Short Public Report

Recertification No. EP-S-LZ8DSG

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

Name:	*teamplay*
Version	*Version „Magnesium"*
Function as provided in:	*October 2018*
Finalisation of Evaluation:	January 2019

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:	*Ruediger Bertsch, Dr. Ute Rosenbaum*

3. Time frame of evaluation:

2018/08/01 – 2019/01/22

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 recertification consists of the following components:

- *teamplay Receiver, to be installed as a gateway service with the operator (teamplay user)*
- *teamplay Platform, with modules Usage, Dose, Protocols, Images and Images Research, Store and Cardio.*

No target of evaluation (ToE) are further services and products of Siemens Healthcare GmbH such as teamplay for markets outside the EEA / EU and the website www.healthcare.siemens.de with general product information. Furthermore, not ToE are further applications accessible in teamplay Store nor their operation or procurement. Also, not ToE is the Microsoft Azure Cloud, components of the data centres, the Auth0 platform and its PaaS. 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 the operational environment of the user including tablets, apps or smartphones.

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

Users of teamplay are healthcare providers as hospitals, diagnostic imaging centres or radiologists ("institution"). The teamplay Receiver software has to be installed in the local network of the institution and communicates between the local systems and the teamplay Platform by minimizing data and sending it to the teamplay Platform. By using

https://teamplay.siemens.com a registered teamplay user can access the teamplay applications.

Description of the teamplay modules forming part of the ToE:

***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 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 fulfil a quality control, to reduce liability by over doses and to plan an optimal mix of image quality and radiation dose. It also contains a benchmarking function, which allows comparison of anonymized data of other institutions.*

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

***Images** allows for precise and secure exchange of image data with other teamplay users for collaboration purposes. This module also supports exchange of data with medical devices and is therefore developed according to medical devices quality standards. Images Research supports the exchange and display of image data for research and training purposes. In an „Online Community" data and images can be used internally or across institutions. For this purpose, data is made visible for other users.*

***Cardio** is a module specifically developed for statistics about procedure volumes and turnaround time, and utilization of resources in the area of Cardiology.*

Users can access the closed user group via the teamplay platform, at https://teamplay.siemens.com, and may licence or use applications delivered through the teamplay platform for their institutions. Via the teamplay platform, institutions can initiate a licencing process in a "Store". The licencing process is handled outside the teamplay environment by the respective provider.

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.

Registration and management of users and institutions are communal teamplay Platform components used by all teamplay applications. 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. For teamplay user registration and user authentication, the dedicated authentication service by Auth0 Inc. is used. After the registration of an institution and the authorization assignment users can log in to their own institution's closed platform and can access a dashboard as a start page, which contains an overview about key performance indicators and available applications.

*teamplay **administrative account**s of an institution provide the function "Settings" offering user management, management of institution specific setting and modalities / devices. Also, the teamplay specific privacy settings can be configured.*

Data minimisation by teamplay Receiver – privacy settings

The DICOM standard defines more than 4.000 tags in which the result of an imaging procedure, the pixel data, patient information, examination parameters and device data are stored. From this data, about 300 tags are listed by the standard as related to a person (e.g. name, sex, age of patient, information about physicians and operators). The DICOM standard and the list of possibly personally identifiable information is constantly updated since new device generations require new parameters.

The teamplay Receiver works as a DICOM node. It receives DICOM files from the PACS or directly from the imaging device and, after performing the configured data minimization, uploads the resulting data in the teamplay Platform. The teamplay Receiver processes only DICOM files necessary for the teamplay applications and in addition minimises the content by three possible levels (= privacy profiles). By this process, only DICOM values are stored in the Platform that are necessary for teamplay applications. 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. For the analytics applications Usage, Dose, Cardio, pixel data are not stored with the exception of certain overview pixel data used to calculate the optimal dose. This results in a minimization of data that may even result in a complete anonymization of patient data. The user can select from three privacy profiles for minimization: "Standard privacy"; "High privacy" and "Restrictive".

data group	*standard privacy*	*High privacy*	*Restrictive*
Patient_ID	*Replacement value*	*Replacement value*	*Replacement value*
Patient age	*Reduced accuracy – years only*	*Reduced accuracy – 8 age categories*	*Reduced accuracy – 8 age categories*
Patient characteristics (e.g. height, weight, gender)	*Kept*	*Reduced accuracy (weight and height categories)*	*Removed*
Pixel data	*teamplay Usage / Dose / Cardio: sectional images, black images teamplay Images / Images Research: kept*	*teamplay Usage / Dose / Cardio: sectional images, black images teamplay Images / Images Research: kept*	*teamplay Usage / Dose / Cardio: black images teamplay Images / Images Research: kept*
Time / date	*Kept*	*Kept*	*Reduced accuracy*
Procedure description	*Kept*	*Kept*	*Removed*
Institution information	*Kept*	*Removed*	*Removed*
UID	*Replacement value*	*Replacement value*	*Replacement value*
Technical data / Device information	*Kept*	*Kept*	*Kept*

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. 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)*
- *Identifier, which enables the assignment of multiple tests to a patient (Patient ID)*

is reduced according to the configured privacy profile.

By using the privacy profile "Restrictive", data used for teamplay Dose, Usage and Cardio is anonymized completely. Data from teamplay Images and teamplay Images Research 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 patientID. Using this functionality, dose outliers can be attributed to a patient and further analysed outside teamplay, without processing direct patient identifiers in the teamplay Platform in the cloud.

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 (HIPAA); this is not included in this evaluation.

The target of evaluation of the teamplay (version Magnesium) 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 administration of accounts and related audit and logging mechanisms. 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 EU data protection law, namely Art. 28 GDPR.

teamplay customer support is provided by employees of Siemens Healthcare GmbH in Erlangen, Germany, and by employees of Siemens Healthcare Private Limited (SHPL) at Bangalore, India, as a subcontractor of SHC. Concerning teamplay Cardio access of employees of Siemens Medical Solutions USA Inc. (Malvern, Pennsylvania) to personal data of the productive system in the EU might be necessary for technical support of customers.

The Microsoft Ireland Operations Ltd. is subcontractor of Siemens Healthcare GmbH and is responsible for 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

    The registration and management of users and institutions was restructured and forms an independent component. In addition, the authentication service of Auth0 Inc. is used for user authentication. From user perspective, the process remains unchanged. Thus, access to other Siemens Healthineers applications is facilitated with the teamplay user account.

    On the basis of existing personal data teamplay Dose and teamplay Usage offer new evaluation capabilities, especially the benchmarking functionality. In teamplay Dose, the dose values of individual studies can be commented.

    teamplay Protocols offers additional functionalities, without collecting any patient data.

    New in scope of the evaluation is teamplay Images, Images Research and teamplay Cardio. teamplay Images enables the targeted and secure exchange of image data with other teamplay users for the purpose of collaboration. This module also supports exchange of data with medical devices and is therefore developed according to medical devices quality standards. Images Research supports the exchange and viewing of image data for research and educational purposes. In an "online community", data and images can be used internally as well as across institutes and physicians, making the data visible to other users. The data minimization for teamplay Images can be deactivated when used for clinical purposes. For other modules, this option is not available. Data from teamplay Images and teamplay Images Research might contain pixel data that allows re-identification based on specific patient characteristics (e.g., in a head scan). Individual studies may therefore be anonymous when using restrictive privacy profile, but a general statement of anonymity cannot be made. Depending on the individual circumstances, the processing of this patient data may require a declaration of consent from the persons

concerned and/or a release from medical confidentiality. For this purpose, Siemens Healthcare GmbH has prepared a model patient declaration.

teamplay Cardio is a module developed specifically for cardiology processes and workflows. It supports the analysis of the process volume, the statistics, the utilization of employees, rooms and resources. Besides the DICOM standard, other formatting standards are also used. It might be necessary that employees of Siemens Medical Solutions USA Inc. access personal data of teamplay Cardio in the productive system in the EU for support issues. The contracting party is informed about this fact. Furthermore, there is a personal consent template for Cardio in which this possibility is listed.

New in scope of ToE is the solution store, which allows institutions abonnements of a variety of services and applications. New "Terms and Conditions" regulate the relation between the institution and Siemens Healthineers concerning the use of the solution Stores and the services provided in relation to the Solution Stores by Siemens Healthineers as well as the conclusion of contracts between the institutions and service providers.

12. Changes in the legal and/or technical situation

teamplay was further developed in conformity with the GDPR and additional functionalities. Changes were made concerning the adjustment of the Master Service Agreement, the adjustment of the Privacy Notice and the creation of an optional marketing consent.

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 hereon. 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. For this, the Siemens Healthcare GmbH provides a model patient clause.

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 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 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 blacklist 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 if privacy profile "Standard Privacy" or "High Privacy" is configured. The re-identification completely takes places 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. In case of privacy profile "Restrictive" no re-identification is possible.

Data from teamplay Images and teamplay Images Research 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, might be possible. This data is further protected by the high security standard in the Azure Cloud and the operating environment of teamplay.

According to the Microsoft Operations Concept, remote maintenance takes place exclusively via an EEA service. The user is informed of this fact in the MSA. 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.

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. Due to applied pseudonymization, data of a patient is only identifiable by combined manual effort of the institution and Siemens Healthcare. Data will then be deleted manually in the teamplay data bases by Siemens Healthcare personnel. If the cryptographic keys used for pseudonymization in the teamplay Receiver are not available, identification is practically impossible. 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

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 2020-06-19. 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 2020-06-13. 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 was made 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 use of personal data minimized to the needs of the institution. Depending on the chosen profile, patient data are pseudonymized or even anonymized. Legal basis for the processing of (pseudonymous) patient data is consent. Siemens Healthcare GmbH provides a sample of an appropriate consent form. Transfers of personal data to third countries taking place when teamplay is used are justified by the consent of the patients or by standard data protection clauses pursuant to Art. 46(2)(c) GDPR.

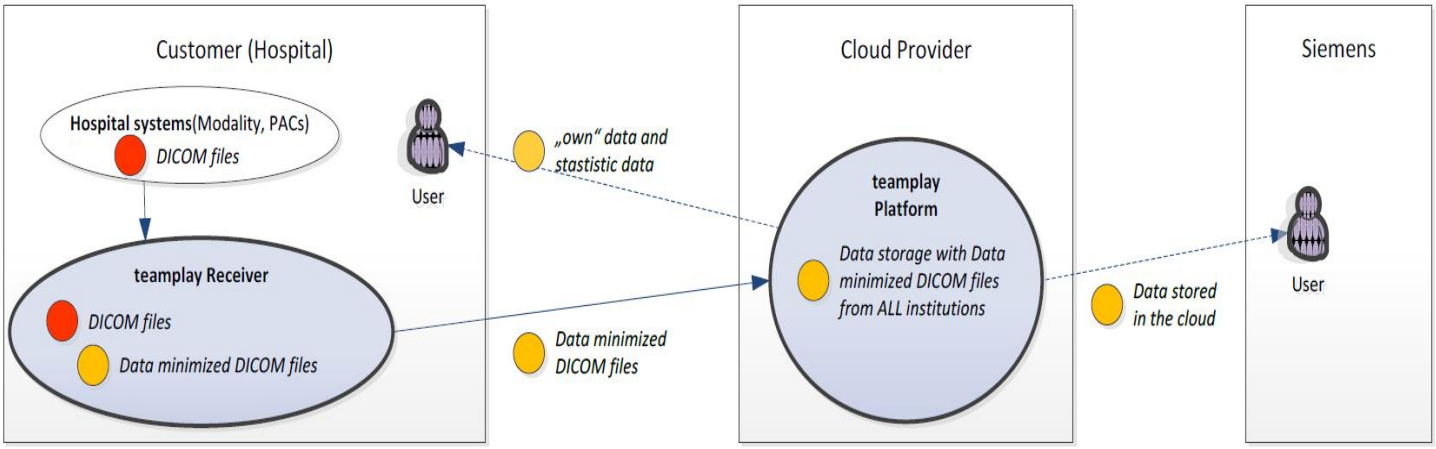
Operator data is part of the processed DICOM data. Upload of this data is disabled by default and can be configured by the institution. Thus, employee data protection can be implemented optimally.

As part of the institution registration name of the contact person are recorded (business email address, first and last name, work phone number, password, name of institution). These data are mainly of commercial nature, the first and last name identify an employee

of the institution. For teamplay user registration only email address, first and last name, country is collected. Thus, personal data collected of teamplay users is adequate.

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 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.

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, 2019-03-11 Dr. Irene Karper LLM.Eur. 

Place, date	Name of Legal Expert	Signature of Legal Expert

Bremen, 2019-03-11 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: 2019.05.29 16:00:58 +02'00'

Place, Date	Name of Certification Authority	Signature