Data Protection Impact Assessment for the Use of IGPR Software for Redaction of Subject Access Requests and Other Reports

Date of Assessment

07/07/2025

Data Protection Officer

- **Name**: Practice Manager / Designated DPO, Highfield surgery
- **Contact Information**: blackpool.highfieldenquiries@nhs.net

Overview of the Project

This Data Protection Impact Assessment (DPIA) concerns the implementation and use of IGPR (Information Governance and Patient Records) software at Highfield surgery. The primary purpose of this software is to facilitate the efficient and compliant redaction of sensitive and third-party information from Subject Access Requests (SARS) and other reports (e.g., medical reports for insurance, solicitors, or other third-party requests) prior to their disclosure. This project aims to enhance data protection compliance, streamline information disclosure processes, and mitigate risks associated with manual redaction, thereby ensuring the practice meets its legal obligations under the UK GDPR and Data Protection Act 2018 while upholding individuals' rights.

Description of Data Processing

- **Nature of Processing**: The processing involves the systematic review, identification, and redaction of specific personal data within existing patient health records and other related documents. This includes the creation of a redacted version of the original record for disclosure, while the original record remains intact.
- **Scope of Processing**: The processing encompasses all patient health records and associated administrative documents that are subject to a Subject Access Request or other legitimate requests for disclosure requiring redaction. This will affect data for patients of Highfield surgery who have submitted such requests or whose records are part of a third-party request.
- **Context of Processing**: Data is accessed and processed by authorised administrative and clinical staff (e.g., Practice Manager, DPO support, designated administrative staff) who have been specifically trained in the use of the IGPR software and data protection principles. The processing occurs within the secure IT environment of Highfield surgery, with the software running on secure workstations. The redacted documents are then securely shared with the requesting individual or authorised third party.
- **Purposes of Processing**: The primary purposes of this processing are:
    - To fulfil the legal obligation to provide individuals with access to their personal data (Subject Access Requests) in a timely and compliant manner.
    - To ensure that personal data of third parties, or other information exempt from disclosure (e.g., information likely to cause serious harm, confidential references), is appropriately protected and not inadvertently disclosed.

- To maintain the accuracy, confidentiality, and integrity of patient records during the disclosure process.
- To streamline and improve the efficiency of the redaction process, reducing the risk of human error associated with manual redaction.

Consultation Process

Consultations have been undertaken with key stakeholders within Highfield surgery, including the Practice Manager, the designated Data Protection Officer (DPO) support, and administrative staff involved in handling SARs and information disclosure. Training on the use of the IGPR software and data protection principles will be provided to all relevant staff. Consideration has been given to guidance from the Information Commissioner's Office (ICO) and NHS Digital regarding data sharing and subject access rights. Internal IT support has been consulted regarding the secure implementation and maintenance of the software.

Necessity and Proportionality

The use of dedicated IGPR software for redaction is considered necessary and proportionate to achieve the stated objectives. Manual redaction is time-consuming, prone to human error, and poses a significant risk of inadvertent disclosure of sensitive or third-party data. The software provides a systematic, auditable, and more secure method for identifying and redacting information. This ensures that the practice can meet its legal obligations under data protection law to provide access to personal data (necessity) while simultaneously protecting the rights and freedoms of other individuals and maintaining confidentiality where legally required (proportionality). It allows the practice to process a potentially large volume of data efficiently while mitigating significant data breach risks.

Risk Assessment

The following potential risks to data subjects' rights and freedoms have been identified:

- **Risk of Incomplete or Incorrect Redaction**: Despite using software, human error in identifying or confirming redactions could lead to inadvertent disclosure of sensitive patient data or third-party information.
- **Software Vulnerabilities**: Potential for technical vulnerabilities in the IGPR software that could be exploited, leading to unauthorised access or data breaches.
- **Unauthorised Access to Redacted Documents**: Redacted documents, if not handled securely after processing, could still be accessed by unauthorised individuals.
- **Integrity of Original Records**: While the software creates a copy, any malfunction or misuse could theoretically impact the integrity of original, unredacted records, though this is mitigated by strict access controls to the core patient record system.
- **Over-Redaction**: Incorrect configuration or excessive caution could lead to over-redaction, potentially denying data subjects access to information they are entitled to receive.
- **Audit Trail Failures**: Inadequate logging or audit trails within the software could hinder accountability and traceability in the event of an incident.

Measures to Address Risks

The following measures and safeguards are implemented to mitigate the identified risks:

- **Staff Training**: Comprehensive and mandatory training for all staff using the IGPR software on its proper use, data protection principles, and the specific rules around redaction (what to redact and why).
- **Access Controls**: Strict role-based access controls to the IGPR software, ensuring only authorised and trained personnel can access and use it. Access to original patient records remains separate and highly restricted.
- **Secure Environment**: The software operates within Highfield surgery's secure IT infrastructure, protected by firewalls, anti-virus software, and regular security updates.
- **Quality Assurance (QA) Process**: Implementation of a robust QA process where redacted documents are reviewed by a second, trained staff member (e.g., Practice Manager or DPO support) before final disclosure.
- **Software Updates and Maintenance**: Regular updates and patches for the IGPR software as provided by the vendor to address security vulnerabilities and ensure optimal performance.
- **Audit Trails**: Utilisation of the software's built-in audit trail features to log all redaction activities, including who performed the redaction, when, and on which documents.
- **Secure Storage and Transmission**: Redacted documents are stored securely (encrypted if possible) and transmitted via secure methods (e.g., encrypted email, secure portal, or recorded delivery) to the requesting party.
- **Vendor Due Diligence**: Due diligence performed on the IGPR software vendor to ensure their compliance with data protection standards and their commitment to security.

Compliance with Data Protection Principles

- **Lawfulness, Fairness, and Transparency**: Processing is lawful based on a legal obligation (Article 6(1)(c) UK GDPR) and the vital interests of the data subject or legitimate interests of the practice (Article 9(2)(h) for health data processed for management of health services). The process is fair, aiming to balance the data subject's right of access with the rights of third parties. Transparency is maintained through privacy notices informing patients of their rights, including SARs.
- **Purpose Limitation**: Data is processed solely for the legitimate purpose of fulfilling SARs and other disclosure requests, specifically for redaction to comply with legal obligations.
- **Data Minimisation**: The software facilitates the precise redaction of only the necessary information (e.g., third-party data, exempt information), ensuring that only relevant and disclosable data is shared.
- **Accuracy**: The software aids in ensuring the accuracy of the disclosed information by preserving the core record while accurately redacting specific parts.
- **Storage Limitation**: Original records are retained according to NHS retention schedules. Redacted copies are retained only for as long as necessary for audit purposes or potential legal challenge related to the disclosure, typically in line with the retention period of the original SAR request documentation (e.g., 6 years for legal defence).

- **Integrity and Confidentiality (Security)**: Robust technical and organisational measures, including secure software, access controls, training, and QA processes, are in place to ensure the integrity and confidentiality of the data throughout the redaction and disclosure process.
- **Accountability**: Documentation of this DPIA, internal policies, audit trails, and staff training demonstrate the practice's commitment to accountability under the UK GDPR.

Data Retention

Original patient records are retained in accordance with the NHS Records Management Code of Practice. The redacted versions of documents created by the IGPR software are retained only as long as necessary for the purpose for which they were created (i.e., to fulfil the SAR or disclosure request) and for audit or dispute resolution purposes. Typically, a copy of the redacted disclosure, alongside the SAR request and any related correspondence, will be retained for a period of six years from the date of disclosure, to address any potential legal challenges or complaints. After this period, they will be securely disposed of.

Data Subjects' Rights

Highfield surgery fully upholds the rights of data subjects. The use of IGPR software directly supports the **right of access** by enabling the practice to fulfil SARs efficiently and compliantly.

- **Right to Access**: Individuals can submit Subject Access Requests (SARs) via various channels (written, email, in-person). The practice’s privacy notice details how to make an SAR. The IGPR software facilitates the accurate and timely provision of this information.
- **Right to Rectification**: If a data subject identifies inaccuracies in their health record, the practice has a clear procedure for rectification. While the IGPR software deals with redaction for disclosure, it does not alter original records, which remain subject to rectification requests.
- **Right to Erasure/Restriction**: These rights are subject to specific conditions, especially within a healthcare setting due to legal obligations for record keeping. Any requests for erasure or restriction are handled on a case-by-case basis in line with UK GDPR and DPA 2018 guidance.
- **Right to Object**: Data subjects have the right to object to processing in certain circumstances. This right is handled in accordance with the practice’s data protection policy.