DATA SECURITY

This remains the cornerstone of any software product introduced for patient management in today’s healthcare world. Both clinicians and patients need to trust that all data is securely protected with no risk of compromise of this information.

GENERAL DATA PROTECTION REGULATION (GDPR)

Approved by the European Parliament in April 2016, the GDPR supersedes national laws, such as the UK’s DPA, to unify data protection laws and facilitate the flow of personal data across the 28 EU member states.

The GDPR will came into effect on 25 May 2018, and organisations around the world that process the personally identifiable information of EU residents are required to abide by a number of provisions or face fines of up to 4% of annual global turnover or Û20 million – whichever is higher.

GDPR comprises of the following components:

• Data must be processed lawfully, fairly and in a transparent manner.

• Personal data should be protected through pseudonymisation and approved encryption.

• Personal data can only be collected for defined purposes. Storage limitations will apply.

• Organisations have to meet new requirements to secure data subjects’ consent.

• Data subjects have been granted extended rights.

• Organisations need to be able to demonstrate compliance.

• Data subjects can bring legal action against organisations in case of data breach.
The GDPR encourages the adoption of certification schemes as a means of demonstrating compliance. Certification to ISO 27001 can help organisations achieve their compliance objectives, protect their data and create greater business efficiency. ISO 27001 is the internationally recognised best-practice standard that lays out the requirements of an ISMS (information security management system) and provides a holistic approach to information security that encompasses people, processes and technology.

Context Health has a robust approach to GDPR, specifically that the software was developed at the time exactly when GDPR was first introduced in 2016. This has meant that the solution has built in 'Privacy by Design'. Other solutions have had to retrofit GDPR which, we believe, will always be an inferior approach.

DATA PROTECTION ACT (2018)

The Data Protection Act is important because it provides guidance and best practice rules for organisations and the government to follow on how to use personal data including:

1. Regulating the processing of personal data.

2. Protecting the rights of the Data Subject. This is a 'natural' person or individual who is the subject of personal data. This is an important term in the context of GDPR where the Data Subject has certain rights that need to be adhered to ensure that people's data is being properly handled at the risk of punishment.

3. Enabling the Data Protection Authority (The ICO) to enforce rules.


The DPA’s rules are very thorough and cover rules around sharing of data, and data security. At the heart of it are eight common sense rules known as the 'data protection
principles’ that all organisations collecting and using personal information are legally required to comply with.

The law provides stronger protection for more sensitive information such as:

- Ethnic background
- Political opinions
- Religious beliefs
- Health
- Sexual life
- Criminal history

The Data Protection Act was replaced in May 2018 by the General Data Protection Regulations (GDPR).

DATA SECURITY AND PROTECTION TOOLKIT (DSPT) CERTIFICATION

The DSPT is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian’s 10 data security standards. This forms an essential part of the process that ensure adherence to these standards and all organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

DSPT Overview

CONTEXT Health DSPT Certification
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

HIPAA is required by the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. Safeguards must be in place to ensure appropriate protection of electronic protected health information.

The following link provides a good overview explanation of the process required for a system to be deemed safe to use in the United States:

[HIPAA Overview](#)

CREST CERTIFIED PENETRATION (PEN) TESTING

CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST provides internationally recognised accreditations for organisations and professional level certifications for individuals providing penetration testing, cyber incident response, threat intelligence and Security Operations Centre (SOC) services.

The Context Health solutions have been externally tested and validated as safe as defined by the CREST standards.

Further information can be found below:

[CREST Overview](#)