Global Enterprise Security

Technical & Organizational Data Protection & Security Measures (TOMs)

Cerner and any other processor engaged by Cerner for carrying out specific processing activities on behalf of our clients (sub-processor) is bound to adhere to the highest standards of data privacy and security. These technical and organizational data protection and security measures introduce you to our minimum levels of protection and security for personal data. Our Global Privacy Office together with our Enterprise Security Team oversee all of Cerner's data processing activities.

Access Control

Description
Physical access, system access and data access to data-processing specific resources, which also process and use personal and patient-related data, is only permitted to authorized users and under consideration of purpose, data economy, separation control and resilience. It must also be ensured that access, input, changes or deletion of data can be tracked in person and timestamped. Only authorized users are granted physical, system and data access.

Measurement
Cerner* protects persons, campus, buildings, rooms, data processing systems, data and information with adequate physical and logical access control mechanism that ensure secure identification, authorization, processing, storage, deletion and traceability. This includes security classification, including asset management, for all relevant resources, including but not limited to buildings, rooms, data processing facilities, data and information, as well as employees, suppliers, partners and other service providers.

Appropriate methods include, but are not limited to, access profiles, pin pads, video surveillance, security guards, intrusion detection systems and intrusion prevention systems, role-based authorization management, credential- and key management, data encryption, an end-point specific device and patch management.

Cerner only allows authenticated users access to personal data and patient health information. Successful and unsuccessful attempts to access personal data is recorded in log files capturing creation, alteration, and removal according to the applicable legislation.

***Any Sub-processor assumes responsibility for adhering to the same or appropriately adequate measures by entering into a service agreement with Cerner.**

Cerner

Disclosure Control

Description
It must be ensured that personal data cannot be read, copied, changed or removed without authorization when being transferred electronically, during its transport, or storage on a data carrier, and that the location to which a transfer of personal data is intended to be made using data communication equipment can be verified and determined.

Measurement
Protection of electronic communication channels by equipment, closed networks and procedures for secured data transfers and data encryption which prevent the access and/or manipulation of the data. Cerner tracks access to and activity on network devices, security infrastructure components, and server systems, and monitors usage by transferring logs to a centralized repository for analysis, troubleshooting, compliance, and auditing purposes. Risk assessments are carried out to assess the way the data are used and the overall sensitivity of the data.

If a physical data carrier transport takes place there are verifiable transport processes which protect against unauthorized data access or consequential loss. Physical data carriers are disposed of in accordance with applicable regulations that adheres to the HIPAA Security Rule 164.310(d)(1), ISO27001:2013, or NIST 800-88.

Order Control

Description
Personal data that is being processed as part of the assignment is only processed according to Client‘s documented instructions.

Measurement
Cerner has established processes designed to ensure compliance with Client’s instructions. This includes the requirements of the EU General Data Protection Regulation (GDPR).

Cerner documents instructions and the identities of those persons giving and receiving the instructions. Cerner enforces regulatory or contractual requirements through agreements with its subcontractors. Cerner requires data processing agreements and nondisclosure agreements with its suppliers, including Third-Party Data Centers, as appropriate based on that entity's access to data and other confidential information. Cerner performs an annual supplier security risk assessment and additional due diligence based on risk. A Data Security Questionnaire is required to be completed prior to the execution of new Master Service Agreements for vendors supporting Cerner’s hosting organization.

Availability Control

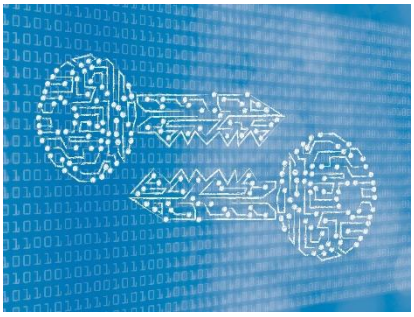
Description
It is to be ensured that personal data are protected against accidental or forced destruction or loss as well as that the data collected can be recover.

Measurement
If any data is saved, it is protected in redundant systems for recovery. In addition, the Cerner uses uninterruptible power supplies and redundant infrastructure components (e.g. UPS, batteries, generators, air condition, network equipment) to protect the data center's function set.

Cerner uses multiple overlapping security applications and countermeasures to protect the Platforms. For example, regularly updated antivirus software and spyware filters are available on the network and on applicable Data Processing systems. In addition, Cerner grants access to client systems based upon role, completion of required training, and the principle of least privilege necessary for access. This concept enables separate processing and a separation of clients on the hardware or software side. Personal data will be stored in an appropriate encrypted form in accordance with Cerner policies. Test and production systems are separated.

Cerner provides a redundant and highly available infrastructure to minimize disruptions to the production environments. If a disruptive incident occurs, Cerner follows an established, exercised and documented contingency program to restore service as quickly and effectively as possible, using commercially reasonable measures. The incident management portion of Cerner's contingency planning program is tested, reviewed, and updated annually. Cerner offers different levels of disaster recovery services based on the applicable Platform.

Unrecognizable Data



Description
Cerner ensures, in compliance with the local binding law and/or requirement, that proper pseudonymizing and encryption mechanisms are in place to safeguard the data that are generates, consuming, deleted or transferring between systems.

Measurement
Cerner maintain specific procedures to ensure that Information may be pseudonymized, if required. Possible scenarios for pseudonymous information are data exports or data operations within test environments.

Encryption and its mechanism are properly implemented, to provide a reasonable level of assurance that sensitive data cannot be viewed and/or altered by unauthorized parties. It is ensured that the implemented encryption is appropriate to meet the requirements for the specific situation where encryption is required. That is achieved by required determination of data's sensitivity, periodically evaluation of the used and available cryptographical functions and solutions as well as holistic key management, which is auditable against applicable policies.

Effectiveness Evaluation

Description

It must be ensured that the efficiency of the implemented technical and organizational controls is continuously evaluated and that all deployed and/or provided services and solutions follows Cerner's Security by Design approaches. The controls must be assessed, to ensure that they are conform to the state of the art.

Measurement

Cerner has developed an overarching global framework for managing information security, extended by local (national) frameworks. It provides a high level of protection against attacks from in- and outside to prevent the provided the processed data for any data manipulation, data misuse or data leakage.

Cerner engage specific teams which performs continuous health checks in environments to identify vulnerabilities and to initiate appropriate measurements to resolve issues. Furthermore, Cerner maintain appropriate Quality Management Systems and is continual audited by external accredited companies to ensure the effectiveness of the controls implemented. During the implementation phase, the controller receives adequate guidance and training on appropriate configurations and/or settings (e.g. of user access rights and the system's security options).

Global Enterprise Security

Technical & Organizational Measures (TOMs)