datenschutz cert

EuroPriSe European Privacy Seal

Short Public Report

teamplay

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

Name:	*teamplay*
Function as provided in:	*August 2016*
Finalisation of Evaluation:	*August 2016*

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

Company Name:	*Siemens Healthcare GmbH*
Address:	*Henkestraße 127, 91052 Erlangen, Germany*
Web:	*https://teamplay.siemens.com and* *https://bps-healthcare.siemens.com/teamplay*
Contact Person:	*Frank Rottmayer and Dr. Ute Rosenbaum*

3. Time frame of evaluation: *2015/05/01 – 2016/08/28*

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

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

5. Certification Body:

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 consists of the following components:

- *teamplay Receiver, to be installed as a gateway service with the operator (teamplay user)*
- *teamplay Platform, with modules home, usage, dose and protocols.*

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. Already active, but not ToE, is the module "Images" for common use of data and images and to build an Online Community, as well as the authentication using the Siemens Corporate Entitlement Service, that provides an alternative login functionality. Furthermore, not ToE is the Microsoft Azure Cloud or components of the data centres. Remote access may be necessary which may include access to personal data. These remote access services are always a separate service and therefore not ToE. Not ToE is at least the operational environment of the operator including tablets, apps or smartphones.

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

Users of teamplay are clinical centres, diagnostic imaging centres or radiologists ("institution"). The teamplay Receiver must be installed in a local network and communicates between the imaging systems and the teamplay Platform by minimizing data and sending it to the Platform. The standard for communication is DICOM („Digital Imaging and Communications in Medicine"), an international standard for the exchange of images and data in radiology.

teamplay is offered as basic and premium account. Basic accounts are free of charge with the possibility to upgrade to further functionalities with costs. Target of this evaluation is the premium account, encompassing all functionalities of the basic account.

By using https://teamplay.siemens.com a registered user can access statistical information. The standard user account consists of the functions teamplay Home, Usage, Dose, and Protocols.

***Home** is the landing page with an overview of user account data and functionalities.*

***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.*

***Dose** provides evaluations about the used radiation dose and helps to monitor and minimize the radiation dose. With this function, a requirement of the US-American law with respect to transparency of radiation doses is fulfilled. The module also helps to fulfil a quality control, to reduce liability by over doses and to plan an optimal mix of image quality and radiation dose.*

***Protocols** gives an overview of device protocols used.*

*The **administration account** has the function „Settings“ which provides user administration for the registered institute. Information about the institute, modalities and users are managed here. Also the teamplay specific privacy profile can be configured and reports can be activated.*

teamplay will have further modules in the near future, such as benchmarking with anonymized data of institutions to compare to other institutions. Active but not ToE are the module "images" for a common use of data and images and to build up an online community and the authentication process using Siemens Corporate Entitlement Service, which gives an alternative log-in mechanism. These functionalities are not ToE now but they are mentioned in the privacy statement.

teamplay has the following functionalities:

- *usage and dose analytics of data from several operators, not only Siemens modalities.*
- *Individual dose consumption with a dashboard dose analysis.*
- *Dose PACS-callup, that can be used to call up the PACS interface for a dose event, in order to improve the image quality (PACS = „Picture Archiving and Communication System“).*
- *Patient-specific dose views, which shows the number of treatments per patient in the institution (only available with privacy profile „standard privacy“ and "high privacy")*
- *Dose SSDE to normalize the dose value per patient height from DICOM HEADER Information or derived CT topograms (comes only with privacy profile „standard privacy“).*

DICOM and data minimisation by teamplay Receiver – privacy profiles

The DICOM standard defines about 4.000 tags in which the result of an imaging procedure, the image itself including patient data, examination parameters and device data are stored. From this data, about 250 tags are personal data or related to a person (e.g. name, sex, age of patient, doctor related data with respect to the guidelines of the DICOM standard, part 15, annex E, version 2011, PS 3.15-2011[1]). Such data can be anonymized by deleting or changing the value.

The teamplay Receiver works as a DICOM node. It receives certain, specified DICOM files from the PACS or directly from the imaging device. The teamplay Receiver gets only certain DICOM files and in addition minimises the content by three possible levels (= privacy profiles). By this process only DICOM values are stored that are necessary for teamplay statistics. Especially personal data or data that could be used for re-identification are removed, replaced by a pseudonym or less precise values depending on the selected privacy profile. Image data are not stored with the exception of certain overview images, used to calculate the optimal dose. The purpose of this minimization is a reduction of the data that may even result in reduced patient data being completely anonymous. The user can select from three privacy profiles for minimization: "Standard privacy"; "High privacy" and "Restrictive". Only by using the privacy profile "Restrictive", data are anonymized completely.

data group	standard privacy	High privacy	Restrictiv
Device information and technical data	kept	kept	kept
Time / date	kept	kept	reduced accuracy
Patient age	reduced accuracy	reduced accuracy	reduced accuracy
Institution personnel data	kept	kept	Replacement value
Patient-ID	Replacement value	Replacement value	Replacement value
UID	Replacement value	Replacement value	Replacement value

[1] cf. *http://medical.nema.org/dicom/2011/11_15pu.doc* (09/2016).

Procedure description	kept	kept	removed
Patient characteristics	kept	reduced accuracy	removed
Institution information	kept	removed	removed

Table 1 privacy profiles to minimize DICOM-tags

The left column in the table is a summary of data groups. The data minimization is shown for each DICOM tag of such a group in detail in the product documentation. First, in all three profiles all information is deleted that allows a direct reference to a patient, such as name, address, telephone number. Then, information is identified which may be supportive to identify the patient. These are values for

- *Time / date of examination*
- *age*
- *gender*
- *Patient characteristics (e.g., weight, height, body mass index)*
- *Identifier, which enables the assignment of multiple tests to a patient (Patient ID).*

8. Transnational issues:

Siemens Healthcare GmbH offers teamplay on European and US markets. On the US market teamplay is optimized for use in accordance with the Health Insurance Portability and Accountability Act (HIPPA) and is only offered for this market, which is not included in this evaluation. The US teamplay Platform is operated on servers in the United States and maintained by employees of Siemens Medical Solutions USA Inc. Correspondingly, the contractual framework with customers for this separate solution differs.

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

Siemens Healthcare GmbH (SHC) is in charge of application security, the configuration of the teamplay Platform and the local administration accounts and related audit and logging mechanism. At the request of the user data will be deleted by SHC. 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 users. Rights and obligations of the parties are regulated by the "Master Service Agreement (MSA) on the use of teamplay". The contracts fulfil the requirements of data protection law.*

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 Siemens Group worldwide uniform and binding corporate rules for the protection of personal data (BCR) exist. The BCR are not doubted even after the so called Safe Harbor judgment of the ECJ. Furthermore, the parties have completed the EU standard contractual clauses for the transfer of personal data, including a contract for processing of data by a processor, which fully meet the privacy law requirements. Possibilities of access and legal effectiveness were evaluated by a law firm without objection.

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 Dublin or - as a fall back - in Amsterdam. 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 the provider of the IT-based service:

None.

10. Edition of EuroPriSe Criteria used for the evaluation:

The experts used EuroPriSe Criteria Catalogue, version November 2011.

11. Evaluation results:

Data minimization, use of pseudonyms, anonymity

Patient ID and Study UID are in all profiles replaced by cryptographic replacement values to ensure data consistency. The remaining 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. 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, that 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 anonymised values of the name of the device operator are 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 this by using the optical character recognition (OCR) and automatically removes the burned in patient name and date of birth, 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 blacklist in the teamplay Receiver. Therefore, data of celebrity or selected persons can be completely exempted from this upload.

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 the 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 account will be locked and can no longer be visited. The disabled user account will be deleted if it is not assigned to any other institution anymore.

Data security

The physical security of the server is ensured by the security of Microsoft data centres which are holding e.g. an ISO 27001 certificate, as well as SOC 1 Type 2 - and SOC 2 Type 2 - audits has been reviewed and confirmed by an independent body. The auditors have had the opportunity to view a recent security report. Furthermore, a partial inspection of the data center in Ireland took place, which confirmed the high level of security.

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. For the pre-organization of the SHPL, an ISO 27001 certification was given in September 2015, which should be renewed on the SHPL until March 2017th. A contract between Siemens Healthcare GmbH and SHPL also fully complies with the relevant EU regulations for data processing by a processor.

The access protection of administrative accounts is ensured by a two-factor authentication and a clear separation of roles. There are only two 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 an 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 / users

For teamplay we have a comprehensive product documentation, 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.

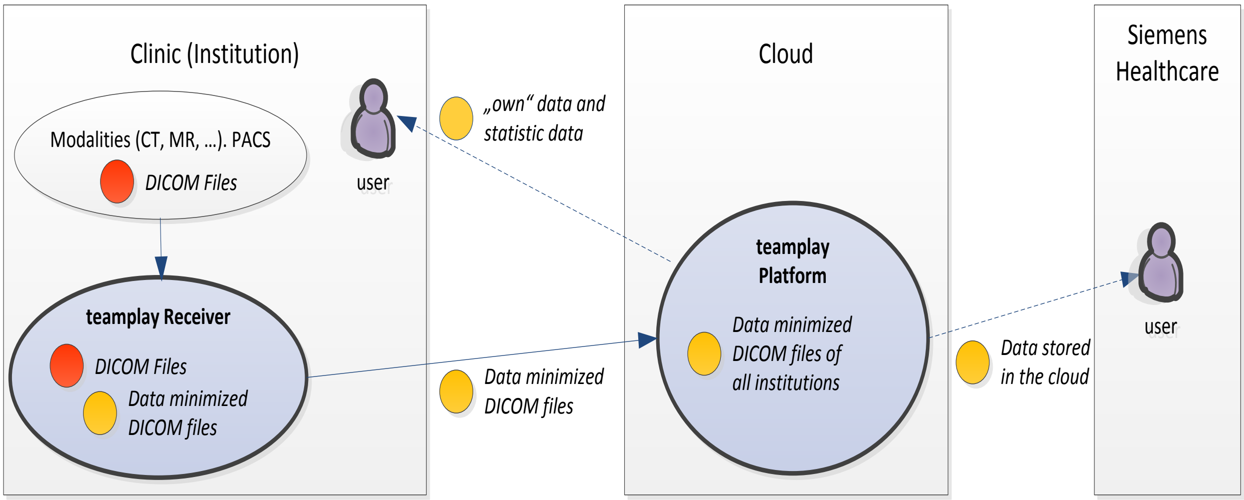
Processing of personal data

teamplay processes patient, operator, and user data. Patient data are DICOM data (the full list comes with the document "teamplay data privacy and security white paper again). Furthermore, girth and internal structures (organs, bones) are visible in the pixel data of the localizer images. Any obvious medical indications could therefore be seen in the localizer image. 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. Legal basis for the processing of (pseudonymous) patient data is then consent, for which 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 test, and were rated as adequate.

12. Data flow:


Clinic (Institution)
Modalities (CT, MR, ...). PACS
DICOM Files
user
teamplay Receiver
DICOM Files
Data minimized DICOM files
„own" data and statistic data
Data minimized DICOM files
Cloud
teamplay Platform
Data minimized DICOM files of all institutions
Data stored in the cloud
Siemens Healthcare
user

13. 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 and security measures developed by Siemens Healthcare GmbH are model examples of the principle of privacy-by-design.*

Furthermore, organizational and technical measures on data security in the data centres are exemplary and above legal standards.

14. Issues demanding special user attention:

There are no issues demanding special user attention.

15. Compensation of weaknesses:

There are no requirements assessed as "barely passing".

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	adequate	teamplay offers a variety of mechanisms for anonymisation and pseudonymisation. Data avoidance and minimisation are fulfilled from adequate to excellent
Transparency	adequate	Documentation, such as privacy leaflets, FAQ and user videos are informative, up-to date and understandable
Technical-Organisational Measures	excellent	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.

Table 2 Decisions

Experts’ Statement

We affirm that the above-named IT product and 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, 2016-09-27	Dr. Irene Karper LLM.Eur.	Irene Karper
Place, date	Name of Legal Expert	Signature of Legal Expert
Bremen, 2016-09-27	Ralf von Rahden	Ralf v. Rahden

Certification 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