KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Population Health Tool (HealtheIntent)

Technical and Organisational Measures to Protect Personal Data

Sources

[Data Protection Act 2018 (DPA)]

[General Data Protection Regulations (EU) 2016/679 (GDPR)]

[Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)]

Definitions and Context

- Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- While information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures
- Measures taken should consider available technology, costs, nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
- The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- The impact of non-secure data processing can be as serious as becoming a victim or fraud or being put at risk of physical harm or intimidation
- Additionally, individuals are entitled to be protected from less serious kinds of harm like embarrassment or inconvenience
- the data should be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and

- the data should remain accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

Risk Assessment

Risk	Low	Medium	High
Sensitivity of the information at risk (highly personal / stigmatised information)			🟥
Number of data subjects who may be affected, should the data be disclosed			🟥
The potential impact on rights and freedoms if confidentiality was compromised			🟥
The potential impact on rights and freedoms if data was unavailable		🟧	
The potential impact on rights and freedoms if data was of poor integrity			🟥
Based on the corporate appetite, estimate the potential reputational damage			🟥
Based on the type of data, estimate the financial cost of a breach			🟥

Confidentiality, Availability and Integrity

HealtheIntent processes data that is inherently high risk where appropriate technical and organisational measures are not put in place.

This assessment will therefore explore each of the elements drawn out within data protection legislation for mitigation of those risks.

Encryption of Personal Data in Transit

The core communications channel used for the project will be the HealtheIntent Data Upload Utility (HDUU). The system encrypts the data in transit (256 bit) and transmits it across HSCN / N3 into the Cloud Platform.

- The Data Upload Utility (DUU) is used to upload files to HealtheIntent, which resides in Cerner's cloud.

- The collector is an HTTP endpoint used to upload data into the cloud.
- The endpoint is protected by CernerCare's OAuth Service.
- HDUU is a command line tool that sends files to the collector to upload.
- Upload parameters are specified to identify and describe the file being sent to the collector.
- A companion metadata file is uploaded with the source file and contains metadata about the source file, (for example, character encoding).
- The practice will request a system account.
- The utility uses the system account to authenticate the system calling the Collector's upload service.
- The system account has a corresponding account oauth-secret, which is essentially the password to the system account that authenticates the encryption.

Encryption of Personal Data at Rest

All NHS Issued devices are encrypted as standard. The clinical systems from which the data is extracted via HDUU provide encryption to best practice standards as required by NHS Digital.

The Cloud Platform that hosts HealtheIntent is describes as encrypted at rest to 256 bit standard, according to the Cerner Enterprise Security Programme.

Pseudonymisation

GDPR identifies four categories of data;

(1) Identified (subject is immediately identified)

(2) Identifiable (subject could be identified through indirect identifiers such as NHS No)

(3) Article 11 De-Identified (identity is not apparent from the data; data is not directly linked with data that identifies the person. Could potentially be re-identified if matched to additional identifying data. No known, systematic way for the party to reliably create or re-create a link with identifying data)

(4) Anonymous / Aggregated. Identification is not possible.

- The category of the data at the point of extraction is Category 1 – *individual is identified*

- The category of data being held within the HealtheIntent Cloud Platform (Integrated) is **Category 1** – *individual is identified*
- The category of data being held within the Health Analytics Tableau will depend on the access provided and will be approved at IG Working Group. Likely to be **Category 3 or 4** – *subject could be identified through NHS Number*
- The category of data being accessed through the primary care interface is **Category 1** – *individual is identified*

The objective of delivering direct care to the individual could not be achieved with information that is not identifiable.

The object of undertaking risk stratification does not always require identification of the individual. Access to Categories 3 or 4 will generally be provided at this level. Where it is necessary to access Category 1 or 2, this will be approved by IG Working Group on a case by case basis.

It therefore appears that pseudonymisation has been applied in so far as reasonably practicable to reduce the risk to the rights and freedoms of data subjects.

Role Based Access

Stakeholders accessing HealtheIntent or Health Analytics will be authorised by WSFT in accordance with the authorisation process at Appendix A.

Access will be in accordance with the Role Based Access Schedule at Appendix B. This ensures that those accessing HealtheIntent for direct care purposes are able to access identified / identifiable data and that those accessing Health Analytics for healthcare management / public health / risk stratification for population health purposes are only able to access category 3 or 4 as standard.

Access Control and Authorisation

To ensure that access is only gained by those who have been authorised, WSH and the Joint Controllers have agreed to collaborate to ensure appropriate access control across all stakeholders.

Access is via two factor authentication which provides authentication and an audit trail of access[1].

The practice and other controllers will have their system IP addresses whitelisted to ensure that the access is authorised by WSH – Cerner will not take an extraction from an IP address that is not whitelisted

Access Audit

The Practice shall be responsible for requesting access audits from Cerner to ensure that access is appropriate.

The Information Sharing Agreement provides an agreement to collaborate in the event of an incident such as inappropriate access.

Obligations of Secrecy

To ensure that all employees are aware of best practice with regard to confidentiality of personal data, there is a confidentiality clause in all Practice employment contracts.

The Practice are responsible for ensuring that the clinical system contract binds their system provider (as a Processor) to confidentiality in line with GDPR Article 28 and s 59 DPA 2018.

Systems and Information Governance Training

The Information Sharing Agreement provides that parties shall ensure adequate training for staff involved in the project.

As the project matures, there will be a central training programme developed to ensure that new starters are properly briefed on the use of the system.

Information Incidents

The Practice has an Information Incidents Protocol in place that aligns with the changes introduced by GDPR and DPA 2018. Incidents will be monitored and discussed collaboratively and are required to be shared at the IG Working Group by virtue of the sharing agreement.

[1] https://digital.nhs.uk/services/registration-authorities-and-smartcards#how-are-records-protected-

The Practice Information Incident Protocols in place cover data breaches and system compromises, including a communication plan that aligns with the notification requirements brought about by recent changes in data protection law. This should be replicated in the IG Working Group TOR.

How Do the Stakeholders Ensure that the Data Remains Accessible and Usable?

HealtheIntent is subject include Business Continuity Measures as described as below;

Cerner's commitment for access to cloud-based solutions in the event of a disaster is a commercially acceptable, "best effort" recovery. Cerner is able to allocate and configure replacement infrastructure in a timely manner to restore services as quickly as possible.

Disaster recovery is defined as the complete and total loss of a data centre which cannot be recovered in a relatively short interval (typically less than 24 hours). Cerner's disaster recovery and backup plan includes the use of multiple data centres. The primary data centre will be used for production environment and includes full N+1 infrastructure and operations redundancies. The alternate data centre will be used for disaster recovery and back-up preparedness. All of the source data will be replicated to an alternate data centre. Cerner has the necessary capabilities including disaster recovery tools, services, and a defined process to replicate the production environment to the alternate data centre.

How Do the Stakeholders Ensure that the Data is Protected from Cyber Attack?

Cerner's cybersecurity infrastructure is described in detail in their Cerner Security Enterprise Programme document and is comprehensive in nature. Summarily it includes;

Presence of a Cybersecurity Program to address the increased cybersecurity threat that the healthcare sector is facing

Internal vulnerability and testing team to continuously interrogate environments proactively

Reviews the administration of security appliances and technologies

Applies National Institute Standards Technology (NIST) standards

Presence of a Computer Security Incident Response Center (CSIRC) – responsible for 24x7 continuous monitoring and incident management

Presence of a Vulnerability and Threat Management who scan the infrastructure for vulnerabilities

The VTM Team also undertake penetration testing of systems and applications at least annually

Conclusion: Technical and Organisational Measures to Protect Personal Data

- The parties have put in place measures to protect data at rest and in transit.
- Access to personal data is controlled, authorised and able to be audited.
- Appropriate contracts in place with employees and with third party processors are required by the agreement.
- There are measures in place to back up critical assets and to respond in the event of a data breach.
- There are measures to protect the resulting information assets from cyber attack
- Incidents shall be responded to in line with data protection legislation and will be monitored.
- It is concluded that the HealtheIntent project has put in place appropriate technical and organisational measure to protect personal data such that they align with best practice, industry standards and are commensurate to the level of identified risk.

Risk Identification

Risk / Gap	Action	Status
There is a risk that data is not protected in transit	Confirm encryption of data in transit to best practice standards	Complete
There is a risk that data is not protected at rest	Confirm encryption of data at rest to best practice standards	Complete
There is a risk that pseudonymisation has not been applied where reasonably practicable	Confirm that, where possible, pseudonymisation has been applied	Pending

There is a risk that access is not assessed according to a legitimate business need	Ensure that Role Based Access is in place	Complete
There is a risk that Access is not appropriately controlled and authorised	Ensure that there is a documented protocol for authorisation and a joint approval process	Pending
There is a risk that access will not be appropriately audited	Ensure that there is an access audit schedule in place and that the outcome is jointly discussed by controllers	Pending
There is a risk that there are not obligations of secrecy in place for processing health data	Ensure that processors and employees are bound by appropriate contracts	Complete
There is a risk that stakeholders are not appropriately trained in the use of the system and wider information governance	Ensure that DSA mandates training for all stakeholders	Complete
There is a risk that Information Incidents will not be identified and managed in accordance with the law and in a timely manner	Ensure that DSA and processing contract with Cerner include requirement to report and cooperate on incidents	Complete