PRIVACY IMPACT ASSESSMENT

1. CLINICAL REVIEW SERVICES

The General Data Protection Regulation mandates "data protection by design[1]" to ensure privacy and data protection compliance are considered at the earliest stages.

This privacy impact assessment is being carried out for the **Clinical Review Services** that are carried out by Interface Clinical Services.

2. SCREENING ASSESSMENT

This project has been assessed against the screening questions provided by the Information Commissioner's Office and a full privacy impact assessment is required.

3. PRIVACY IMPACT ASSESSMENT

Step one: Project details: Clinical Review Services

Interface employs pharmacists to deliver clinical review services that assist healthcare organisations implement systematic approaches to the health and wellbeing of patients with long term conditions. Interface technicians can also be authorised to access practice computer systems using secure encrypted connections.

The primary aim for all services is to enhance patient care or to benefit the NHS and maintain patient care.

Step two: Information flows

Interface pharmacists work within GP practices and secondary care settings.

Personal data is processed as well as patient health data, which is a special category of data as defined by the GDPR.

Step three: What legal condition for using the personal data is being relied upon?

Interface accesses patient data as a Data Processor under a signed contract with the healthcare organisation, the Data Controller.

[1] GDPR Articles 35, 36 and 83

Step four: Explain how subject rights to the use of their personal data will be addressed (where applicable)

All requests to exercise subject rights are directed to the healthcare organisation, as Interface does not retain patient identifiable data.

Step five: Who will have access to the personal data?

Only authorised Interface staff (pharmacists or technicians) will access the personal data.

Interface does not use third party data processors.

Step six: What organisational controls will be in place to protect the personal data?

Interface is an NHS Business Partner and meets the same Information Governance requirements as NHS organisations. This is demonstrated through self-assessment in the NHS Data Security and Protection Toolkit[2].

All staff complete the NHS IG training on induction and annually thereafter and must achieve at least 80% to pass each assessment.

The company has robust policies covering data protection and confidentiality, information security, records management and confidentiality for the use of NHS Smartcards. We also follow the NHS requirements for reporting security events and incidents.

No patient identifiable data is transferred into Interface systems.

Step seven: What technical controls will be in place to protect the personal data?

Our internal servers are protected by a managed firewall, secure settings, access controls, virus and malware protection and by keeping devices and software up to date in accordance in accordance with the Data Security and Protection Toolkit.

Interface obtained Cyber Essentials[3] certification in February 2018. Cyber Essentials is a Government backed scheme that helps protect organisations against common cyber-attacks.

[2] https://www.igt.hscic.gov.uk/Home.aspx and https://www.dsptoolkit.nhs.uk/

[3] https://www.cyberessentials.ncsc.gov.uk/

Step eight: What level of risk has been identified in relation to the data protection principles?

Interface advises healthcare organisations to update their privacy notices to reflect this data processing to mitigate any transparency risks

Interface follows NHS information governance policies and trains staff comprehensively in data protection and confidentiality to minimise the risks to privacy and security.

No other risks have ben identified.

Step nine: Consultation requirements

This privacy impact assessment has been produced by the company Data Protection Officer and signed off by the Caldicott Guardian and Senior Information Risk Owner.

No risks have been identified that require consultation with the supervisory authority.