Short Public Report

Recertification No. 2 (2021/09)

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

Name:	*teamplay*
Version	*Version „Potassium“*
Function as provided in:	*March 2021*
Finalisation of Evaluation:	*August 2021*

2. Manufacturer or vendor of the IT product and Provider of the IT-based service:

Company Name:	*Siemens Healthcare GmbH*
Address:	*Henkestraße 127, 91052 Erlangen, Germany*
Contact Person:	*Frank Rottmayer, Dr. Ute Rosenbaum*

3. Time frame of evaluation:

2021/02/01 – 2021/08/03

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

Name of the Legal Expert:	*Dr. Irene Karper LLM.Eur.*
Address of the Legal Expert:	*datenschutz cert GmbH, Konsul-Smidt-Str. 88a, 28217 Bremen, Germany* *ikarper@datenschutz-cert.de*
Name of the Technical Expert:	*Dr. Irene Karper LLM.Eur.*
Address of the Technical Expert:	*datenschutz cert GmbH, Konsul-Smidt-Str. 88a, 28217 Bremen, Germany* *ikarper@datenschutz-cert.de*

5. Certification Authority:

Name:	EuroPriSe Certification Authority
Address:	Joseph-Schumpeter-Allee 25
	53227 Bonn
	Germany
eMail:	contact@european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

The ToE of the teamplay certification is teamplay as provided to customers in the EU / EEA. It consists of the following components:

- *teamplay Receiver, to be installed as a gateway service*
- *teamplay Platform (https://teamplay.siemens.com), with modules Usage, Dose, Protocols, Images, Insights, Reports, Mammo Dashboard and Digital Marketplace.*

No target of evaluation (ToE) are further services and products of Siemens Healthcare GmbH such as teamplay for the US market or other markets outside the EEA / EU. Furthermore, not covered by the ToE are other applications accessible in teamplay as well as their operation or procurement. Moreover, not part of the ToE is the Microsoft Azure Cloud (as such), components of the data centres, the Auth0 platform and its PaaS. Remote access to the teamplay Receiver may be necessary for dedicated professional services like installation and trouble shooting and may include temporary access to personal data stored on the device. These remote access services are always a separate service and therefore not within the scope of the ToE. Also, not part of the ToE is the operational environment of the teamplay user including tablets, apps or smartphones.

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

Users of teamplay are medical centres, diagnostic imaging centres or radiologists ("institution").

The teamplay modules provide statistical analyses (e.g. average doses, image analytics) in order to improve imaging methods in connection with the treatment of patients and for quality assurance and quality management, particularly to reduce the radiation exposure in connection with imaging methods; as well as to improve utilization, examination processes and capacity planning and the

calculation and creation of benchmark values (e.g. average dose consumptions) for other institutions and the development and improvement of utilities and applications to improve systems of the hospital and the treatment of patients.

The teamplay modules covered by the target of evaluation are introduced below:

Usage *gives an overview about devices (e.g. MRT, CT) and statistics about system utilization and changeover times. Therefore, the user can optimize clinical workflows. Usage also contains a benchmarking function, which allows the user to compare anonymised data of his institution to anonymised data of other institutions.*

Dose *provides evaluations about the used radiation dose and helps to monitor and minimize the radiation dose. With this function, fulfilment of requirements of the US-American law and the EU directive 2013/59/EURATOM with respect to transparency and documentation of radiation doses is supported. The module also helps to implement quality assurance processes, to reduce liability due to overdoses and to plan an optimal balance of image quality and radiation dose. It also contains a benchmarking function, which allows comparison to anonymized data of other institutions.*

Reports *creates country-specific reports for teamplay Dose for reporting dose deviations to quality bodies, e.g. for reportable procedures.*

Protocols *provides an overview over available, created or changed image acquisition protocols (configuration of imaging parameters of scanners) of the devices. This application serves device management purposes; no personal data is processed.*

Insights *provides a customizable dashboard for analysing dose values, device utilization and workflows. It is based on data from teamplay Dose, teamplay Usage and teamplay Protocols and supports the user in optimizing workflows, utilization and resource planning.*

Images *enables the targeted and secure exchange of image data with other teamplay users for the purpose of collaboration as well as forwarding to partner applications, for example for automated evaluations, including the return transport of results to the institutions. Images supports the exchange and viewing of image data for research and education purposes.*

*On further special **dashboards**, already existing data in teamplay can be prepared in a more subject-specific way within the above-mentioned applications. Within the Target of Evaluation is:*

- teamplay Mammo Dashboard. This is a more specific view from "Insights" specifically for optimal preparation of mammography data.

- Other specific dashboards in teamplay are currently not covered by the ToE, such as "teamplay X-ray Dashboard".

Users can access the closed user group via the teamplay platform, at https://teamplay.siemens.com, and may licence or use embedded applications for their institutions. In addition to teamplay, including the modules listed above, further applications for the support of medical care are embedded. Via the teamplay platform institutions can initiate a licencing process in a "Digital Marketplace". The licencing process is processed outside the teamplay environment by the respective provider. These other applications within the teamplay platform are not within the scope of the ToE.

Furthermore, not part of the ToE is the platform www.healthcare.siemens.de where only an overview of teamplay can be found.

Registration of users and institutions and the user authentication are independent components. The teamplay user account is based on a „Siemens Healthineers ID", which in addition to the access to teamplay applications can also be used for access to other Siemens Healthineers applications. The dedicated authentication service by Auth0 Inc. is used for the registration of users and the user authentication. After the registration of an institution and the authorization assignment users can log in to their own institution's closed user group and can access a dashboard as a start page, which contains an overview about key performance indicators and available applications.

*The **administration account** has the function „Settings", which provides user administration for the registered institution. Information about the institution, modalities, and users are managed here. Also, the teamplay specific privacy settings can be configured.*

Data minimisation by teamplay Receiver – privacy settings

The teamplay Receiver works as a DICOM node. It receives DICOM files from the customer systems as Picture Archiving and Communication System (PACS),

and, after performing the configured data minimization, uploads the resulting data in the teamplay Platform.

The DICOM standard defines the file format that is used to store the result of an imaging procedure, i.e. the generated pixel data, patient information, examination parameters and device data. Only DICOM files necessary for the teamplay applications are selected for upload in the teamplay Platform. Prior to the upload, the content of the DICOM files is minimized using allow-lists for the tags defined in the DICOM standard to ensure a robust data minimization and pseudonymization of patient data.

The user can select from three privacy profiles for minimization: "Standard privacy"; "High privacy" and "Restrictive".

Data cluster	***Standard privacy***	***High privacy***	***Restrictive***
Patient ID	*Keyed hash*	*Keyed hash*	*Dummy value*
Patient age	*Reduced accuracy – years only*	*Reduced accuracy – 8 age clusters*	*Reduced accuracy – 8 age clusters*
Patient characteristics (e.g. size, weight, gender)	*Retained*	*Reduced accuracy – clustered weight and size values*	*Not retained*
Pixel data	*Dependent on application*	*Dependent on application*	*Dependent on application*
Time/Date	*Retained*	*Retained*	*Reduced accuracy – only month of examination and time is kept*
Institution information	*Retained*	*Not retained*	*Not retained*
UIDs	*Keyed hash*	*Keyed hash*	*Keyed hash*
Device information	*Retained*	*Retained*	*Retained*
Technical data	*Retained*	*Retained*	*Retained*

Table 1 privacy profiles to minimize DICOM-tags

The data minimization is shown for each DICOM tag of such a group in detail in the product documentation. All three profiles do not keep any information that allows a direct reference to a patient, such as name, address, telephone number. Information which may be supportive to identify the patient as time / date of examination, age, gender, patient characteristics (e.g., weight, height, body mass index), and the patient ID, are reduced according to the configured privacy profile.

For the analytics applications Usage and Dose, pixel data are not retained with the exception of certain overview pixel data, used to calculate the optimal dose.

By using the privacy profile "Restrictive", data used for teamplay Dose and teamplay Usage, as well as other teamplay applications based on these applications, such as teamplay Insights, is anonymized completely. Data from teamplay Images includes pixel data that might allow re-identification independent from the privacy profile (e.g., head scan).

If either the privacy profile "Standard Privacy" or "High Privacy" is used, teamplay supports re-identification of studies and Patient ID. Using this functionality, DICOM studies can be attributed to a patient without processing direct patient identifiers in the teamplay Platform in the cloud, e.g. to analyse dose outliers within teamplay Dose.

Data transfer to third countries

In the context of the integration of sub-service providers with a third-country connection (Siemens Healthcare Private Limited, Microsoft, Auth0) the legal base of international data transfer (e.g. Schrems II) has been addressed by teamplay following the EDBP recommendation.

teamplay is pointing out the legal basis for the transfer to the user in the MSA and by contractually obligating the user to do so. For use cases in which a third country transfer would exist, the sample consent declarations can also be used.

From the evaluator's point of view, the EDPB requirements for the use of ***patient data*** *in teamplay in the Microsoft Azure Cloud have been met. In this context, the pseudonymization of the data must be recognized as an additional guarantee for the protection of this data. It is supported by the use of Microsoft's current DPA, which protects the rights of data subjects. If users process patient data in teamplay, they have been sufficiently informed in the MSA about the service providers used and the fact that this results in data transfer to third parties. In this context, users can, for example, establish a transfer authorization with the help of the sample consent declarations. In the sample declarations, patients are informed about data transfers to third countries as well and can consent to this.*

With regard to the ***operator data****, it should be noted that these are not even uploaded in the standard version of teamplay. Suitable guarantees for the*

protection of operator data are therefore provided by teamplay's standard settings. teamplay supports awareness-raising by providing appropriate information.

*With regard to the **user data**, the mandatory data for user identification and authorization are essential. The optional user data is provided voluntarily by the data subject and is also rarely used in practice. All user data is kept to a minimum. Users can read in the privacy notice at any time where and how their data is processed. Furthermore, users are also sensitized to comply with data protection compliance, so that transparency is still satisfied.*

All data is subject to the contractual protection of the DPA. Siemens Healthcare demonstrates in an assessment that appropriate safeguards as defined in Art. 46 GDPR are in place for a potential third country transfer, which minimize the risk to the protection of all personal data in teamplay. The EuroPriSe expert acknowledges this risk-minimizing approach here. The risk to the data subjects is significantly reduced by the measures identified above.

*Furthermore, the requirements of the EDPB for the use of the **DevOps of SHPL** are fulfilled. In this context, the pseudonymization of the data is to be recognized as an additional guarantee for the protection of the data. All data is subject to the contractual protections of the DPA. Siemens Healthcare GmbH demonstrates in the assessment that appropriate safeguards as defined in Art. 46 GDPR are in place for a potential third country transfer, which minimize the risk to the protection of all personal data in teamplay. The EuroPriSe expert acknowledges this risk-minimizing approach here. The risk to the data subjects is significantly reduced by the measures identified above.*

*The transfer impact assessment has been conducted for **Auth0** as well. The data is limited to a minimum (email, user name) and is mandatory for identification and authorization. The data collection supports data security according to Art. 32 DSGVO. Users can read in the privacy notice at any time where and how their data is processed, so that transparency is still satisfied. SIEMENS and Auth0 have concluded corresponding additional agreements to supplement the standard contractual clauses. All data is subject to this additional protection. Siemens Healthcare demonstrates in the assessment that for a potential third country transfer there are appropriate safeguards as defined in Art. 46 GDPR that minimize the risk to the protection of all personal data in teamplay. The EuroPriSe expert*

acknowledges this risk-minimizing approach here. The risk to data subjects is significantly reduced by the measures identified above.

Overall, the EuroPriSe expert concludes that a third-country transfer in connection with the teamplay evaluated here is proper under data protection law.

8. Transnational issues:

Siemens Healthcare GmbH offers teamplay worldwide. Contractual frameworks differ depending on the local regulations. On the US market teamplay is offered in accordance with the Health Insurance Portability and Accountability Act (HIPPA); this is not included in this evaluation.

The target of evaluation of the teamplay (version Potassium) certification is exclusively addressed to the European market and is especially geared to the privacy regulations of the European Union (EU).

teamplay customer support is either provided via employees of Siemens Healthcare GmbH in Erlangen, Germany, or via employees of Siemens Healthcare Private Limited (SHPL) at Bangalore, India, as a subcontractor of SHC. Within the international Siemens Healthcare Group, EU standard contractual clauses have also been concluded.

The Microsoft Ireland Operations Ltd. is also subcontractor of Siemens Healthcare GmbH and is assigned with the secure hosting and housing of the system components of the teamplay Platform including system updates, administration of the Azure cloud, the assignment of user accounts on the Azure cloud, audit processes and logging mechanisms. The location of these services is a data centre in Amsterdam or - as a fall back - in Dublin. Rights and obligations relating to data protection and security are governed by a comprehensive agreement, which fully meets the legal requirements for data processing by a processor.

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

None.

10. Edition of EuroPriSe Criteria used for the evaluation:

The expert used EuroPriSe Criteria Catalogue, version January 2017. Additionally, the expert used EuroPriSe-Commentary, Version 05/2017.

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

teamplay Cardio is no longer part of the EU deployment. Images Research has been merged into Images. Newly added are the applications "teamplay Insights" and "teamplay Reports". However, they only process the data provided by the user from teamplay Dose, Usage and Protocols and provide specific analyses for this purpose, e.g. on radiation dose or equipment utilization. Overviews and analyses for these specific application areas are displayed on the specific dashboard "teamplay Mammo Dashboard". No new personal data is processed here; instead, existing data from the above-mentioned applications is used.

The Master Service Agreement (MSA) as well as some essential documents, such as Whitepaper, Privacy Concept, Security Concept and the Privacy Policy have been revised. Due to the third country references through the use of subcontractors (Microsoft, Auth0, SHPL India), the effects of the ECJ case "Schrems II" had to be considered. A risk analysis was prepared for teamplay. Among other things, contractual bases were examined. The fact that teamplay only processes pseudonyms or even anonymous data in restrictive mode minimizes the risk.

TLS certificates of the web pages were updated. The Allow list of DICOM attributes has been extended. In teamplay Images, the configuration option for data minimizations has been improved. These can be set specifically for the module. The patient age can now be kept, because this is often necessary for medical reasons. Images now also has configuration options for automatic deletion and filters for SOP Classes. teamplay enables forwarding in the receiver to other applications via AET (Application Entity Titles). For each AET, individual deletion times can now be defined; furthermore, DICOM studies can be excluded from forwarding based on their SOP Class. Forwarding of DICOM studies has to be configured explicitly. A new feature is the possibility to exclude certain types of DICOM studies from forwarding. In terms of Privacy by Default, the deletion period has been preset to 7 days.

Dose now specifically supports mammography use cases, for example by extending the Allow list with specific, typical attributes (e.g. "Volume of Breast", "Pregnancy Status"). This is also where the use cases for the new teamplay Mammo Dashboard are located. Only more specific data for mammograms is processed. The attributes themselves are not directly "person-identifying." This data is also subject to the respective privacy profile set by the user in teamplay.

In Dose and Usage, the identification of SHS scanners has been improved. The Study Instance UID and the Series Instance UID are still modified in case of data minimization. However, these are now extracted in Receiver and written to a new attribute, which is used to identify the devices. It is not apparent that this results in any extended data processing of patient or employee data.

The user ID (Auth0) is now blocked after only 10 failed attempts from the same IP address and can only be unblocked via a link in an email sent to the user.

The privacy policy is no longer available in the lower frame, but in the upper frame under the collective icon "?". The imprint and copyright, among other things, are also available there. The privacy policy is accessible after 2 clicks for the user, which is still acceptable.

Layout adjustments as well as minor patches took place.

12. Changes in the legal and/or technical situation

    Cf. above.

13. Evaluation results:

    <u>Data minimization, use of pseudonyms, anonymity</u>

    Patient ID and Study UID are in all profiles replaced by cryptographic replacement values to ensure data consistency. The remaining patient characteristics values are taken over largely unchanged in the privacy profile “Standard privacy”. In profile "High privacy" the level of detailed information is already significantly reduced. Therefore, a re-identification of patients by extreme values can be excluded. In privacy profile "Restrictive" most values are removed or replaced by cryptographic replacement values. Only time of examination and recorded month remain. Patient age is specified in categories. This way it can be shown that even with a very cautious statement, a k-anonymity of k = 10 is reached for teamplay Dose and teamplay Usage. Realistic is even a significantly higher k-anonymity. Additional information about the method of treatment will also be deleted to prevent data attacks here on. As in the two less minimized profiles a re-identification of a patient cannot be completely ruled out, these privacy profiles can only be used on a legal basis, which is an informed consent of the persons concerned in conjunction with an exemption of medical confidentiality. For this, the Siemens Healthcare GmbH provides a model patient clause with a confidentiality release for customers.

teamplay enables the analysis of procedures from the device operator (generally an employee). This option is disabled by default in teamplay and can be activated by the user. In the privacy profile "Restrictive" only pseudonymized values of the name of the device operator can be uploaded, that do not allow direct conclusions to the person of the operator.

Some older scanners may still use DICOM Secondary Capture images (so-called "Black Images"), in which the dose information is burned into the image. The teamplay Receiver recognizes the dose values by using the optical character recognition (OCR) and automatically removes the burned in patient information, before the data is passed to the Platform. For this purpose, algorithms are used, which have been assessed as reasonable.

teamplay also allows to exclude individual DICOM studies from an upload to the Platform by adding the respective patients to a Deny list in the teamplay Receiver. Therefore, data of celebrity or selected persons can be completely exempted from this upload.

teamplay supports re-identification of the pseudonyms of study identifier and patientID. The re-identification completely takes place within the sphere of the customer. The re-identified original values are displayed in the teamplay UI shown in the browser of the teamplay user, but are never processed in the teamplay Platform in the cloud.

Data from teamplay Images could include pixel data that allows re-identification of the patient even in a restrictive profile (e.g., in a head scan). Some of these studies may therefore be anonymous. In other studies, a re-identification of the patient on the basis of specific characteristics, however, would be theoretically possible. The user is therefore advised by disclaimer when uploading a study, that hereby possible, no anonymized data is uploaded and he should check this. This data is further protected by the high security standard in the Azure Cloud and the operating environment of teamplay.

The MSA informs the customer about the 3rd country sub processors. In addition, teamplay maintains appropriate patient consent forms. Taking into account these organizational and information security measures (cf. below, data security), teamplay promotes compliance with patient data protection appropriately.

Cookies

For technical reasons, the use of the ai_authUser, ai_user, and ai_session cookies by the Microsoft Azure ***Application Insights*** *analysis library is*

unavoidable. These cookies have no content, have expired when set and will be deleted immediately. In this respect, there is an exception to the consent requirement of Article 5 (3), second sentence of Directive 2002/58/EC.

Furthermore, a session ***cookie*** *ARRAffinity is set. The cookie is used for load balancing and is deleted after the browser session ends. In this respect, there is also an exception to the consent requirement of Article 5 (3) of Directive 2002/58/EC.*

Strictly necessary cookies are set by the third-party provider ***Auth0*** *as part of the authentication process. These first party cookies are necessary for the implementation of the session layer for single sign-on, for attack detection and anomaly detection.*

Finally, cookies from the third-party provider ***WalkMe*** *are set. WalkMe is a service to improve the user experience, e.g. through walkthru's or smart tool tips as well as analytics services with statistics about user behaviour. The WalkMe analytics services actually require teamplay users to upload their pseudonyms to WalkMe servers. However, these services have been intentionally disabled. For downloading the current teamplay WalkMe configuration, a proxy operated by teamplay is used as an intermediary to avoid processing IP addresses of teamplay users by WalkMe. Therefore, WalkMe is ultimately not relevant in terms of data protection law and does not have to disclose any information to data subjects, for example. The cookie set here is also technically necessary and therefore falls under the exception. Consent is not necessary.*

Data blocking and data deletion

Immediately after successful upload of the minimized DICOM files the original files are deleted from the teamplay Receiver through an OS API call. In the event that a patient withdraws his consent for data use, he must appeal to the data sending institution. Data of a patient are only identifiable in teamplay when the cryptographic key has not been changed in the Receiver. In that case, the associated patient ID can only be manually assigned to the cryptographic replacement value by the institution. With this value, the records could be identified and then cleared on behalf of the institution in the database by one of the so-called DevOps Admins. Data will not be automatically deleted in teamplay to enable long-term reports. At the request of an authorized user or after the contract ends uploaded DICOM data will be deleted manually by employees of Siemens Healthcare GmbH. With the end of the contract also the institution

account will be locked and can no longer be visited. teamplay user accounts can be deleted on request.

Depending on the configuration, employee data (name of the operator of a device) may be contained in the data of an institution. Targeted deletion of one employee's data (in millions of records) is only theoretically possible and would involve a disproportionate effort; with such a deletion the productive data would be changed; this could lead to inconsistent statistics, which should be avoided. However, the corresponding privacy configuration can be changed with effect for the future, so that the uploading of the operator data is avoided.

Data security

Siemens Healthcare GmbH (SHC) is in charge of application security, the configuration of the teamplay Platform and the administration accounts and related audit and logging mechanism. Employees have administrative access to the servers through a VPN connection of Siemens network in Germany. When providing the service, SHC acts as a processor on behalf of the teamplay customers.

The physical security of the server is ensured by the security of Microsoft data centres which are holding e.g. an ISO/IEC 27001 certificate (for Ireland and the Netherlands), valid until 2023-06-18. Audits have been reviewed and confirmed by an independent body. The auditors have had the opportunity to view a recent security report.

Concerning data protection and security measures of SHPL at India location excerpts were viewed from the test documents for information security and privacy in the context of the latest internal audit of the Siemens Group. The SHPL holds an ISO/IEC 27001 certification, valid until 2023-06-13. A contract between Siemens Healthcare GmbH and SHPL also fully complies with the relevant EU regulations for data processing by a processor.

Furthermore, the Auth0 Ltd. is holding an ISO/IEC certificate for its information security management system (ISMS) supporting the Auth0 identity platform, valid until 2021-07-26.

The access protection of administrative accounts of the Platform is ensured by a multi-factor authentication and a clear separation of roles. There is only a very small number of administrator accounts for the production environment. All activities related to user management are logged in secure audit logs. The logical

security is realized by an appropriate role- and permission-concept and by adequate transmission reliability due to the use of encrypted communication.

The connection between the Receiver and teamplay Platform in the Microsoft Azure cloud is based exclusively via HTTPS with TLS.

The user is responsible for the physical security of the user environment, so this is not part of teamplay. The document "teamplay data privacy and security white paper" stipulates how to set up a secure operating environment.

Awareness of users

For teamplay, a comprehensive product documentation is available, including the transparent and sustainable aspects for data protection and data security. The user is also sensitized accordingly e.g. in the published FAQ for teamplay on the web portal and in user-videos.

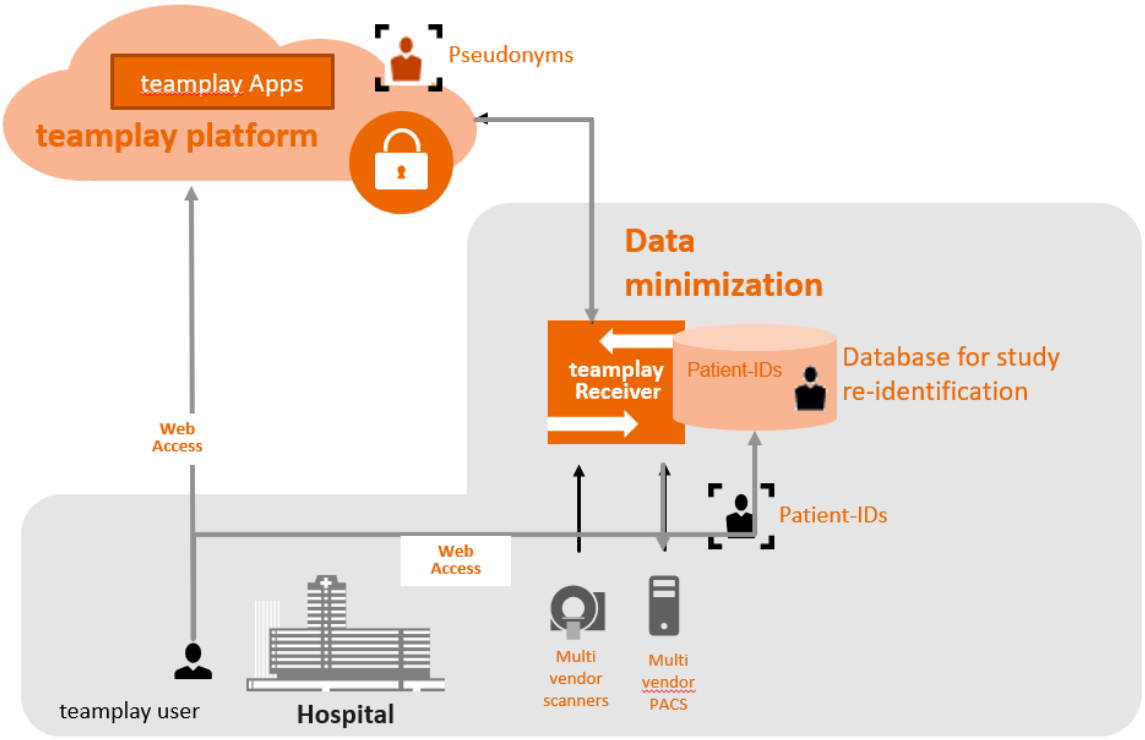
Processing of personal data

teamplay processes patient, operator, and user data. Patient data are DICOM data (the full list of used tags comes with the document "teamplay data privacy and security white paper" again). The choice of the data protection profile for the reduction of patient information at teamplay allows a sparing use of personal data. Depending on the chosen profile, patient data are pseudonymized or even anonymized. The institution is responsible for the legal base of processing of (pseudonymous) patient data. Siemens Healthcare GmbH holds a sample of a patient's consent.

As part of the registration and use of teamplay data of the user and the local administrator are recorded (business email address, first and last name, work phone number of the local administrator, password, name of institution). These data are mainly of a commercial nature, the first and last name may identify an employee of the institution. By the configuration, which data should be collected, the employee data protection can be implemented optimally.

In order to guarantee the services also different logs are produced on the systems. The contents and data retention periods have been part of the evaluation and were rated as adequate.

14. Data flow:



15. Privacy-enhancing functionalities:

    teamplay encourages data protection in many ways. The implemented measures of data minimization, pseudonymization and anonymization of patient data deserve to be highlighted. The data protection measures, such as pseudonymisation and transparency, developed by Siemens Healthcare GmbH are model examples of the principle of privacy-by-design. Transparent information and descriptions enable users to process employee and patient data in a data protection-compliant and data-minimizing manner.

    The technical and organizational data security measures taken at Siemens Healthcare and its subcontracted service providers go beyond legal standards. The implemented security concept enables customers to securely use teamplay. Only ISO/IEC 27001-certified sub-processors are used with high level physical data center protection and advanced availability and recovery mechanism.

16. Issues demanding special user attention:

    There are no issues demanding special user attention.

17. Compensation of weaknesses:

    There are no requirements assessed as "barely passing".

18. Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	excellent	teamplay offers a variety of mechanisms for anonymisation and pseudonymisation.
Transparency	adequate	Documentation, such as privacy leaflets, FAQ and user videos are informative, up-to date and understandable
Technical-Organisational Measures	adequate	Organizational and technical measures on data security and privacy are above legal standards. The data centres meet all high level requirements regarding (e.g.) physical access control, recovery mechanisms as well as network and transport security.
Data Subjects' Rights	adequate	Siemens Healthcare GmbH provides information on how to implement processes dealing with data subject rights and how to react on consumer requests in the privacy leaflet.

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.

Bremen, 2021-08-03 Dr. Irene Karper LLM.Eur. 

Place, date | Name of Legal Expert | Signature of Legal Expert

Bremen, 2021-08-03 Dr. Irene Karper LLM.Eur. 

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.

Sebastian Meissner

Digitally signed by Sebastian Meissner
DN: cn=Sebastian Meissner, o=EuroPriSe GmbH, ou=EuroPriSe CA, email=meissner@european-privacy-seal.eu, c=DE
Date: 2022.01.21 17:35:53 +01'00'

Place, Date	Name of Certification Authority	Signature