# Short Public Report

# Recertification No. 3

## 1. Name and version of the IT-based service:

Haemoassist® 2 2021

## 2. Manufacturer / Provider of the IT-based service:

**Company Name:**

Statconsult Gesellschaft für klinische und Versorgungsforschung mbH

**Address:**

Am Fuchsberg 11, 39112 Magdeburg

**Contact Person:**

Jan Reichmann

## 3. Time frame of evaluation:

*April 2021 – August 2022*

## 4. EuroPriSe Experts who evaluated the IT-based service:

**Name of the Legal Expert:**

Jörg Schließke

**Address of the Legal Expert:**

TÜV Informationstechnik GmbH (TÜV Nord Group)

Am TÜV 1

45307 Essen

**Name of the Technical Expert:**

Tobias Mielke

**Address of the Technical Expert:**

TÜV Informationstechnik GmbH (TÜV Nord Group)

Am TÜV 1

45307 Essen

## 5. Certification Authority:

Name: EuroPriSe Certification Authority
Address: Joseph-Schumpeter-Allee 25
53227 Bonn
Germany
eMail: contact@euprivacyseal.com

## 6. Specification of Target of Evaluation (ToE):

Haemoassist® is a smartphone and web-based therapy management tool for patients with haemophilia. The patient app and the corresponding website with access for the attending physician make it possible to easily and conveniently document the treatment with clotting factor preparations (substitution therapy) as required by the Transfusion Law. The physician in charge can access the documented data promptly and easily via a web portal, monitor the success of the therapy and adjust it if necessary.

Haemoassist® enables prompt and efficient information and evaluation of events that have occurred (e.g. by using the integrated messenger). Clear graphics show, among other things, bleeding, factor administration and patient stocks. The regularity of factor administration in prophylaxis patients or accumulations of bleeding in target joints can be recognised at a glance. Evaluation functions and automatic notification functions enable the physician to promptly recognise trends in bleeding events and to react to unusual events.

The pharmacy module supports pharmacies in the implementation of the documentation and reporting obligation according to ApBetrO[1] § 17 para. 6a. medicine expenditure by the pharmacy is also stored directly in the Haemoassist® database.

The target of evaluation (ToE) covers the following components

- Provision of the electronic patient diary as well as the doctor portal. This includes all functions and all generated network traffic resulting from the use of the provided functions (e.g. also the new functions notes from patient and the delivery process for medicines)
- the User Login process
- All IT systems (servers, network components, storage) and software (operating systems, databases, application software, web interfaces) necessary to provide the electronic patient diary and the browser-based portal. Operating systems and databases themselves are not certified, but only the information processing necessary for the provision of the IT-based service using these components
- Contractual regulations of StatConsult Gesellschaft für klinische und Versorgungsforschung mbH

[1] Ordinance on the Operation of Pharmacies (Apothekenbetriebsordnung – ApBetrO)

    - with clinics and doctors,
    - subcontractors and third parties
    - Pharmacies
- Data processing in the pharmacy module (storage and transmission) with regard to the GSAV[2] -reports according to § 17 para. 6a ApBetrO
- Encryption of patient data in the pharmacy module
- Personal data processing in Messenger
- Configuration of the Messenger Server
- Encryption of messages in Messenger

**The following components are excluded from the Target of Evaluation**:

- Neither the IT systems (clients) used by doctors nor the smartphones used by patients to access the Haemoassist® service are included in the assessment. This definition includes both the hardware and the operating systems of the aforementioned computing devices.
- Neither networks or active network components nor other IT systems that serve to transmit or process data are included in the evaluation.
- Data entry for the transmission of reports according to § 21 TFG[3] to the DHR[4] within the framework of the DHR Client 2.0 WebModule (interface)
- Encryption of patient data in the DHR Client 2.0 WebModule
- Patient consent form for admission to the DHR

## 7. General description of the IT product or IT-based service:

Haemophilia is a hereditary disease that inhibits blood clotting. Its symptoms are treated by administering the coagulant either preventively or as needed. In the context

---

[2] Gesetz für mehr Sicherheit in der Arzneimittelversorgung

[3] Transfusion Law - Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz - TFG)

[4] German Haemophilia Register - Deutsches Hämophilieregister (DHR)

of independent home care with minimal medical supervision, the administration of the coagulant is carried out by the patients themselves

Haemoassist® is a smartphone-based therapy management application for haemophilia patients and their doctors. It consists of an electronic patient diary (application) in combination with a web-based monitoring interface for the treating physicians. The Haemoassist® is also available to patients via web access. In addition, a pharmacy module is available

Section 14 TFG requires immediate and detailed documentation of the treatment by the attending physician, including relevant patient information, detailed batch and product information, and time of administration

The following functions are provided for doctors and patients as well as pharmacies:

- Medication reminder function
- Calculation of the factor level
- Calendar views on medication, bleeding and treatment adherence
- Messenger

The electronic patient diary offers the following functions to the patient:

- Documentation of preventive and needs-based administration (factor replacement)
- Barcode reader functionality for fast scanning of coded batch information
- Documentation of the bleedings as well as the origin of the individual bleedings
- Possibility of photo documentation of bleeding with the built-in ability to send images directly to the attending physician

- Inventory tracker for factor preparations in stock with corresponding warning if a minimum stock level is not reached or due dates are exceeded.
- Various ways of contacting the doctor directly by e-mail, Short Message Service (SMS), Multimedia Messaging Service (MMS) or telephone call.

The doctor's web application serves the following functions:

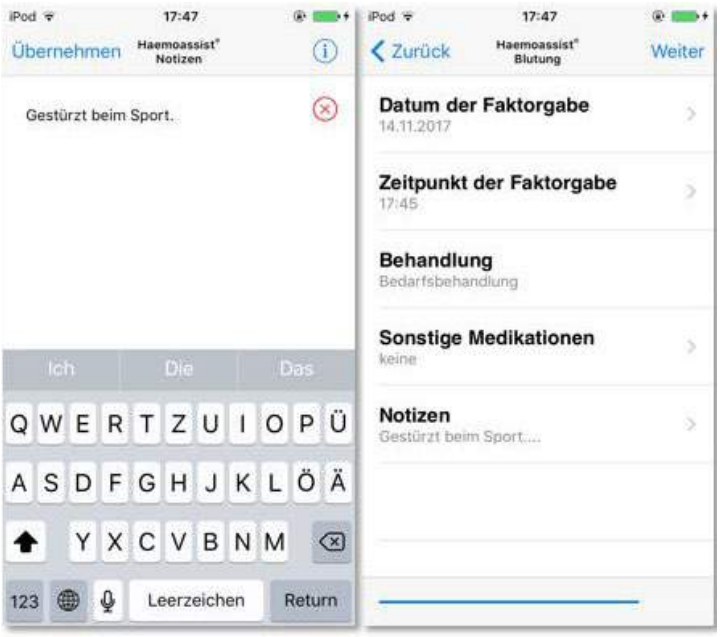
- Simple overview of the collected patient data
- Search for individual patient data or filter data for all patients based on predefined supplementation batches
- Graphical display of patient data for easy interpretation via cockpit diagrams, graphical analysis and various filter functions.
- Emails and alerts about possible serious adverse events (SAEs) and events that may require a change in therapy.
- Alarms about unusual bleeding
- Therapy monitoring

The IT-based service Haemoassist® uses only pseudonymised data for the patient diary: The patient's name is not stored in the service's database, but is only known to the patient and his personal doctor. The patient himself could only reveal the identity of the patient in the database of StatConsult IT-Service GmbH by uploading an identifiable picture or personal notes by himself or by his doctor, who - theoretically - could use the free text field to note the name of the patient.

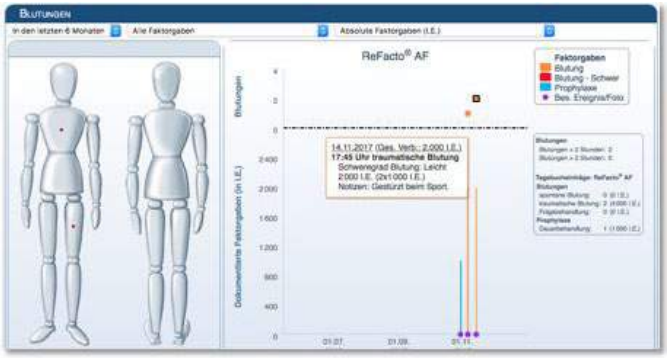
In order for the pharmacy module to be used to document the dispensing of haemophilia medication and to report this dispensing to the prescribing doctor or the haemophilia centre, a consent must be given by the patient for the processing of personal medication data. The data from the pharmacy module are not pseudonymised.

The patient or user has the possibility to collect some notes on factor supplements and bleeding in the application. He can comment on bleedings or unplanned factor supplements to discuss them with his doctor. The notes are stored in encrypted form and only the doctor has access to these notes. The notes are visualized in the individual patient and calendar view.

**Notes by the patient:**




**View for the doctor:**

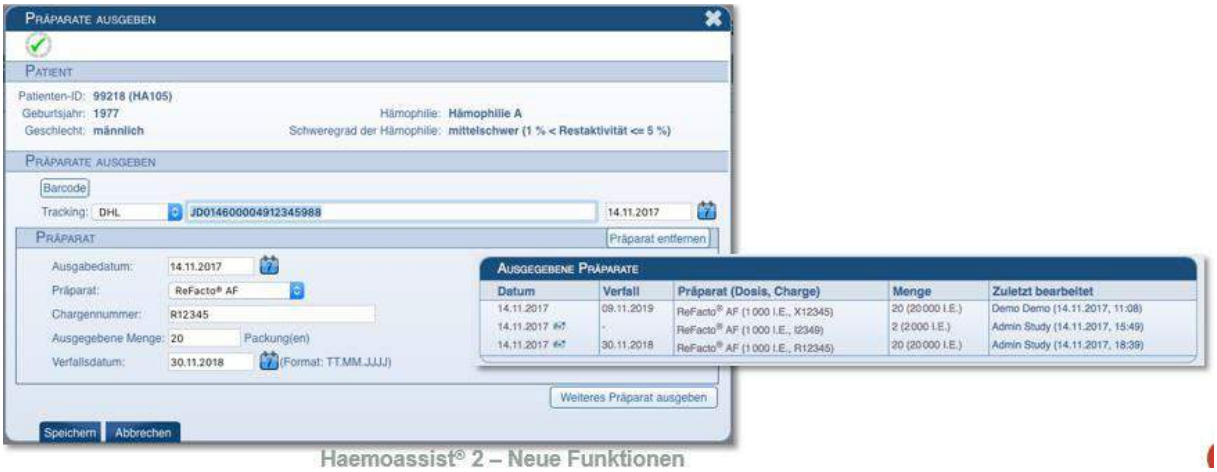



The patient is informed by the application before the first use of the function for creating notes that the physician can also view these. This information button can always be called up..

**Workflow in the context of dispensing medicines**

The doctor has the option of documenting the tracking number of the package sender in the medication dispensing application.

The patient is informed about a new medication shipment. A hyperlink to the package sender is available to view the shipment notification. He also has the possibility to view the medication shipments of the last 30 days.




Haemoassist® 2 – Neue Funktionen

The purpose of the IT-based service Haemoassist® is to provide online documentation for haemophiliacs and their doctors. No other purposes can be pursued with Haemoassist®. The pseudonymised data of the patient diary are only made accessible to the IT staff of StatConsult IT-Service GmbH. Only the patient's doctor is able to link the patient identifier stored in the StatConsult IT-Service GmbH database with the patient's name. The documentation of this remains exclusively with the doctor.

With the pharmacy module, pharmacies release medicines for the patient. In addition to reporting to the pharmacies, the released medicines are also stored in the Haemoassist® warehouse management. The pharmacies are direct contractual partners of Haemoassist® and are managed in Haemoassist®.

The data from the pharmacy and the HZ are stored separately. The data recorded in the pharmacy belong to the pharmacies and the data transmitted / recorded in the haemophilia centre belong to the haemophilia centre.

With the help of a messenger function, ad-hoc messages and image transmissions from the patient to the medical team and haemophilia centre. in Haemoassist® are to be made possible. Furthermore, the function can be used to send bleeding images to the centre without creating a diary entry. Based on these images, support can be provided by the haemophilia centre. in making therapy decisions.

## 8. Transnational issues:

The Haemoassist® 2 application is restricted to EU member states and the data is stored on IT servers located in Germany.

## 9. Tools used by the manufacturer of the IT product / provider of the IT-based service:

The aim of the Haemoassist® 2 application is to provide online documentation for haemophilia patients and their doctors. The provider uses tools to deliver the IT-based services. These tools are necessary for the provision of the electronic patient diary and the web(browser)-based application portal (server, network components, storage) for patients and physicians as well as the necessary software (operating systems, databases, application software, web interfaces). The operating systems and databases themselves are not certified, but only the information processing required to provide the IT-based service using these components.

## 10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria from January 2017

EuroPriSe Commentary from May 2017

## 11. Modifications / Amendments of the IT product or IT-based service since the last (re)certification

**Pharmacy module**

With the pharmacy module, pharmacies release medicines for the patient. In addition to reporting to the pharmacies, the released medicines are also stored in the Haemoassist® warehouse management. The pharmacies are direct contractual partners of Haemoassist® and are managed in Haemoassist®.

The data from the pharmacy and the haemophilia centre (HC) are stored separately. The data recorded in the pharmacy belong to the pharmacies and the data transmitted / recorded in the HC belong to the HC.

**Messenger in Haemoassist®**

With the help of a messenger function, ad-hoc messages and image transmissions from the patient to the medical team and HC in Haemoassist® are to be made possible. Furthermore, the function can be used to send bleeding images to the centre without creating a diary entry. Based on these images, support can be provided by the HC in making therapy decisions.

## 12. Changes in the legal and/or technical situation

Currently, there are no legal or technical changes that would affect the results of the evaluation of the test object compared to the re-evaluation in 2019. The Federal Data Protection Act, the Transfusion Law (TFG), Section 203 of the German Criminal Code and the Ordinance on the Operation of Pharmacies (ApBetrO) were also taken into account to the evaluation.

## 13. Re-Evaluation methods:

A workshop, interviews, a document review and a web and mobile test as well as scans were conducted. The following technical reviews were carried out as part of technical evaluation:

- Testing against the frontend and backend of the mobile and web-based applications
- The following example of methods were used for this purpose:
    - Web Application OWASP testing guide (Web and API Top 10)
    - OWASP Top 10 Privacy Risks
    - mobile applications OWASP Mobile Top 10 (based on some aspects from OWASP Mobile Security Testing Guide)
    - Configuration analysis of systems (including patch management, EOL, etc.)

## 14.- Re-Evaluation results:

The evaluation of Haemoassist® focused on the following components:

- Provision of the electronic patient diary as well as the doctor portal. This includes all functions and all generated network traffic resulting from the use of the provided functions (e.g. also the new functions notes from the patient and the delivery process for medicines).

- The user login process.
- All IT systems (servers, network components, storage) and software (operating systems, databases, application software, web interfaces) necessary to provide the electronic patient diary and the browser-based application portal. Operating systems and databases themselves are not certified, but only the information processing necessary for the provision of the IT-based service using these components.
- Contractual arrangements of StatConsult Gesellschaft für klinische und Versorgungsforschung mbH with hospitals and physicians, subcontractors and third parties, pharmacies
- Data processing in the pharmacy module (storage and transmission) with regard to the GSAV reports according to § 17 para. 6a ApBetrO
- Sample declaration of consent of patients participating in the pharmacy link for the exchange of data between HZ and pharmacy
- Encryption of patient data in the pharmacy module
- Personal data processing in Messenger
- Configuration of the Messenger Server
- Encryption of messages in Messenger

Haemoassist® is a smartphone-based therapy management application for the disease haemophilia. It consists of an electronic patient diary (application) in combination with a web-based monitoring interface for the treating physicians.

Among other things, health data of haemophiliacs are processed here. This health data is collected from patients via the Haemoassist® app or via their doctor, who can add further information to the patient's diary in the StatConsult database, e.g. by using pre-configured fields to document additions.

Every patient automatically receives a starter kit from their doctor detailing the Haemoassist® service before downloading and using the Haemoassist® app. These package contains:

1.Guide for patients

2.Haemoassist® "First Steps

3.Patient consent forms

4.Haemoassist® - Guidance Patient Web Portal

5.Patient information sheet

6.Security instructions for patients

The "starter kit" is easily accessible for patients; updates are delivered via the patients' doctors. The brochure is only available in German, but can be provided in other languages upon request to the responsible person. No special knowledge is required to understand the description of the Haemoassist® service. The source code is only accessible to the IT staff of StatConsult IT-Service GmbH..

Patients can upload a picture of bleeding. These images provide information about the patient's state of health, so they are to be classified as health data. Due to the fact that photographs may represent a whole face, they are only to be considered as a special category of personal data if they are processed by special technical means that allow the unique identification or authentication of a natural person. StatConsult IT-Service GmbH does not use any special technical means, such as facial recognition systems, so that the images uploaded to Haemoassist® do not constitute biometric data.

Overall, the information on the medicines to be taken by the patient, the batch name and the quantity of the medicine can also provide information on the state of health.

The notes function allows patients to record notes that may contain health information. This also applies to information sent via the integrated messenger.

The design of Haemoassist® complies with data protection principles and security of processing requirements.

The data processing takes place in Haemoassist® as well as within the framework of the pharmacy module of Haemoassist®, on the basis of the patient's consent. The examination of the lawfulness of the data processing taking place within the framework of Haemoassist® and within the framework of the pharmacy module has shown that the data processing is to be recognised as permissible. StatConsult provides its users with numerous information sheets as

samples, which inform about the use and functions of Haemoassist® in a detailed and comprehensible manner.

Personal data is only processed in the Haemoassist® application for specified purposes. Further processing for other purposes does not take place.

A patient can only enter data that are necessary for the documentation of his/her illness and its course. Personal data processed with the help of the pharmacy module are only used for the purpose of tracing dispensed blood preparations in accordance with § 17 para. 6a ApoBetrO within the legally permissible scope.

All patient-identifying data is stored encrypted in such a way that only users of the respective responsible parties (haemophilia centre, pharmacy) can decrypt and read this data. In addition to encryption, all patient-identifying data is stored on a separate server, physically separated from the Haemoassist® database.

The accuracy, completeness and timeliness of personal data in the Haemoassist® service is ensured by the following measures:

a) The patient himself decides on the upload of his personal data via the Haemoassist® app.

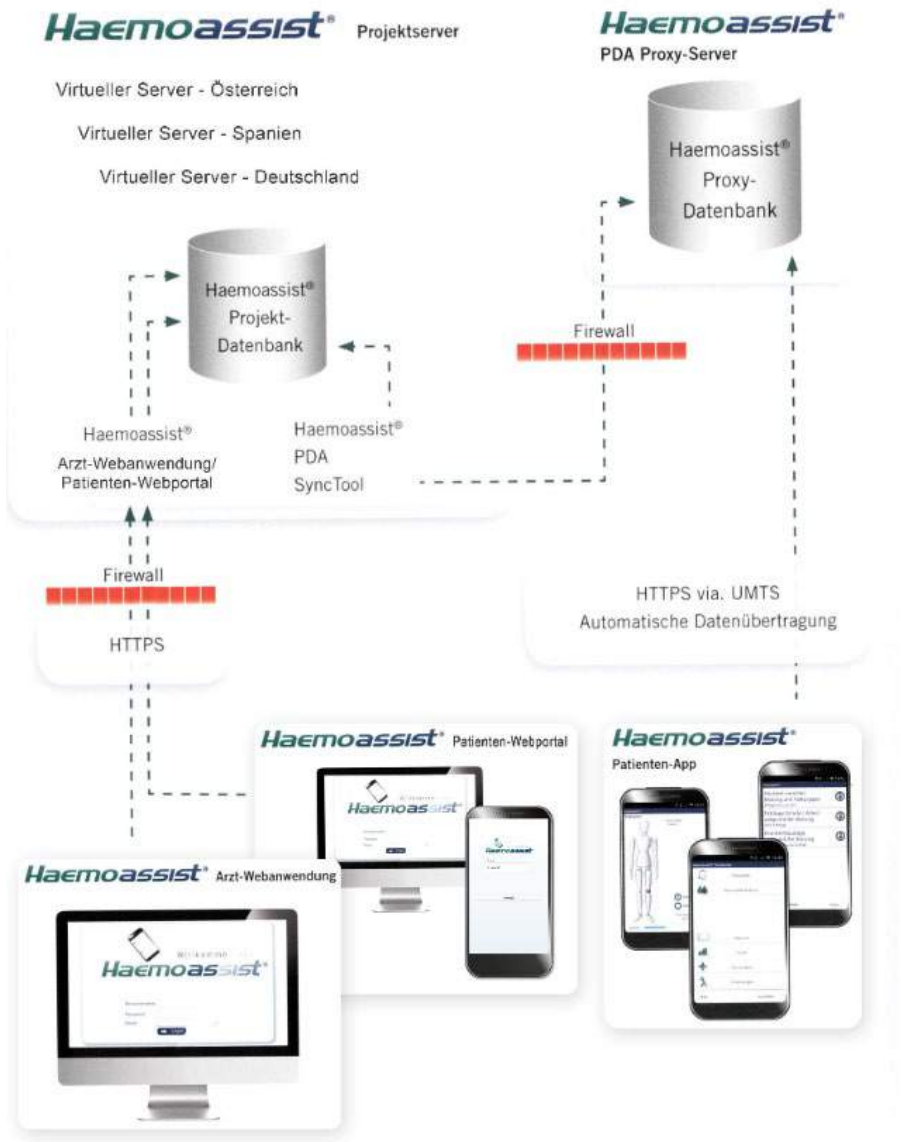
b) The patient's doctor can add, change or delete further information via the Haemoassist® web interface.

c) StatConsult IT-Service GmbH has defined a change, development and test process for software updates and new releases. Updates/releases must be released by the managing director. A tool (Polarion) is used for documentation.

d) The patient's doctor informs the StatConsult IT service if data are not correct, complete or up-to-date. This leads to a processing case in Incident Management (1st Level Support). The managing director decides on concrete measures (2nd level support).

## 15. Data flow:

The following illustrations show the use of the Haemoassist® applications and the interfaces to the pharmacy module (*only in German*)


Haemoassist® Projektserver
Virtueller Server - Österreich
Virtueller Server - Spanien
Virtueller Server - Deutschland
Haemoassist® Projekt-Datenbank
Haemoassist®
Arzt-Webanwendung/
Patienten-Webportal
Haemoassist®
PDA
SyncTool
Haemoassist®
PDA Proxy-Server
Haemoassist® Proxy-Datenbank
Firewall
Firewall
HTTPS
HTTPS via. UMTS
Automatische Datenübertragung
Haemoassist® Patienten-Webportal
Haemoassist®
Patienten-App
Haemoassist® Arzt-Webanwendung

1
Vertragliche Schnittstelle
beauftragt mit der Erbringung des Haemo Assist Service, dem Betrieb der notwendigen Server und der Entwicklung der Anwendungssoftware

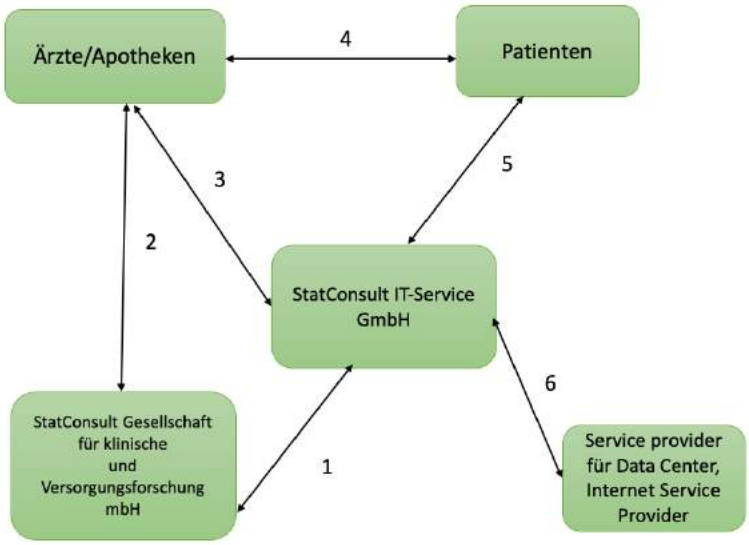
2
Vertragliche Schnittstelle
AV Vertrag Haemoassist

3
Physische Schnittstelle
Telefonschnittstelle: Verifizierung von Patientapplikationen, Elektronische Schnittstelle via Webapplikation (Austausch von Benutzerdaten (https))
E-Mail: StatConsult informiert Arzt per E-Mail zum Anlegen eines neuen Patientendatensatzes in WebApp

4
Physischer Kontakt Arzt
Behandlung, Unterzeichnung der Haemoassist-Einverständniserklärung und Erhalt der Haemoassist-Informationsbroschüre mit individuellem Aktivierungscode. Elektronischer Kontakt per Anwendung (E-Mail, SMS, MMS, Telefonanruf, Haemoassist Messenger)
Physischer Kontakt Apotheke
Ausgabe von Medikamenten gegen Rezept

5
elektronischer Kontakt per Smartphone: Download der Software Haemoassist und freiwillige Installationshilfe per Telefon
Austausch von Aktivierungscodes

6
Vertragliche Schnittstelle
vertragliche Leistungen: Erbringung von Dienstleistungen wie Internet, Service Providing, Serverhosting, etc.




Die nachfolgenden Abbildungen stellen den Datenfluss zum Verarbeitungsprozess der StatConsult IT-Service GmbH dar:

**No. 1:**

The doctor concludes a contract with StatConsult Gesellschaft für klinische Versorgungsforschung mbH and configures the web application.

**No. 2:**

The doctor receives a doctor's folder and further information brochures / starter boxes for patients from Statconsult.

**No. 3:**

The patient signs a consent form with the doctor (the form remains with the doctor).

**No. 4:**

The doctor documents the patient ID and name on the doctor's folder and sticks an individual activation code on the patient's starter box. The doctor also generates TAN lists.

**No. 5:**

The patient receives the information leaflets/starter box from the doctor.

**No. 6:**

The patient downloads the Haemoassist® application directly from the StatConsult IT service (standard username and password or via the QR code from the information brochure) to the smartphone.

**No. 7:**

The patient enters the individual activation code from the starter box to activate the application

**No. 8:**

An e-mail is automatically generated to StatConsult with an automatically generated device ID and activation code.

**No. 9:**

StatConsult recognises which activation code has been used and connects the device to the doctor. StatConsult informs the doctor by email to create a new record of a patient in the WebApp and to connect the device to the patient's record.

**No. 10**:

StatConsult activates the app for the corresponding patient

## 16. Privacy-enhancing functionalities:

The IT-based service Haemoassist® uses pseudonymised data, except in the pharmacy module: The patient's name is not stored in the service's database, but is only known to the patient and his personal doctor. The patient himself could only reveal the identity of the patient in the StatConsult IT-Service GmbH database by uploading an identifiable picture or personal notes by himself or by his doctor, who - theoretically - could use the free text field to note the patient's name. However, this seems unnecessary and even highly unlikely, as the doctor knows the patient personally and also his patient ID in the StatConsult IT-Service GmbH database.

All patient-identifying data is stored in encrypted form in such a way that only users of the respective responsible parties (haemophilia centre, pharmacy) can decrypt and read this data (even the administrators of the servers have no possibility of accessing this data in plain text).

In addition to encryption, all patient-identifying data is stored exclusively physically separate from the Haemoassist® database on a separate server, the Haemoassist® DataSafe Server (separation of clinical and patient-identifying data), so that only pseudonymised data is stored in the Haemoassist® database.

The collected primary data of the patients are needed for the medical treatment of the patient by his doctor and are therefore necessary. This is the only reason for data collection within the IT-based Haemoassist® service. Each patient must sign a consent form [46] before using the Haemoassist® service.

The Transfusion Law stipulates that the doctor must document the use of preparations for haemophilia in detail, e.g. name, surname, date of birth, address, medicinal product used, name of pharmaceutical company, etc. If the coagulation factor preparations are used by the haemophilia patient in accordance with § 14 sub-section 2a as part of home self-treatment, the haemophilia patient must carry out the documentation in accordance with sub-sections 1 and 2. The doctor who permanently treats this patient for haemostasis disorders (haemophilia treatment doctor) must check the haemophilia patient's documentation for conclusiveness and completeness at least once a year and include it in his own documentation.

Therefore, the collected data can be classified as absolutely necessary for medical purposes. Data collection takes place directly via the patient's Haemoassist® app or via the web interface of the physician and the patient - both connected to the database of StatConsult IT-Service GmbH, a subcontractor of StatConsult Gesellschaft für klinische und Versorgungsforschung mbH. The data is not passed on to other subcontractors or third parties.

The Transfusion Law stipulates in § 14 Para. 3 TFG that records, including computerised data, must be kept for at least 15 years and data according to § 14 Para. 2 TFG must be kept for at least thirty years. The patient's doctor can request deletion of the data from StatConsult IT-Service GmbH at any time and without giving reasons. The doctor's contact data will be deleted by StatConsult IT-Service GmbH 10 years after termination of the contract if the data is no longer required for billing purposes.

Secondary data is not primarily used for the use of the IT-based service. However, as they ensure the authentication of users and the technical delivery of the service to the correct recipient, they are still necessary for the use of the service - especially to ensure data protection and information security, e.g. in case of alleged security incidents.

The collection and processing of primary data is necessary for medical reasons. The collection and processing of secondary data is necessary for authentication and information security reasons.

## 17. Issues demanding special user attention:

Patients and doctors should pay special attention to data protection-relevant aspects of their IT components (smartphones, clients, PCs, etc.), as these elements are not included in the ToE

## 18. Compensation of weaknesses:

not relevant

## 19. Decision table on relevant requirements:

| *EuroPriSe Requirement* | *Decision* | *Remarks* |
|---|---|---|
| Data Avoidance and Minimisation | *adequate* | *In principle, the patient can only enter data that are necessary for the documentation of his/her illness and its course. Personal data processed with the help of the pharmacy module are only used for the purpose of tracing dispensed blood preparations in accordance with § 17 para. 6a ApoBetrO within the legally permissible scope.*<br>*All patient-identifying data is stored encrypted in such a way that only users of the respective responsible parties (haemophilia centre, pharmacy) can decrypt and read this data. In addition to encryption, all patient-identifying data is stored exclusively physically separate from the Haemoassist® database on a separate server, the Haemoassist® DataSafe Server (separation of clinical and patient-* |

| | | |
|---|---|---|
| | | *identifying data).* |
| Transparency | *adequate* | *Every patient automatically receives a starter kit from their doctor detailing the Haemoassist® service before downloading and using the Haemoassist® app.*<br>*The "starter kit" is easily accessible to patients; updates are delivered via the patients' doctors. No special knowledge is required to understand the description of the Haemoassist® service.*<br>*Patients receive easily accessible and detailed information about the Haemoassist® service.* |
| Technical-Organisational Measures | adequate | *All patient-identifying data is stored in encrypted form in such a way that only users of the respective responsible parties (haemophilia centre, pharmacy) can decrypt and read this data (even the administrators of the servers have no possibility of accessing this data in plain text).*<br>*In addition to encryption, all patient-identifying data is stored exclusively physically separate from the Haemoassist® database on a separate server, the Haemoassist® DataSafe Server (separation of clinical and patient-identifying data), so that only pseudonymised data is stored in the Haemoassist® database.* |
| Data Subjects' Rights | adequate | *Statconsult has a documented process for asserting data subject rights that supports the data controller. Within the framework of the data protection declaration, data subjects are informed about the data subject rights and referred to the communication channel via Haemoassist®@statconsult.de.* |

## Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

| | | |
|---|---|---|
| Essen, 14.09.2022 | Jörg Schließke | |
| Place, Date | Name of Legal Expert | Signature of Legal Expert |

| | | |
|---|---|---|
| Essen, 14.09.2022 | Tobias Mielke | |
| Place, Date | Name of Technical Expert | Signature of Technical Expert |

## Recertification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

| | | |
|---|---|---|
| Place, Date | Name of Certification Authority | Signature |