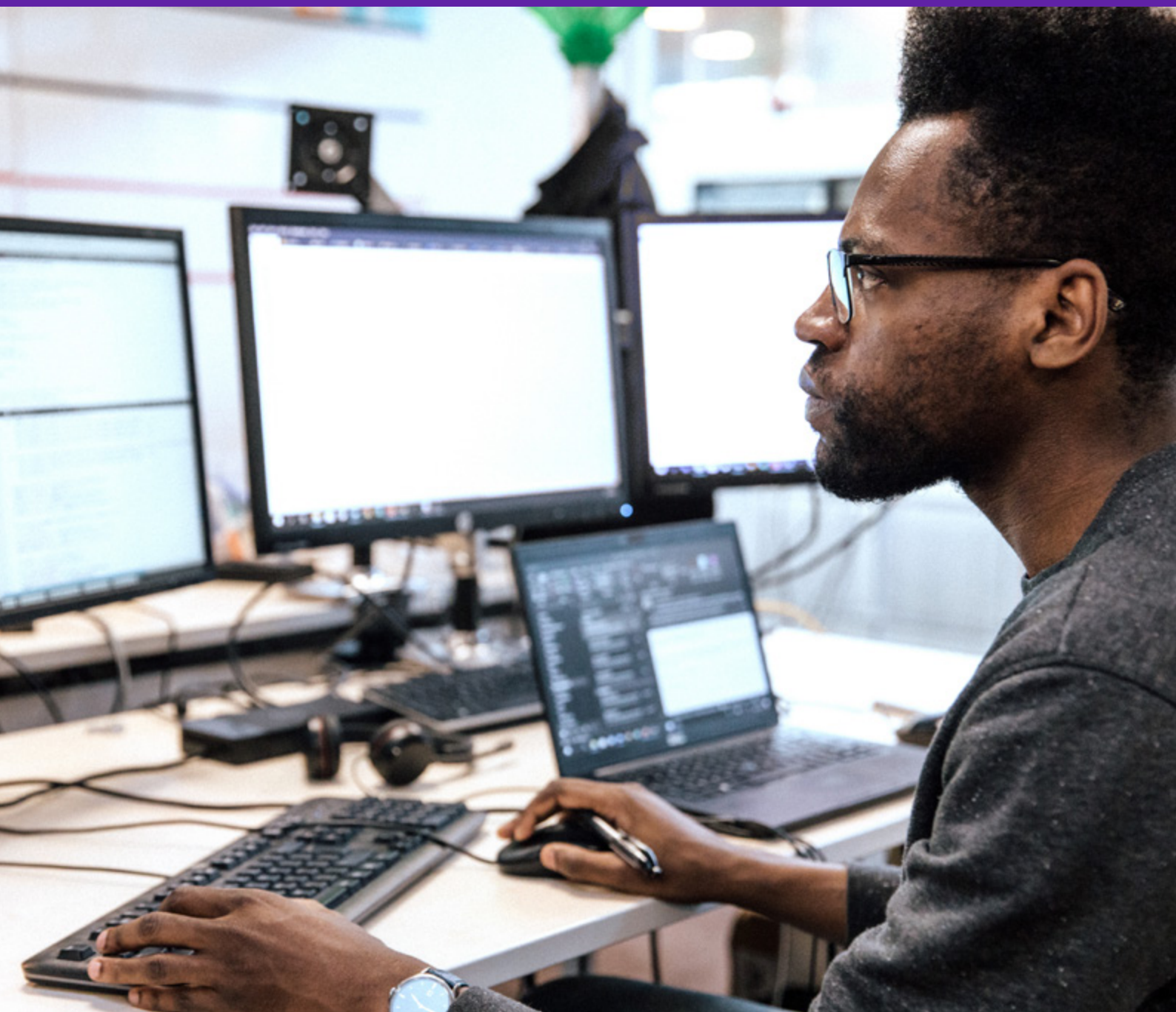
GE HealthCare

How Does GE HealthCare Protect Customer Data?



You care about your patients and their data. So do we.

At the heart of the GE HealthCare integrity program is The Spirit & The Letter, consisting of our code of conduct and a set of global company policies that cover our integrity commitments for critical subjects and risk areas.

The Spirit & The Letter must be followed by anyone who works for or represents GE HealthCare. It is underpinned by a customer data protection framework composed of the Customer System Personal Information (CSPI) policy and standard, which is further supplemented by our ISO 27001 certified Information Security Management System.

Why is data protection important?
In today's digital economy, information has become a precious resource and its security is of paramount importance. GE HealthCare's provision of services may require access to customer data. To ensure its security, we have a customer data protection framework.

Who is in scope?
These requirements apply to all GE HealthCare employees, contractors, consultants and agents working for and on behalf of GE HealthCare.

What is customer data?
Customer System Personal Information (Customer Data) is data originating from customer systems, including reports, databases, data extracts, DICOM Studies, images, logs (including network analysis files) and other files that may contain personal information or sensitive information.

If the classification of the data is unclear, the data is treated as personal information.

What is the GE HealthCare approach to data protection?
At GE HealthCare we:

- Strive to protect customer data with the appropriate technical and organizational measures to ensure confidentiality, integrity and availability.
- Design our program to comply with data protection laws and regulations.
- Continuously improve our privacy and security processes, tools and controls.

GE HealthCare is a trusted partner

GE HealthCare will only obtain, use, or store customer data as contractually agreed upon and only under the protection of our technical and organizational controls.

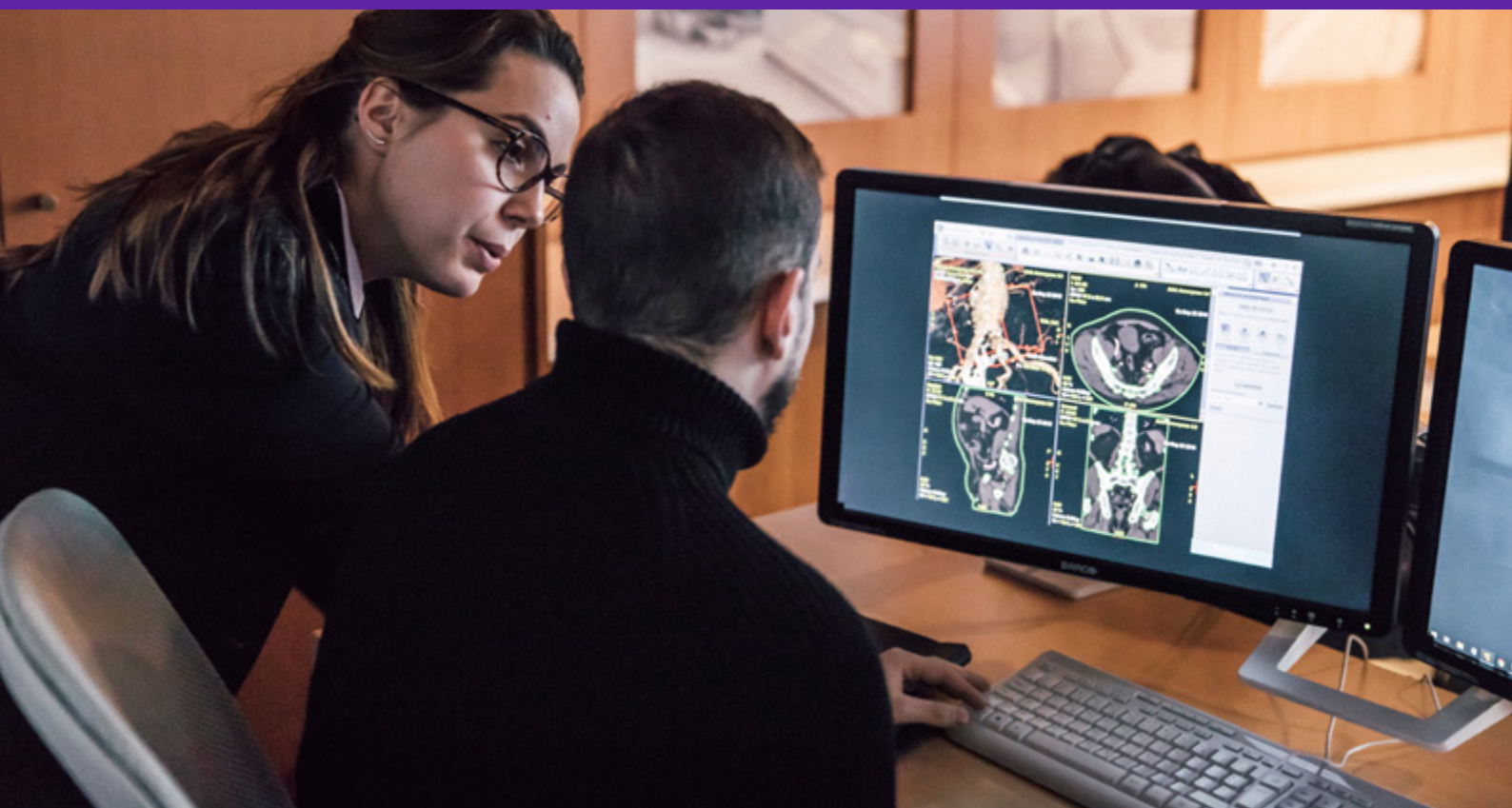
Limitation on use of customer data
Customer data will be used only for legitimate business purposes and shall be processed only for the purposes of performing the specific activity.

Activity records
Any activity performed by GE HealthCare on customer data, or customer systems, shall require a record documenting the actions performed by GE HealthCare.

Data minimization and de-identification
For any activity involving customer data, the data set is minimized so far as reasonably possible to the task being performed, and de-identification is conducted whenever possible. De-identified data is considered personal information and subject to the controls of the standard.

Data storage and retention
Customer data is stored only on approved devices and is retained for only as long as reasonably necessary for the activity to which it relates.

Access to customer data
Technical and organizational controls are in place to limit access to customer data and to protect it during the performance of any activity. Access is limited only to individuals who have legitimate business purposes to process it, and then only where the prescribed privacy and security training has been completed. Further, any GE HealthCare personnel granted access to customer information whether on a customer system or a GE HealthCare asset are required to not further share or disclose that information to others unless similarly authorized.



Data privacy is a priority

Business Approved Methods
When performing activities with customer data, GE HealthCare personnel are only allowed to use approved devices, technologies, tools and methods.

Technology Evolution

GE HealthCare strives to continuously improve the suitability, adequacy and effectiveness of our data privacy framework through proactive monitoring and continuous improvement.

Security & Privacy

Any event which has the potential to impact the confidentiality, integrity or availability of customer data or systems are reported, investigated, and managed via the GE HealthCare Incident response process.

Education

Privacy and security training is completed by all GE HealthCare personnel with access to customer data. Only GE Healthcare personnel who have successfully completed the training and have been approved by their leader are permitted to work with customer data.

Control

Periodic audits are conducted by qualified and, where appropriate, independent parties to verify compliance with fundamental privacy and security principles. The results of such audits are communicated to GE HealthCare's Global Head of IT Security and Chief Privacy and Data Protection Officer.

How GE HealthCare manages your data

Cross border transfer of customer data
Where required, customer data may be transferred out of country. Appropriate legal mechanisms are in place prior to any data transfer.

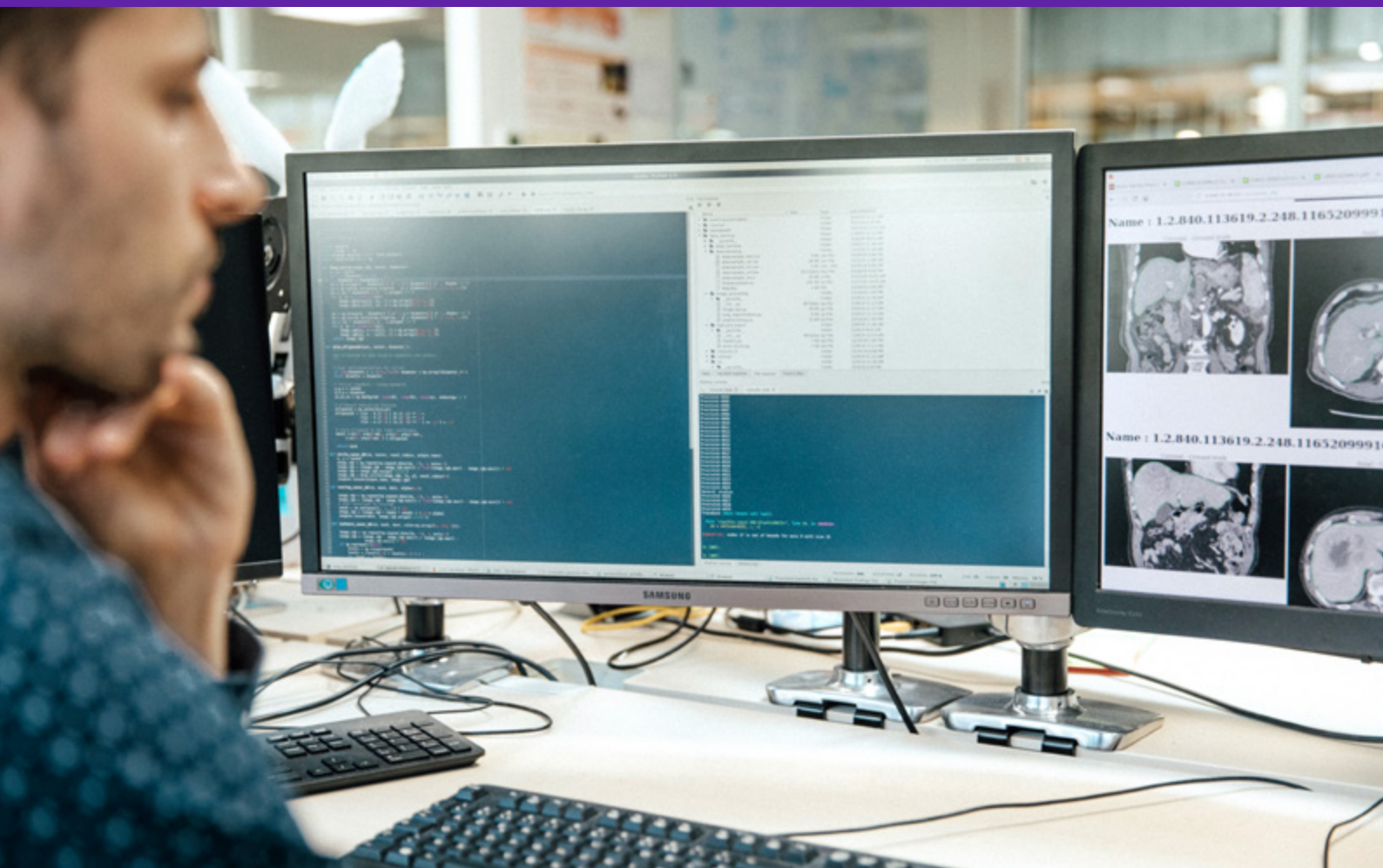
Data removal
Media containing customer data will be returned, securely wiped, or destroyed at the end of an activity.

Automated activity
In alignment with contractual service level agreements, GE HealthCare authorized agents may automatically connect to customer systems to perform service activities. All activity is tracked and recorded in an associated service case.

Connecting to customer systems
Connections to customer systems will only be made by a qualified GE HealthCare employee, from a GE HealthCare issued and maintained device, using only approved and validated methods. No personal devices are permitted.

Transfer of customer data
Transfers of customer data will only be made with company assets. No personal devices are permitted.

Receipt of unsolicited media
If GE HealthCare receives unsolicited data from a customer via any media, such as portable media, email, paper, film, etc., the data will be transferred to an approved storage solution and the original media will be returned to the customer or destroyed.



GEA35411 (7/2024)
JB29161XX

GE HealthCare