung von Einwilligungsinhalten mittels gICS beinhaltet, beachten Sie die Hinweise zur Druckskalierung. Der Vorlagendruck muss für eine erfolgreiche Inhaltserkennung mindestens 85% der ursprünglichen Seitendruckgröße gewährleisten. Eine entsprechende Hinweismeldung erscheint beim Vorlagendruck.

Der Anwender hat die Möglichkeit eine leere Vorlage zu drucken oder aber, sofern der unterzeichnende Teilnehmer bereits bekannt ist, 1 - n bereits ausgefüllte Druckvorlage zu erzeugen. Dafür notwendige Signer-IDs können per Hand angegeben oder per CSV importiert werden (vgl. **Abbildung 7-19**). Der generierte Druckauftrag enthält daraufhin entsprechend viele vollständige Einwilligungsvorlagen.

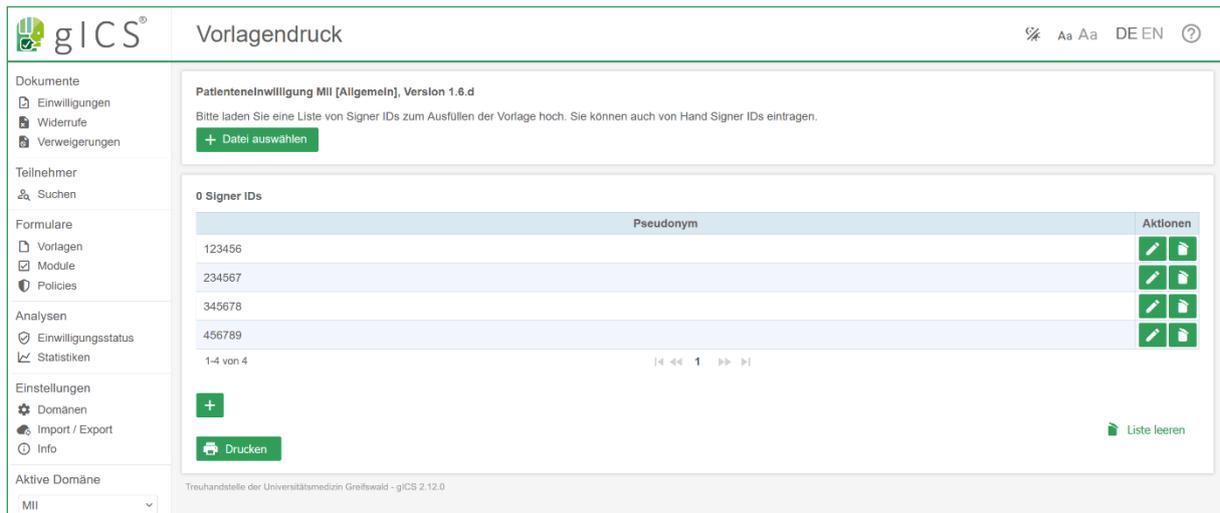


Abbildung 7-19: Es können mehrere Exemplare von Einwilligungsvorlagen auf einmal gedruckt / als PDF exportiert werden. Dabei können für jedes Exemplar Signer-IDs vorgeben werden.

Automatische Erkennung von Einwilligungsinhalten

⚠ Hinweis: Die automatische Erkennung von Einwilligungsinhalten steht derzeit nur im gICS bereit, wenn dieser auf einem System mit dem Betriebssystem Windows ausgeführt wird. Außerdem

Ab gICS 2.12.0 können Einwilligungsinhalte automatisch von Scans erkannt werden. Wurde eine Einwilligung auf Basis einer von gICS 2.12.0 (oder größer) erzeugten Druckvorlage erzeugt, kann ein Scan dieser Einwilligung bei der Dokumentation der Einwilligung in gICS automatisiert verarbeitet werden. Dazu sollte unter *Einwilligungen* eine neue Einwilligung *Hochgeladen und einlesen* werden.

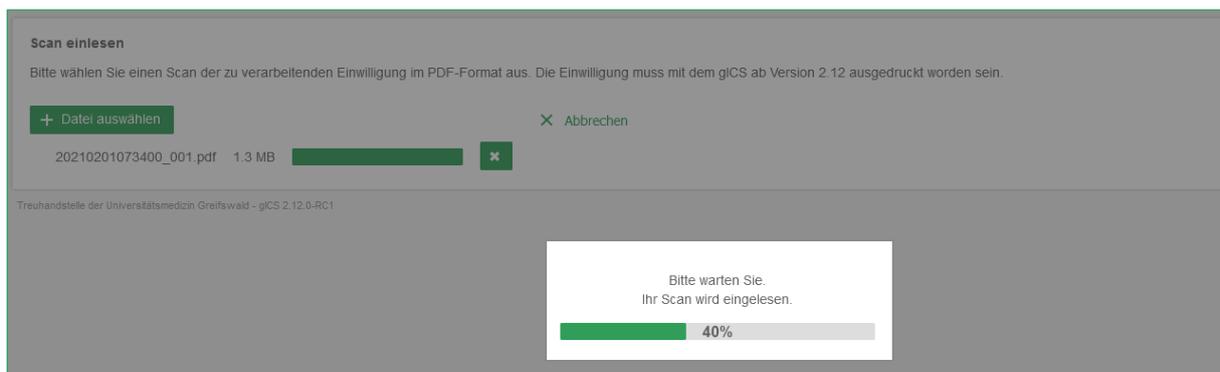


Abbildung 7-20: Automatische Erkennung der Einwilligungsinhalten bei Import einer gescannten Einwilligung im PDF-Format.

Nachdem die entsprechende PDF-Datei des Scans ausgewählt wurde, werden alle Seiten des Scans analysiert. Dabei sucht gICS den beim Druck erzeugten QR-Code der Vorlage im Dokument, der sowohl die Vorlagen-Kennung als auch eventuell vorhandene Signer-IDs enthält. Außerdem werden sämtliche im Scan vorhandenen Einwilligungsmodul sowie zugehörige vorhandene oder fehlende Kreuzchen des Teilnehmers ermittelt. Bereits während der Inhaltsermittlung variiert gICS die einzelnen Parameter und Schwellwerte, um bestmögliche Erkennungsergebnisse zu erzielen.

Im Anschluss wird das Ergebnis des Erkennungsprozesses angezeigt.

⚠ **Warnung: Skalierte Druckversion erkannt.** Enthaltene QR-Codes sind ggf. zu klein. Für optimale Erkennungsergebnisse darf beim Druck der Vorlage eine Skalierung von 85% nicht unterschritten werden.

ℹ **Information:** Bitte die erkannten Einwilligungsinhalte vor dem Speichern prüfen und ggf. vorhandene Freitextfelder manuell setzen.

Vorlage

Einwilligungserklärung SARS-CoV-2 - Klinische Datenbank und Biobank (Studie 2)
 Version 1.4.a

Abbildung 7-21: Automatische Erkennung der Einwilligungsinhalten bei Import einer gescannten Einwilligung im PDF-Format.

⚠ **Hinweis:** Wurde die Einwilligungsvorlage nicht auf 100% der Druckgröße gedruckt, erscheint die "Meldung skalierte Druckversion erkannt. Enthaltene QR-Codes sind ggf. zu klein. Für optimale Erkennungsergebnisse darf beim Druck der Vorlage eine Skalierung von 85% nicht unterschritten werden."

Nach Verarbeitung des Scans, werden automatisch die erkannte Vorlage der entsprechenden Einwilligungsdomäne in der korrekten Vorlagen-Version ausgewählt, werden vorhandene Signer-IDs in die entsprechenden Felder übernommen und wird das PDF dem Einwilligungsdatensatz direkt als gescanntes Dokument angehängen. Eine zusätzliche digitale Unterschrift ist nicht erforderlich.

Alle erkannten Einwilligungsmodule, für die ein Einwilligungsstatus erkannt wurde, wurden bereits entsprechend gesetzt. Sollten zu wenige/zu viele Einwilligungsmodule erkannt worden sein, weist eine entsprechende Meldung den Anwender darauf hin. Gleiches gilt, sollten zu wenige/zu viele als die erwarteten Einwilligungsstatus je Modul erkannt worden sein.

Der Anwender sollte nun eine Sichtprüfung (Original/erkannte Werte) durchführen und die Information zum Teilnehmer und zur aufklärenden Person übertragen.

8 Qualitätsstatus

Zu jeder Einwilligung, jedem Widerruf und jeder Verweigerung (allgemein Dokument) kann ein Qualitätsstatus hinterlegt werden. Die Option zum Setzen oder Ändern des Qualitätsstatus wird entweder in der jeweiligen Dokumentenliste über das Kontextmenü oder über die Dokument-Details (vgl. **Abschnitt 7.5**) erreicht. Der Status kann grundsätzlich zwischen *gültig* und *ungültig* festgelegt werden, wobei es weitere Abstufungen geben kann. So gibt es für gültige Status die Ausprägungen: *Geprüft, geringfügige Fehler* und *Geprüft, keine Fehler*. Der Status für ungültige Status besitzt die Ausprägung: *Geprüft, wesentliche Fehler*. Je nachdem wie die Domäne konfiguriert wurde (vgl. unten) kann der Status *Nicht geprüft* festgelegt werden. Beim Setzen des Status ist zusätzlich noch die Angabe einer prüfenden Person erforderlich. Des Weiteren kann ein optionaler Kommentar hinterlegt werden. Der Dialog zum Setzen oder Ändern des Qualitätsstatus ist in **Abbildung 8-1** abgebildet.

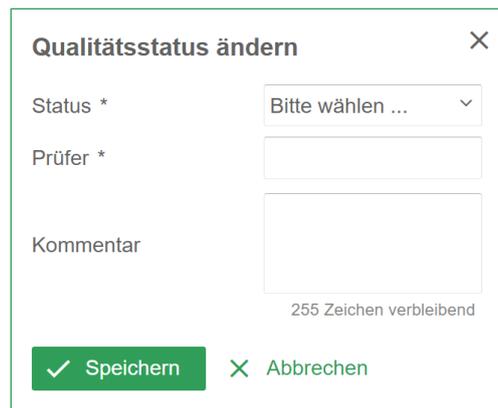


Abbildung 8-1: Dialog zum Setzen oder Ändern des Qualitätsstatus einer Einwilligung, eines Widerrufs oder einer Verweigerung.

Nach dem Anlegen einer Einwilligung wird der Qualitätsstatus mit *Automatisch* angegeben. Dieser Status kann nach erfolgter Prüfung durch den entsprechenden Status ersetzt werden.

Ob ein Dokument auch ohne eine Überprüfung gültig ist, wird bei der Erstellung der Domäne festgelegt (siehe **Abschnitt 7.1**). Hier kann unter dem Punkt *Qualitätssicherung* angewählt werden, ob ungeprüfte Dokumente erlaubt sind. Wird das Kästchen angewählt, kann der Qualitätsstatus bei einem Dokument der Status auf geprüft mittels der Ausprägung *Nicht geprüft* gesetzt werden. Andernfalls ist diese Option nur für den Status *ungültig* möglich. In **Abbildung 8-2** wird die entsprechende Option dargestellt.

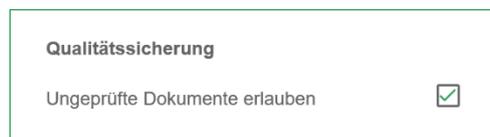


Abbildung 8-2: Option (beim Erstellen einer neuen Domäne) um ungeprüfte Dokumente zu erlauben/nicht zu erlauben. Hier werden exemplarisch auch ungeprüfte Dokumente mit dem Status gültig zugelassen.

9 Logging

⚠ Hinweis: Details für die Anpassung der Logging-Konfiguration entnehmen Sie bitte der beigelegten Beschreibung docker-compose/README.md (Abschnitt Logging).

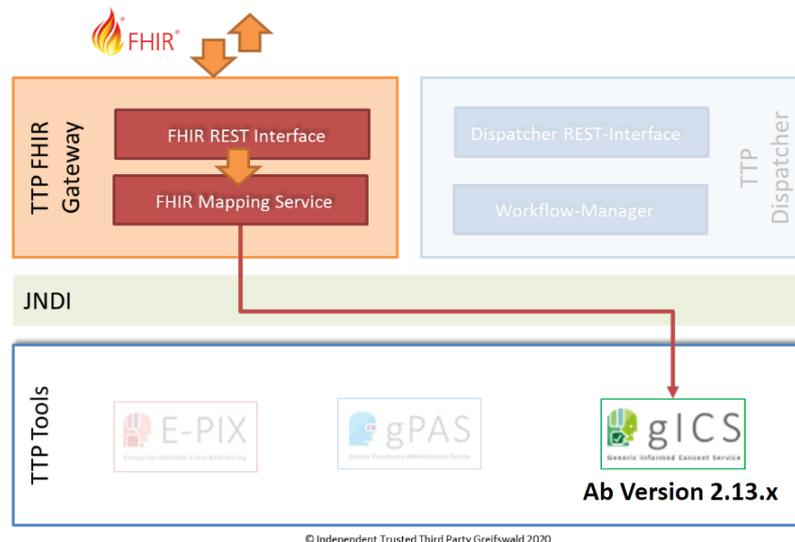
10 FHIR-Unterstützung für gICS per TTP FHIR-Gateway

„Fast Healthcare Interoperability Resources (kurz: FHIR®) ist ein von HL7 erarbeiteter Standard. Dieser unterstützt den Datenaustausch zwischen Softwaresystemen im Gesundheitswesen. FHIR beschreibt Datenformate und Elemente als sogenannte „Ressourcen“ und bietet eine Schnittstelle an, um diese auszutauschen“⁵.

⁵ https://de.wikipedia.org/wiki/Fast_Healthcare_Interoperability_Resources, Zugriff am 22.01.2021

Um sowohl bestehende Anwenderprojekte als auch künftige Nutzer bei der Umsetzung FHIR-orientierter Infrastrukturen und Prozesse zu unterstützen, wird ab gICS-Version 2.13.0 ein zusätzliches Treuhandstellen-FHIR-Gateway (kurz: TPP-FHIR Gateway) als Mittler von FHIR-spezifischen Infrastrukturkomponenten und gICS bereitgestellt.

⚠ Hinweis: Da gICS als datenhaltendes System sämtliche Einwilligungen und Widerrufe verwaltet, ist gICS auch für die Generierung und Verwaltung der erforderlichen FHIR-UUIDs verantwortlich. Dieses Feature wird erst ab gICS 2.13.x unterstützt.



Für ausgewählte Funktionalitäten zum Abruf von Einwilligungsinhalten in FHIR wurden nachfolgende Funktionen (Auszug) umgesetzt und sind nach erfolgreichem Deployment des TPP FHIR Gateways direkt per REST nutzbar.

Der aktuelle Funktionsumfang (FHIR-Operations) des TPP FHIR Gateway (Auszug) umfasst unter anderem:

- Abruf aller Einwilligungen einer Einwilligungsdomäne
- Abruf der aktuellen Einwilligung eines Patienten (unter Angabe des Templates, z.B. MII Broadconsent 1.6.f)
- Personenspezifische Einwilligungsstatusprüfung
- Abruf aller unterzeichneten Policies einer Person

⚠ Hinweis: Die Profilierung der erforderlichen Profile, Codesysteme und Operations erfolgte in Zusammenarbeit mit der Fa. gefyra6. Deren Umsetzung setzt auf den Vorarbeiten der AG Einwilligungsmanagement auf.⁷

⁶ <https://www.gefyra.de/>, Zugriff am 2021-06-08

⁷ <https://simplifier.net/Einwilligungsmanagement>, Zugriff am 2021-06-08

⚠ Hinweis: Sämtliche Profile, Codesysteme und OperationDefinitions sind unter <https://simplifier.net/ths-greifswald> dokumentiert. Insbesondere ist ein einheitliches und erweiterbares Codesystem für Einwilligungspolicies⁸ entstanden, das gängige Policies der Treuhandstelle Greifswald abdeckt und per Default bei FHIR-Consent-Exporten mittels FHIR Gateway berücksichtigt wird.

Der zugehörige Implementation Guide mit konkreten Beispielen (Work-in-Progress) ist zu finden unter <https://simplifier.net/guide/ttp-fhir-gateway-ig/Einwilligungsmanagement>. In diesem wird ebenfalls auf die verfügbaren [Suchparameter](#) zum FHIR-Abruf von ausgewählten Ressourcen verwiesen, wie

- *Domain* ([Consent Domain](#) erweitert Interop-Profil [ResearchStudy](#))
- *Policies* ([ConsentPolicy](#) basierend auf ActivityDefinition)
- *Modulen* ([Consent Module](#) erweitert das bestehende Interop-Profil [ConsentManagementTemplateModules](#))
- *Vorlagen* ([Consent Template](#) erweitert das bestehende Interop-Profil [Consent Template Frame](#))
- *Druckfähige Vorlage* (Interop-Profil [QuestionnaireComposed](#))
- *Ausgefüllten Einwilligungen* (Interop-Profil [QuestionnaireResponse](#))
- *Operationalisierten Einwilligungen* (Interop-Profil [Consent](#))

⚠ Hinweis: Standardmäßig liefert das FHIR Gateway, sofern vorhanden, gICS-spezifische Varianten der einzelnen Einwilligungsprofile aus. Die Auslieferung der Inhalte in den jeweiligen Interop-Varianten sind im Regelfall per `_profile`-Parameter möglich.

Festlegung des SAFE_SIGNERID_TYPE

Diese Konfiguration erfolgt als Teil der Domänen-Konfiguration. Weitere Details unter **Abschnitt 7.1 Anlegen von Domänen**.

Individualisierung von FHIR Ressourcen

Standardmäßig werden bei der Bereitstellung von gICS-Inhalten in Form von FHIR Ressourcen durch das TTP FHIR Gateway gICS-spezifische Referenzen und Codings für z.B. bei Antwortoptionen in Vorlagen (Questionnaires), Referenzen auf Fragen bei Einwilligungsmodulen (TemplateFrame) und Policy-Semantik (Consent.Provisions), verwendet.

Diese können durch Verwendung entsprechender External Properties zum Beispiel über die gICS-Oberfläche konfiguriert oder durch Import eines benutzerdefinierten Template-Import-Formates angepasst werden (vgl. Export und Import). Nachfolgende Tabellen zeigen External Properties, die bei Vorhandensein bei der Erzeugung von FHIR Ressourcen berücksichtigt werden. Die drei Individualisierungsmöglichkeiten können unabhängig voneinander genutzt werden.

⁸ <https://simplifier.net/guide/ttp-fhir-gateway-ig/Policy>, Zugriff am 2021-06-08

Tabelle 10-1: Individualisierung von FHIR Consent.Provision.Coding durch ausgewählte External Properties.

External Property	Zugehöriges Einwilligungselement	Berücksichtigung bei FHIR Element	Optional
fhirPolicyCodesystem	Einwilligungsvorlage. Wirkt sich auf alle der Vorlage zugewiesenen Policies aus.	Consent.Provision.Coding.System	Nein
fhirPolicyCode	Einwilligungspolicy	Consent.Provision.Coding.Code	Nein
fhirPolicyDisplay	Einwilligungspolicy	Consent.Provision.Coding.Display	Ja

Tabelle 10-2: Individualisierung von FHIR Questionnaire.Item.linkId durch ausgewählte External Properties.

External Property	Zugehöriges Einwilligungselement	Berücksichtigung bei FHIR Element	Optional
fhirQuestionCode	Einwilligungsmodul	Questionnaire.Item.linkId	Ja

Tabelle 10-3: Individualisierung von Antworten und Antwort-Optionen bei FHIR Questionnaire und FHIR QuestionnaireResponse durch ausgewählte External Properties.

External Property	Zugehöriges Einwilligungselement	Berücksichtigung bei FHIR Element	Optional
fhirAnswerValueSet	Einwilligungsvorlage.	Questionnaire.Item.Item.AnswerValueset	Ja
fhirAnswerCodeSystem	Einwilligungsvorlage	Questionnaire.Item.Item.Initial und QuestionnaireResponse.Item.Anwer	Nein
fhirAnswerCodeYes	Einwilligungsvorlage	Questionnaire.Item.Item.Initial und QuestionnaireResponse.Item.Anwer	Nein
fhirAnswerDisplayYes	Einwilligungsvorlage	Questionnaire.Item.Item.Initial und QuestionnaireResponse.Item.Anwer	Ja
fhirAnswerCodeNo	Einwilligungsvorlage	Questionnaire.Item.Item.Initial und QuestionnaireResponse.Item.Anwer	Nein
fhirAnswerDisplayNo	Einwilligungsvorlage	Questionnaire.Item.Item.Initial und QuestionnaireResponse.Item.Anwer	Ja
fhirAnswerCodeUnknown	Einwilligungsvorlage	Questionnaire.Item.Item.Initial und QuestionnaireResponse.Item.Anwer	Nein
fhirAnswerDisplayUnknown	Einwilligungsvorlage	Questionnaire.Item.Item.Initial und QuestionnaireResponse.Item.Anwer	Ja

⚠ Hinweis: Änderungen an External Properties sind auch nachträglich bei bereits finalisierten und aktiv genutzten Vorlagen möglich, z.B. durch Import aktualisierter Einwilligungsvorlagen (Häkchen bei *allowUpdates* nicht vergessen).

Absicherung des FHIR-Gateway-API per Keycloak

Ab TTP-FHIR Gateway Version 2.0.0 ist eine Absicherung der TTP-FHIR-Gateway-Schnittstelle je Endpunkt (und somit je Werkzeug) vorgesehen und nach Bedarf konfigurierbar. Weitere Details sind separat dokumentiert unter <https://www.ths-greifswald.de/ttpfhirgateway/keycloak>.

11 Authentifizierungs- und Autorisierung

Die bereitgestellte gICS-Version (ab 2.12.0) bietet unterschiedliche Umsetzungsoptionen der Authentifizierungs- und Autorisierung in der **Docker-Compose**-Variante.

In der Standard-Ausgabe vom gICS ist keine Authentifizierung notwendig. Möchte man den gICS jedoch nur für bestimmte Nutzergruppen (Admin-Nutzer, Standard-Nutzer) zugänglich machen (vgl. **Tabelle 11-1**), oder sogar das Anlegen von neuen Domänen beschränken, können zwei Authentifizierungsverfahren angewendet werden. gRAS und keycloak, wobei es für KeyCloak zwei verschiedene Varianten gibt.

⚠ Hinweis: Die Auswahl der einzelnen Varianten erfolgt in der Docker-Compose Version innerhalb der `docker-compose.yml`. Details für die notwendige Anpassung der Docker-Konfiguration können der beigelegten Beschreibungen (<https://www.ths-greifswald.de/ttp-tools/keycloak>) sowie `docker-compose/README.md` entnommen werden.

Tabelle 11-1: Nutzer der Gruppe Admin und User haben unterschiedliche Zugriffsrechte in der Web-Oberfläche.

<i>Bereich/Seite</i>	<i>Zugang ohne Login</i>	<i>Zugang mit User-Rechten</i>	<i>Zugang mit Admin-Rechten</i>
<i>Dokumente: Einwilligungen</i>		×	×
<i>Dokumente: Widerrufe</i>		×	×
<i>Dokumente: Verweigerungen</i>		×	×
<i>Dokumente: Suche</i>		×	×
<i>Formulare: Templates</i>			×
<i>Formulare: Module</i>			×
<i>Formulare: Policies</i>			×

<i>Analysen: Einwilligungsstatus</i>		×	×
<i>Analysen: Statistiken</i>		×	×
<i>Einstellungen: Domänen</i>			×
<i>Einstellungen: Import / Export</i>			×
<i>Einstellungen: Info</i>	×	×	×

11.1 Verwendung von KeyCloak

Details zur Vorbereitung des KeyCloak-Servers sind in der beigelegten Beschreibung **KeyCloak-Einrichtung.md** zu finden.

Die Client-seitige KeyCloak-Konfiguration kann sowohl per Config-Datei als auch per Environment-Variablen bei Start des Docker-Compose erfolgen. Details sind in **docker-compose/README.md** beschrieben.

11.2 Verwendung von gRAS

Die gRAS Authentifizierungs- und Autorisierungsmechanismen basiert auf MySQL und JAXWS per Wildfly-Konfiguration. Nutzer müssen sich für die Nutzung des gICS mittels Benutzernamen (user@ths) und Passwort einloggen. Je nach zugeordneter Rolle enthalten sie unterschiedliche Berechtigungen. Eine Übersicht der Rollen und Rechte ist in der vorherigen **Tabelle 11-1** zu finden.

Bei der Installation des gICS mittels Docker werden standardmäßig ein Admin-Nutzer „admin“, sowie ein Standard-Nutzer „user“ angelegt. Die Anmeldung erfolgt unter Angabe der Domäne „THS“.

```
[Default-Admin] username="admin@ths", password="ttp-tools"
[Default-User]  username="user@ths", password="ttp-tools"
```

Die Autorisierung kann werkzeugübergreifend erfolgen. So kann ein und dieselbe Person z.B. beim E-PIX Standard-Nutzer und beim gICS Admin-Nutzer sein.

11.2.1 Verwaltung der Nutzer, Rollen und Rechte mittels MySQL und Docker EXEC

Die Verwaltung der Nutzer (anlegen, aktivieren, deaktivieren, Passwort ändern) und das Zuweisen von Rechten kann direkt in der entsprechenden Datenbank (gRAS) oder per *Docker EXEC* auf dem entsprechenden Datenbank-Container (hier: gICS-2.12.0-mysql) erfolgen.

Die Verwaltung erfolgt auf Basis entsprechender MySQL-Prozeduren. Diese werden im Zuge der Docker-Installation der Web-Auth-Version für gICS automatisch angelegt.

11.2.1.1 Nutzer anlegen

⚠ Hinweis: Das Nutzer-Passwort wird zwar im Klartext angegeben, die Prozedur jedoch erzeugt automatisch einen SHA-256-Hash, der in der gRAS-Datenbank gespeichert wird.

in Docker

```
docker exec -it gICS-2.13.0-mysql mysql -ugras_user -pgras_password  
-e "use gras;call createUser('BENUTZERNAME','PASSWORT','KOMMENTAR');"
```

in SQL

```
use gras;  
call createUser("BENUTZERNAME","PASSWORT","KOMMENTAR");
```

11.2.1.2 Rechtevergabe

Nutzer haben standardmäßig keine Berechtigungen. Die Vergabe dieser erfolgt je Werkzeug („Projekt“) unter der Angabe von *epix*, *gpas* oder *gics* (Schreibweise wie hier dargestellt).

11.2.1.2.1 Admin-Rechte vergeben

⚠ Hinweis: Admin-Rechte beinhalten die Standard-Rechte.

in Docker

```
docker exec -it gICS-2.13.0-mysql mysql -ugras_user -pgras_password  
-e "use gras;call grantAdminRights('PROJEKTNAME','BENUTZERNAME');"
```

in SQL

```
use gras;  
call grantAdminRights("gICS","BENUTZERNAME");
```

11.2.1.2.2 Standard-Rechte vergeben

in Docker

```
docker exec -it gICS-2.13.0-mysql mysql -ugras_user -pgras_password  
-e "use gras;call grantStandardRights('PROJEKTNAME','BENUTZERNAME');"
```

in SQL

```
use gras;  
call grantStandardRights("gICS","BENUTZERNAME");
```

11.2.1.3 Passwort ändern

in Docker

```
docker exec -it gICS-2.13.0-mysql mysql -ugras_user -pgras_password -e "use  
gras;call changePassword('BENUTZERNAME','NEUES_PASSWORT');"
```

in SQL

```
use gras;
```

```
call changePassword("BENUTZERNAME", "NEUES_PASSWORT");
```

11.2.1.4 Nutzer aktivieren/deaktivieren

⚠ Hinweis: Diese Änderungen werden erst nach einem Neustart des *Wildfly* übernommen.

in Docker

```
docker exec -it gICS-2.13.0-mysql mysql -ugras_user -pgras_password -e "use
gras;call disableUser('BENUTZERNAME');"
```

in SQL

```
call disableUser("BENUTZERNAME"); -- Benutzer deaktivieren
call enableUser("BENUTZERNAME"); -- Benutzer aktivieren
```

11.2.1.5 Erweiterte Rechte-Konfiguration

11.2.1.5.1 Domain anlegen

⚠ Hinweis: Die Authentifizierungsdomain ist unabhängig von den Pseudonymisierungsdomänen.

Innerhalb der gRAS-Authentifizierung wird **per Default die Parent Domain „ths“ genutzt**, um Anmeldung von Nutzern für eine ausgewählte Authentifizierungsdomain (user@domain) zu ermöglichen. Die Individualisierung der Domänen ist möglich.

SQL

```
use gras;
call createDomain('domainName', 'parent domain');
```

11.2.1.5.2 Projekt anlegen

Innerhalb der gRAS-Authentifizierung wird mit dem Projekt das abzusichernde Werkzeug (konkret hier: gICS) bezeichnet. **Per Default wird hier entsprechend das Projekt „gics“ genutzt**. Die Individualisierung des Projektnamens ist möglich.

SQL

```
use gras;
call createProject('domainName', 'parent domain');
```

11.2.1.5.3 Gruppe anlegen

Rechte werden stets nur Gruppen zugeordnet. Per Default werden für die Authentifizierung per gRAS im gICS-Frontend die Gruppen **gICS-users** und **gICS-admins** genutzt. Anpassungen und Ergänzungen sind möglich.

SQL

```
-- createGroup(<projectName>, <groupName>, <description>)
CALL createGroup('gics', 'gics-users', 'this group is for users with basic
right');
```

```
CALL createGroup('gics','gics-admins', 'this group is for users with extended right');
```

11.2.1.5.4 Rolle anlegen

Je Projekt/Werkzeug kann ein-und-derselbe Nutzer unterschiedliche Rollen einnehmen. Per Default werden für die Authentifizierung per gRAS im gICS-Frontend die Rollen **role.gics.user** und **role.gics.admin** genutzt. **Diese Rollen sind fest den jeweiligen Unterseiten des gICS-Frontends zugeordnet und können nicht geändert werden.** Das Ergänzen zusätzlicher Rollen ist möglich.

SQL

```
-- createRole(<projectName>, <roleName>, <description>)
CALL createRole('gics', 'role.gics.user', 'gICS userspace');
CALL createRole('gics', 'role.gics.admin', 'gICS adminsace');
```

11.2.1.5.5 Zuordnung von Gruppen und Rollen

Die finalen Rechte erhält jeder Nutzer durch die Zuordnung von Gruppen (sind in der gRAS-Datenbank per Default in ADMIN und USER unterteilt) und Rollen (sind im Frontend definiert und eingebettet). Das Ergänzen zusätzlicher Zuordnungen ist möglich.

SQL

```
-- createGroupRoleMapping(<projectName>, <groupName>, <roleName>)
CALL createGroupRoleMapping('gics','gICS-users','role.gics.user');
CALL createGroupRoleMapping('gics','gICS-admins','role.gics.admin');
```

12 Empfehlungen zur Absicherung des Anwendungsservers

Der Zugriff auf relevante Anwendungs- und Datenbankserver des gICS sollte nur für autorisiertes Personal und über autorisierte Endgeräte möglich sein. Wir empfehlen die Umsetzung nachfolgender IT-Sicherheitsmaßnahmen:

- Betrieb der relevanten Server in separaten Netzwerkzonen (getrennt von Forschungs- und Versorgungsnetz)
- Verwendung von Firewalls und IP-Filtern
- Zugangsbeschränkung auf URL-Ebene mit Basic Authentication (z.B. mit NGINX oder Apache)

13 Health Check

Der gICS besitzt ab Version 2.12 einen Health Check. Damit ist es möglich einen Status zum Zustand des Dienstes abzufragen. Dabei werden die Erreichbarkeit der Datenbank und der freie Arbeitsspeicher für den Dienst geprüft. Sollte dieser in einen Zustand wechseln oder dies

bevorstehen, in dem dieser nicht mehr ordnungsgemäß arbeiten kann, liefert der Health Check einen entsprechenden Status. Es ist somit möglich, automatisiert den Status abzufragen und im Fall eines unerwünschten Zustands entsprechende Meldung z.B. an einen Administrator zu geben, sodass dieser zeitnah eingreifen kann und mögliche Probleme behebt.

⚠ Hinweis: Der Health Check kann derzeit nur mit dem Wildfly 16 betrieben werden. Eine Anpassung auf spätere Wildfly Versionen erfolgt in der gICS Version 2.13.

13.1 Abfrage

Der Health Check wird über die URL des Wildfly-Servers unter dem Port 9990 aufgerufen. Bsp.:

```
http://example.org:9990/health
```

Der Wildfly-Server fragt dabei den gICS ab, welcher die entsprechenden Zustandsdaten liefert. Dies erfolgt im JSON-Format und kann demnach auch automatisiert weiterverarbeitet werden. Eine exemplarische Rückgabe ist im Folgendem zu sehen:

```
{
  "outcome": "UP",
  "checks": [
    {
      "name": "gICS Database Healthcheck",
      "state": "UP",
      "data": {
        "updated": "Mon Jan 25 19:48:51 CET 2021"
      }
    }, {
      "name": "gICS Memory Healthcheck",
      "state": "UP",
      "data": {
        "total": 6737100800,
        "maximal": 13362528256,
        "threshold": 104857600,
        "free": 5425185360,
        "updated": "Mon Jan 25 19:48:52 CET 2021"
      }
    }
  ]
}
```

Die Health Checks für den gICS sind als „gICS Database Healthcheck“ und „gICS Memory Healthcheck“ benannt. Diese beinhalten zusätzliche Informationen zum jeweiligen Health Check. Die Health Checks werden nicht bei jedem Aufruf ausgeführt, sodass ggf. der Dienst damit belastet wird, sondern die Ergebnisse werden standardmäßig 10 Sekunden gecached. Diese Zeitspanne ist konfigurierbar (siehe **Abschnitt 13.2**). Der Zeitstempel wird im Feld `updated` mitgeliefert. Beide Health Checks liefern außerdem den Status im Feld `state` zurück. Solange der Dienst ordnungsgemäß ausgeführt wird, wird der Wert `UP` geliefert. Im Fehlerfall `DOWN`. Der Health Check zur Arbeitsspeicherüberwachung liefert darüber hinaus noch den belegten Speicher der Java Virtual Maschine (JVM) (`total`), den maximal der JVM verfügbaren Speicher (`maximal`), den noch freien Speicher (`free`) und den

konfigurierbaren Schwellwert (`threshold`), ab wann der Dienst in den Status `DOWN` wechseln soll (standardmäßig 100 MB). Letzteres dient als Schutzmaßnahme, damit der Dienst zwar grundsätzlich ordnungsgemäß funktioniert, jedoch bevor ein endgültiges volllaufen des Speichers erreicht ist, Gegenmaßnahmen getroffen werden können.

13.2 Konfiguration

Die Konfiguration der Health Checks erfolgt in der Datei `healthcheck-gics.xml`. Diese liegt im Servlet des Backends (`*.ear`).

⚠ Hinweis: Die direkte Bearbeitung der Datei innerhalb des Servlets zur Laufzeit ist nicht zu empfehlen und führt zu einem Neustart des Dienstes. Es wird empfohlen den Dienst für eine Änderung herunterzufahren. Optimalerweise genügt eine einmalige Konfiguration vor dem ersten Hochfahren.

Standardmäßig beinhaltet die Konfigurationsdatei folgenden Inhalt:

```
<ma:HealthCheckConfiguration
  xmlns:ma=http://www.ttp.icmvc.emau.org/gics/healthcheck/model
  xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
  xsi:schemaLocation="http://www.ttp.icmvc.emau.org/gics/healthcheck/model
healthcheck-config-1.0.0.xsd">
  <service-name>gICS</service-name>
  <database-configuration>
    <persistence-unit-name>gics</persistence-unit-name>
    <update-time>10</update-time>
  </database-configuration>
  <memory-configuration>
    <available-memory-threshold>104857600</available-memory-threshold>
    <update-time>10</update-time>
  </memory-configuration>
</ma:HealthCheckConfiguration>
```

Mit dem Feld `service-name` kann ein frei wählbarer Name vergeben werden. Dieser wird lediglich vor die konkrete Bezeichnung des Health Checks gelegt. Das Feld `persistence-unit-name` gibt den internen Namen für die Datenbank an. Eine Änderung ist nicht zu empfehlen. Die Zeitspanne des Caches für den Health Check Zustand, wird mit dem Feld `update-time` in Sekunden angegeben. Um den Schwellwert für den Health Check zur Speicherüberwachung anzugeben, wird das Feld `available-memory-threshold` in Byte verwendet. Standardmäßig sind hier 100 MB definiert. Bei Unterschreitung dieses Schwellwerts wird nur der Status des Health Checks auf `DOWN` gelegt. Der Dienst funktioniert ordnungsgemäß weiter, bis der Speicher komplett belegt ist.

14 Upgrade

Mit dem Upgrade auf die gICS Version 2.12 wird der Qualitätsstatus zu jedem Dokument eingeführt (Details siehe **Kapitel 8**). Bei einem Upgrade kann für bestehende Domänen ein Qualitätsstatus gesetzt werden, der nach dem Upgrade jedem vorhandenen Dokument zugeordnet wird.

Standardmäßig wird der Wert `###_auto_generated_###` gesetzt. In der Oberfläche werden damit alle Dokumente mit dem Qualitätsstatus *Automatisch* dargestellt. Eine nachträgliche manuelle Anpassung des Status ist möglich.

Soll ein anderer Status standardmäßig hinterlegt werden, so kann dies im Datenbank-Update-Skript erfolgen (`update_database_gics_2.11.x-2.12.0.sql`). Dabei wird die erste Zeile angepasst.

```
SET @default_qs_state := '###_auto_generated_###';
```

Der Wert von `default_qs_state` kann dabei einer der folgenden Werte annehmen:

Tabelle 14-1: Qualitätsstatus die bei einem Upgrade gesetzt werden können.

Qualitätsstatus	Beschreibung
<code>###_auto_generated_###</code>	Der Status wird auf „Automatisch“ gesetzt. Das Dokument gilt damit als gültig.
<code>not_checked</code>	Der Status wird auf „Nicht geprüft“ gesetzt. Im Fall eines Upgrades ist das Dokument damit gültig. Bei einer neuen Domäne kann konfiguriert werden, ob ein ungeprüftes Dokument gültig oder ungültig ist (siehe Kapitel 8).

15 Nutzung der Soap-Schnittstelle

Neben der grafischen Benutzerschnittstelle, steht eine maschinenverständliche Web-Schnittstelle zur Verfügung. Diese kann mit dem SOAP-Protokoll angesprochen werden. Beim laufenden Dienst kann die Definition der SOAP-Schnittstelle mit dem folgenden Pfad, an der jeweiligen URL, abgerufen werden.

```
http://example.org:8080/gics/gicsService?wsdl
```

Die neuste Entwicklerdokumentation ist unter der folgenden URL zu finden.

```
https://www.ths-greifswald.de/gics/doc
```

Im Folgendem wird das Abrufen von Einwilligungsinformationen exemplarisch vorgestellt. Hierbei findet eine Unterteilung in dem Abrufen der Consent Informationen und dem Abrufen eines Consent Policy Status statt.

15.1 Abruf von Consent Informationen

Das Abrufen der Einwilligungsinformationen erfordert die Angabe des Erfassungsdatums, der Domäne in der sich die entsprechenden Einwilligungen, Widerrufe oder Verweigerungen befinden,

der Name der jeweiligen Einwilligung, die Version und die Signer-ID und der Typ der Signer-ID. In **Abbildung 15-1** wird eine Anfrage per SOAP-Protokoll exemplarisch dargestellt.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cm2="http://cm2.ttp.ganimed.icmvc.emau.org/">
  <soapenv:Header/>

  <soapenv:Body>
    <cm2:getConsent>
      <consentKey>
        <!--exact date of consent-->
        <consentDate>2019-01-29T11:53:45.429Z</consentDate>
        <!--specific consent template key-->
        <consentTemplateKey>
          <domainName>PROJECTNAME</domainName>
          <name>t_project_basic_consent</name>
          <version>1.5.0</version>
        </consentTemplateKey>
        <!--1-n signerIDs-->
        <signerIds>
          <id>UNIQUE_PSEUDONYM_OF_PATIENT</id>
          <idType>studyPSN</idType>
        </signerIds>
      </consentKey>
    </cm2:getConsent>
  </soapenv:Body>
</soapenv:Envelope>
```

Abbildung 15-1: XML-Repräsentation einer beispielhaften Anfrage von Einwilligungsinformationen über die SOAP-Schnittstelle des gICS.

Ein Auszug aus der entsprechenden Antwort auf die gezeigte Anfrage ist in **Abbildung 15-2** dargestellt. Darin enthalten sind die jeweiligen Module und Policies mit den Einwilligungsstatus (vgl. **Tabelle 2-1**).

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><ns2:getConsentResponse
  <return>
    <key>
      <consentDate>2019-01-29T11:53:45.429Z</consentDate>
      <consentTemplateKey>
        <domainName>PROJECTNAME</domainName>
        <name>t_project_basic_consent</name>
        <version>1.5.0</version>
      </consentTemplateKey>
      <signerIds>
        <id>UNIQUE_PSEUDONYM_OF_PATIENT</id>
        <idType>studyPSN</idType>
      </signerIds>
    </key>
    <moduleStates>
      <entry>
        <key>
          <domainName>PROJECTNAME</domainName>
          <name>m_storage_and_analysis</name>
          <version>1.2.1</version>
        </key>
        <value>
          <consentState>ACCEPTED</consentState>
          <key>
            <domainName>PROJECTNAME</domainName>
            <name>m_storage_and_analysis</name>
            <version>1.2.1</version>
          </key>
          <policyKeys>
            <domainName>PROJECTNAME</domainName>
            <name>p_type_and_duration_of_use</name>
            <version>1.0.0</version>
          </policyKeys>
          [...]
        </value>
      </entry>
      [...]
    </moduleStates>
    <patientSignatureIsFromGuardian>false</patientSignatureIsFromGuardian>
    <patientSigningDate>2018-07-26T00:00:00Z</patientSigningDate>
    <physicanId>AID_12344</physicanId>
    <physicanSigningDate>2018-07-25T00:00:00Z</physicanSigningDate>
    <scanFileType>application/pdf</scanFileType>
    [...]
    <scanBase64><!-- base 64 encoded pdf string--></scanBase64>
  </return>
</ns2:getConsentResponse>

```

Abbildung 15-2: XML-Repräsentation einer beispielhaften Einwilligung (in Auszügen) nach Abruf über die SOAP-Schnittstelle des GICS.

15.2 Abruf eines Consent Policy Status

Der Status einer jeden Consent Policy kann einzeln abgefragt werden. Hierbei kann abgefragt werden, ob ein bestimmter Patient zu einer bestimmten Policy eingewilligt hat. Hierzu wird die Signer-ID und dessen Typ benötigt, die Domäne und der Name und die Version der abgefragten Policy. Außerdem besteht die Möglichkeit bei der Abfrage die Versionsnummer zu ignorieren, den Status der Policy bei der Auswahl „Unknown“ als „Decline“ zu werten und den Matching-Typ. Zu jedem Consent können mehrere Signer-IDs gesetzt worden sein, sodass mithilfe des Matching-Typs angegeben wird, mit welchen und wie vielen Signer-IDs nach einer bestimmten Policy gesucht wird.

Der `idMatchingType`⁹ kann dabei die Werte `AT_LEAST_ONE`, `AT_LEAST_ALL`, `EXACT` annehmen. In **Tabelle 15-1** sind die entsprechenden Werte näher erläutert.

Tabelle 15-1: `idMatchingTypes`

<code>idMatchingType</code>	Bedeutung
<code>AT_LEAST_ONE</code>	Zumindest eine der angegebenen Signer-IDs muss der Policy zugeordnet sein.
<code>AT_LEAST_ALL</code>	Zumindest die angegebenen Signer-IDs müssen der Policy zugeordnet sein.
<code>EXACT</code>	Exakt die angegebenen Signer-IDs müssen der Policy zugeordnet sein.

In **Abbildung 15-3** wird exemplarisch eine Anfrage dargestellt.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cm2="http://cm2.ttp.ganimed.icmvc.emau.org/"
  <soapenv:Header/>
  <soapenv:Body>
    <cm2:isConsented>
      <!--1 or more signerids possible:-->
      <signerIds>
        <!--1-n: e.g. studyPSN:-->
        <id>UNIQUE_PSEUDONYM_OF_PATIENT</id>
        <idType>studyPSN</idType>
      </signerIds>
      <!-- example for single policy request -->
      <policyKey>
        <domainName>PROJECTNAME</domainName>
        <name>p_storage_and_use_of_data</name>
        <version>1.0.0</version>
      </policyKey>
      <config>
        <!--matching multiple signerIds: AT_LEAST_ONE, AT_LEAST_ALL, EXACT;-->
        <idMatchingType>AT_LEAST_ONE</idMatchingType>
        <ignoreVersionNumber>FALSE</ignoreVersionNumber>
        <unknownStateIsConsideredAsDecline>FALSE</unknownStateIsConsideredAsDecline>
      </config>
    </cm2:isConsented>
  </soapenv:Body>
</soapenv:Envelope>
```

Abbildung 15-3: XML-Repräsentation einer beispielhaften Anfrage „Hat Patient ABC in die Policy XYZ eingewilligt?“ zur Ermittlung des Status einer Consent Policy für eine ausgewählte Signer-ID (z.B. ein Studien-Pseudonym) über die SOAP-Schnittstelle des gICS.

In **Abbildung 15-4** wird die daraus resultierende Antwort auf die Anfrage dargestellt. Auf die Frage, ob eine Einwilligung für die entsprechende Policy vorliegt, würde hier beispielsweise mit „*Nein*“ beantwortet werden.

⁹ <https://www.ths-greifswald.de/gics/doc>

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:isConsentedResponse xmlns:ns2="http://cm2.ttp.ganimed.icmvc.emau.org/">
      <return>false</return>
    </ns2:isConsentedResponse>
  </soap:Body>
</soap:Envelope>
```

Abbildung 15-4: XML-Repräsentation einer Antwort auf die Anfrage „Hat Patient ABC in die Policy XYZ eingewilligt?“ über die SOAP-Schnittstelle des gICS.

Ist diese Information nicht ausreichend, kann ergänzend die Art des Status mit Hilfe der Funktion `getConsentStatusType` abgefragt werden. Der Inhalt der Anfrage ist identisch (vgl. **Abbildung 15-3**), liefert jedoch exakte Werte (vgl. **Tabelle 2-1**) zurück (z.B. *ACCEPTED*, *DECLINED*, *WITHDRAWN*, etc.).

Die Schnittstellenfunktion `getPolicyStatesForPolicyNameAndSigner` liefert unter Angabe eines Policy-Names und einer Patientenkenung (Signer-ID) alle bekannten und konsentierten Versionen dieser Policy zurück, für die der Patient jemals eingewilligt hat. Auch ist jeweils der konkrete Einwilligungstatus in der Antwort enthalten.

16 Publikationen und Vorträge

Rau, H., Geidel, L., Bialke, M., Blumentritt, A., Langanke, M., Liedtke, W., Pasewald, S., Stahl, D., Bahls, T., Maier, C., Prokosch, HU. & Hoffmann, W.

The generic Informed Consent Service gICS®: implementation and benefits of a modular consent software tool to master the challenge of electronic consent management in research.

(Originalartikel)

Journal of Translational Medicine 18, 287 (2020). <https://doi.org/10.1186/s12967-020-02457-y>

Martin Bialke*; Thomas Bahls*; Lars Geidel; Henriette Rau; Arne Blumentritt; Sandra Pasewald; Robert Wolff; Jonas Steinmann; Tobias Bronsch; Björn Bergh; Galina Tremper; Martin Lablans; Frank Ückert; Stefan Lang; Tarik Idris; Wolfgang Hoffmann

MAGIC: ONCE UPON A TIME IN CONSENT MANAGEMENT - A FHIR TALE.

Journal of Translational Medicine, 2018 Sep 14; 16(1):256,

DOI :10.1186/s12967-018-1631-3. Link: <https://rdcu.be/6LJd>

Bialke M*, Bahls T, Havemann C, Piegsa J, Weitmann K, Wegner T, et al.

MOSAIC. A modular approach to data management in epidemiological studies. (Originalartikel)

METHODS OF INFORMATION IN MEDICINE. 2015; 54(4):364-371.

<http://dx.doi.org/10.3414/ME14-01-0133>

Bialke M*, Penndorf P, Wegner T, Bahls T, Havemann C, Piegsa J, et al.

A workflow-driven approach to integrate generic software modules in a Trusted Third Party

(Originalartikel)

Journal of Translational Medicine. 2015; 13(176).

<http://www.translational-medicine.com/content/13/1/176>

Bialke M, Geidel L, Wolff R, Lablans M, Tremper G, Drepper J, et al.

MAGIC – Ein Grund zum FHIRn? Der Brückenschlag zwischen inhaltlicher Erstellung und digitaler Verarbeitung von modularen Einwilligungen (Vortrag)

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie. 62. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS); 2017 Sep 20; Oldenburg.

<http://dx.doi.org/10.3205/17gmids146>

Bahls T, Liedtke W, Geidel L, Langanke M.

Ethics Meets IT: Aspects and elements of Computer-based informed consent processing.

In Fischer T, Langanke M, Marschall P, et al., editors. Individualized medicine, ethical, economical and historical perspectives.: Springer; 2015. p. 209-229.

Geidel L, Bahls T, Hoffmann W.

Darf ich? – Herausforderungen an eine generische, automatisierte elektronische Verwaltung von Einwilligungen.

In GMDS 2014. 59. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS).; 2014; Göttingen, 07.-10.09.2014.

doi: 10.3205/14gmids131

17 Weiterführende Informationen

Produktseite gICS

<https://www.ths-greifswald.de/gics>

TTP FHIR Gateway für gICS

<https://simplifier.net/guide/ttp-fhir-gateway-ig/Einwilligungsmanagement>

Art-Decor ValueSets der MII Task Force Consent Umsetzung

<http://art-decor.org/decor/services/RetrieveValueSet?id=2.16.840.1.113883.3.1937.777.24.11.36&effectiveDate=2021-04-23T10:55:54&prefix=mide-&format=html&collapsible=true&language=de-DE&ui=en-US>

FHIR Implementation Guide der Arbeitsgruppe Einwilligungsmanagement des Interoperabilitätsforums des BVITG

<https://ig.fhir.de/einwilligungsmanagement/stable/>

Docker Installation

<https://docs.docker.com/install/>

Docker Compose Installation

<https://docs.docker.com/compose/install/>

Docker Cheat Sheet

https://www.docker.com/sites/default/files/Docker_CheatSheet_08.09.2016_0.pdf

Docker und Docker Compose Cheat Sheet

<https://dev-eole.ac-dijon.fr/doc/cheatsheets/docker.html>