****

**Data Protection Impact Assessment Questionnaire**

**Version 5**

Information Governance Team

January 2019

**Do I Need to Complete a DPIA questionnaire?**

No

Are you implementing a new system or service or changing the way you work?

No need to conduct a full DPIA.

Complete the screening questions and note why a full DPIA is not required.

Yes

Does this project involved the collection, recording, storing or processing of person-confidential or business sensitive data?

No

Yes

Document in the business case and/or project documentation.

Complete a DPIA questionnaire.

You may be asked to provide supporting information e.g. contract, system specification, consent forms

When deciding whether a DPIA questionnaire is required, if the first answer is ‘yes’, but the second response is ‘unsure’, please complete the questions in section 1 of the DPIA questionnaire to assist the decision. Further guidance can be sought from the Information Governance Team: [nelcsu.Information-Governance@nhs.net](mailto:nelcsu.Information-Governance@nhs.net).

It is a requirement of the General Data Protection Regulations that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

If you are assessing a system and it does not have a DPIA, including one that identifies that a full DPIA is not required, please complete the relevant section of this questionnaire.

The questionnaire will be reviewed by the stakeholders, including the IG Lead and the recommendation from the questionnaire will be notified to the Director (Information Asset Owner). The recommendation will be either:

* + 1. A full DPIA is required where the new process or change of use of PCD requires more thorough investigation.
    2. The DPIA questionnaire will be signed off by the Information Asset Owner/SIRO and the DPIA log updated by the IG Lead.

There is an Information Security Procurement Questionnaire (for use in the commissioning process for new information systems) available via the IG Team and on SUSI, an Information Risk Questionnaire template and an ICT System Security Risk Assessment available to assist in assessing the risks (embedded in this questionnaire).

1. **Project/service stakeholder information**

|  |  |
| --- | --- |
| Project/Service Lead contact details | |
| Your location | Tarlochan Boparai |
| Your telephone number | 07798858853 |
| Your email address | tarlochan.boparai2@nhs.net |
| Your team | Digital First Primary Care Programme |
| Your directorate |  |
| Information Asset Owner  (if different from above) | GP Practice |

|  |  |
| --- | --- |
| Purpose of the Project/Service | |
| Project/Service Name | Deployment of Edenbridge Healthcare Limited’s APEX workload analysis and workforce planning software to all GP Practices, Extended Access Hubs, Urgent Treatment Centres and Primary Care Networks in East Kent. |
| In brief, what is the purpose of the project/service and how is the processing of information necessary to that work?  Please include expected outcomes. | Edenbridge APEX will provide a comprehensive workload and workforce transformation service to all GP Practices, Extended Access Hubs, Urgent Treatment Centres and Primary Care Networks in East Kent. The Apex Analytical tool is intended to be used with de-identified data in a web-based portal for extracting KPI performance data for the Practices. APEX provides GP Practices and primary care providers with a detailed and factual understanding of the nature of their workload, the types of patient activity they have experienced and how their workforce has managed that activity. Practices use this improved understanding to consider how they can better respond to their patients' needs, improve quality and access to services and explore how more efficient use of clinical resources, in particular, may improve their workforce capacity and the Primary Care experience of both patients and their workforce. In addition, APEX also performs numerous local administrative functions.   * Capacity and demand management * Ability to track performance against local and national targets * Local audit * Service evaluation * Submissions of data for commissioning purposes   The de-identified data, including medical history and treatment dates, are essential for providing these services and to help support and inform how patient care can be improved and delivered based on continuous service improvement. This requires the ability to look back at trends and review the impact of service change, limiting the data restricts the ability for this to be done.  The **Hashed NHS Number and Hashed Local Patient Number** are requiredto provide context within the data. Hashing is a one-way process and the resulting hash values cannot be reversed. |

|  |  |
| --- | --- |
| Timeframe for the Project/Service | |
| When is the Project/Service due to begin? If it’s time limited, please note the expected end/review date. | The deployment of APEX to GP Practices will commence from April 2020 and once the software is deployed this will be reviewed on an annual Software as a Service (SaaS) contract basis. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nature of the information | | | | |
| Will all of the information be truly anonymised information[[1]](#footnote-2)?  Anonymised data must meet [the ICO code of practice](https://icosearch.ico.org.uk/s/redirect?collection=ico-meta&url=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F1061%2Fanonymisation-code.pdf&index_url=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F1061%2Fanonymisation-code.pdf&auth=mDAlWp%2BBK%2B03Se03OnHpRQ&profile=_default&rank=3&query=anonymisation). | Nn |  | No – some of the information will relate to an identified or an identifiable person (either directly or indirectly) |  |
| Will the information be new information as opposed to using existing information in different ways? | | | All information within APEX is processed via the Principal Clinical System environment, namely EMIS Web, so all of information processed is already accessible to end user in a fully identifiable state. All patient related data held in APEX is de-identified through pseudonymisation. | |

|  |  |
| --- | --- |
| **Key Contacts** | |
| Key Stakeholder Names & Roles: | Ben Hampshire | Technical Support | Edenbridge Healthcare Limited |
| Date: | 16/04/2020 |

| **Screening Questions** | **YES or NO** |
| --- | --- |
| Will the project involve the collection of information about individuals? | YES |
| Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business? | NO |
| Will the project compel individuals to provide information about themselves? | NO |
| Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | NO |
| Are you using **personal data/special category data** about individuals for a new purpose or in a new way that is different from any existing use? | YES |
| Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make an automated decision about care. | NO |
| Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services | YES |
| Will the project result in you making decisions about individuals in ways which may have a significant impact on identifiable individuals? i.e. does the project change the delivery of direct care.  **N.B.** If the project is using anonymised/pseudonymised data **only**, the response to this question is “**No**”. | NO |
| Will the project require you to contact individuals in ways which they may find intrusive? | NO |
| Does the project involve multiple organisations, whether they are public sector agencies accessing **personal data/special category data** i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners? | NO |
| Does the project involve new or significantly changed handling of a considerable amount of **personal data/special category data** about each individual? | NO |
| Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources? | NO |

If any of the screening questions have been answered “YES”, then please continue with the full Data Protection Impact Assessment Questionnaire (below).

If all questions are “NO”, please return the document to the Information Governance Team and **do not** complete the full Data Protection Impact Assessment.

Please email the completed screening to [nelcsu.Information-Governance@nhs.net](mailto:nelcsu.Information-Governance@nhs.net)

1. **Controller/s[[2]](#footnote-3) and Processors[[3]](#footnote-4)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Are multiple organisations involved in processing the data?** *If yes, list below and clearly identify where there is a lead Commissioner or Controller.* | | | | Yes/No |
| Yes |
| Name of Organisation | Controller or Processor? | | | Completed and compliant with the DSP Toolkit[[4]](#footnote-5) |
| Yes/No |
| East Kent GP Practices | Controller | | | See “DSPT compliance April 2020.xls” |
| East Kent Primary Care Network | Controller | | | See “DSPT compliance April 2020.xls” |
| East Kent Extended Access Hub | Controller | | | See “DSPT compliance April 2020.xls” |
| Ashford Clinical Commissioning Group | Controller | | | Yes |
| Canterbury and Coastal Clinical Commissioning Group | Controller | | | Yes |
| South Kent Coast Clinical Commissioning Group | Controller | | | Yes |
| Thanet Clinical Commissioning Group | Controller | | | Yes |
| Ashford UTC - East Kent Hospitals University NHS Foundation Trust in partnership with Invicta CIC, IC24, Thanet CIC, Ashford Clinical Providers | Controller | | | TBA once “live” |
| Canterbury UTC - East Kent Hospitals University NHS Foundation Trust in partnership with Invicta CIC, IC24, Thanet CIC, Ashford Clinical Providers | Controller | | | TBA once “live” |
| Deal UTC - Kent Community Health NHS Foundation Trust contract holder in partnership with Channel Health Alliance | Controller | | | TBA once “live” |
| Dover UTC - East Kent Hospitals University NHS Foundation Trust in partnership with Invicta CIC, Integrated Care 24 Ltd (IC24) CIC, Thanet CIC, Ashford Clinical Providers | Controller | | | TBA once “live” |
| Estuary View UTC - Whitstable Medical Practice | Controller | | | TBA once “live” |
| Folkestone UTC - Kent Community Health NHS Foundation Trust contract holder in partnership with Channel Health Alliance | Controller | | | TBA once “live” |
| Faversham UTC - Faversham Medical Practice | Controller | | | TBA once “live” |
| Herne Bay UTC - Herne Bay Integrated Care Limited Community of Interest Company (CIC) (company formed through alliance of Heron and Park Medical Practices) | Controller | | | TBA once “live” |
| Margate UTC - East Kent Hospitals University NHS Foundation Trust in partnership with Invicta CIC, IC24, Thanet CIC, Ashford Clinical Providers |  | | | TBA once “live” |
| Edenbridge Healthcare Limited | Processor | | | YES |
| **Has a data flow mapping exercise been undertaken?**  *If yes, please provide a copy, if no, please ensure this is completed – speak to the IG Team for guidance* | | | | Yes/No |
| YES |
| **Is Mandatory Staff Training in place for the following?** | | Yes/No | Dates | |
| * Data Collection: | | N/A |  | |
| * Use of the System or Service: | | Yes | UTCs utilising EMIS Web clinical system should make a training guide/summary available to system users. | |
| * Collecting Consent: | | NO |  | |
| * Information Governance: | | Yes | Annual | |

1. **Personal data[[5]](#footnote-6)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Use of personal information** | | | | |
| Why would it not be possible to do without personal data? | The specified data, including de-identified medical history and treatment dates, are essential for providing these services and to help support and inform how patient care can be improved and delivered based on continuous service improvement. This requires the ability to look back at trends and review the impact of service change, limiting the data restricts the ability for this to be done. This justification is provided in reference to the medical history processing as the reduction or limitation of this will impact the ability to analyse trends. | | | |
| Please confirm that you will be using only the minimum amount of personal data that is necessary. | No identifiable patient information is used, only de-identified. All patient data is processed in a pseudonymised form as per the Clinical System to APEX Data Flows documentation outlined above. To reiterate as per the Data Flows documentation above, the only personal data processed is the name and job role of the healthcare professional as registered in the Clinical System. | | | |
| Would it be possible for the Controller/s to use pseudonymised[[6]](#footnote-7) data for any element of the processing? | Yes |  | No |  |
| If Yes, please specify the element(s) and describe the pseudonymisation technique(s) that you are proposing to use and how you will prevent any re-identification of individuals.  (If you will be using the NEL pseudonymisation tool, simply enter: “NEL pseudonymisation tool”, no further information is required). | All patient related data held in APEX is de-identified through pseudonymisation. The pseudonymisation process is performed within the Principle Clinical System environment. All directly identifiable fields are either removed (e.g. patient name), abbreviated (e.g. date of birth is abbreviated to year of birth) or hashed (e.g. NHS Number). All fields that may contain free text entered within the clinical system are removed. Data marked as Sensitive or whole records marked as confidential are removed.  The pseudonymisation process uses an open source standard created by The University of Nottingham called *OpenPseudonymiser*, full details are available online at www.openpseudonymiser.org. This is a one-way encryption/hashing process that cannot be reversed.  No key/mapping tables are built, maintained or stored which would allow a data subject to be reidentified. | | | |

|  |
| --- |
| **HEALTHCARE PROFESSIONAL & APEX END USER Description of data: National and local data flows containing personal and identifiable personal information.** What are the required personal data items? |

|  |  |  |  |
| --- | --- | --- | --- |
| **Personal Data** | **Please tick all that apply** | **Special Category Data** | **Please tick all that apply** |
| Name |  | Racial / ethnic origin |  |
| Address (home or business) |  | Political opinions |  |
| Postcode |  | Religious beliefs |  |
| NHS No |  | Trade union membership |  |
| Email address |  | Physical or mental health |  |
| Date of birth |  | Sexual life |  |
| Payroll number |  | Criminal offences |  |
| Driving Licence [shows date of birth and first part of surname] |  | Biometrics; DNA profile, fingerprints |  |
| Please supply a dummy sample, e.g. blank forms or an itemised list of the data items. | | Bank, financial or credit card details |  |
| Mother’s maiden name |  |
| National Insurance number |  |
| Tax, benefit or pension Records |  |
| Health, adoption, employment, school, Social Services, housing records |  |
| Child Protection |  |
| Safeguarding Adults |  |
| Additional data types (if relevant) | | * Job Category | |

|  |
| --- |
| **PATIENT DATA Description of data: National and local data flows containing personal and identifiable personal information.** What are the required personal data items? |

|  |  |  |  |
| --- | --- | --- | --- |
| **Personal Data** | **Please tick all that apply** | **Special Category Data** | **Please tick all that apply** |
| Name |  | Racial / ethnic origin |  |
| Address (home or business) |  | Political opinions |  |
| Postcode |  | Religious beliefs |  |
| NHS No |  | Trade union membership |  |
| Email address |  | Physical or mental health |  |
| Date of birth |  | Sexual life |  |
| Payroll number |  | Criminal offences |  |
| Driving Licence [shows date of birth and first part of surname] |  | Biometrics; DNA profile, fingerprints |  |
| Please supply a dummy sample, e.g. blank forms or an itemised list of the data items. | | Bank, financial or credit card details |  |
| Mother’s maiden name |  |
| National Insurance number |  |
| Tax, benefit or pension Records |  |
| Health, adoption, employment, school, Social Services, housing records |  |
| Child Protection |  |
| Safeguarding Adults |  |
| Additional data types (if relevant) | | * Gender * GP * Medical History * Treatment Dates/ Diagnosis * Year of Birth * Year of Death * Postcode District (First part of postcode, e.g. LS1) * Registration Status and Date * Appointments (Date, Time, Session Holder, DNA etc.) * Hashed NHS Number * Hashed Local Patient Number | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lawfulness of the processing** | | | | | |
| **Conditions for processing for special categories: to be identified as whether they apply** | | | | | |
| **Condition** | **Please tick all that apply** | | | | |
| Explicit consent unless or allowed by other legal route | | Explicit consent |  | Other legal route |  |
| Processing is required by law | | | | |  |
| Processing is required to protect the vital interests of the person | | | | |  |
| Processing is necessary for the performance of a contract | | | | |  |
| Processing is necessary to perform a a task in the public interest | | | | |  |
| Processing is necessary for a legitimate interest or the legitimate interests of a third party | | | | |  |
| Is any processing going to be by a not for profit organisation, e.g. a Charity | | | | |  |
| Would any processing use data already in the public domain? | | | | |  |
| Could the data being processed be required for the defence of a legal claim? | | | | |  |
| Would the data be made available publicly, subject to ensuring no-one can be identified from the data? | | | | |  |
| Is the processing for a medical purpose? | | | | |  |
| Would the data be made available publicly, for public health reasons? | | | | |  |
| Will any of the data being processed be made available for research purposes? | | | | |  |

**The answers will not specifically identify the legality of the data flow; your responses to the questions below need to identify the specific legal route for processing. You will need to identify the legal basis using the GDPR article 6 (for personal data) and article 9 (for special category data) conditions met, as referenced in Chapter 2, section 8 and 10 of the Data Protection Act 2018.**

**The IG Team are available to help you identify the legal route for processing data.**

|  |  |
| --- | --- |
| **Describe the information flows**  The collection, use and deletion of personal data must be documented. | |
| Does any data flow in identifiable form? If so, from which organisation, and to which organisation/s?  Please include a data flow map and confirm the flow has been added to your Information Asset and Data flow register. | No. All patient information’s de-identified at source before flowing in to Apex. See EH-REC-050 - Clinical System to APEX Data Flows on p7. |
| Media used for data flow?  (e.g. email, post, courier, secure electronic means [e.g. SFTP], other – please specify all that will be used) | Data in transit is payload encrypted/cryptographically signed and transmitted over a secure connection.  An external facing FTP server secured with SFTP public key authentication. Access is also restricted by firewall to a single static IP Address provided by Edenbridge Healthcare.  Files stored in de-identified encrypted format using the PGP protocol.  Once the files have been downloaded and stored into the APEX File Store, they are removed from the SFTP server. |

| **Answer all the questions below for the processing of Personal Confidential Data** | |
| --- | --- |
| What is the legal basis for the processing of identifiable data? Please identify the conditions under the Data Protection Act 2018 or the Section 251 approval under the NHS Act 2006– please include the approval reference number.  (See Appendix 1 for Legal basis under the Data Protection Legislation)  Please include a copy of your consent form and identify when and how will this be obtained and recorded? [[7]](#footnote-8) | Public task: GDPR Article 6 (e) ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’  Special categories of personal data (sensitive data), *if applicable:*  Medical related: GDPR Article 9 (h) ‘provision of health or social care or treatment or the management of health or social care systems and services’ |
| Where and how will this data be stored? | De-identified data is stored using an encrypted-at-rest model in the APEX Data Centre. This is a secure environment with restricted access to authorised Edenbridge staff. Services are hosted in a UK data centre, hosted at Microsoft Azure UK South, which complies with the ISO: IEC 27001 standard and has been awarded an accreditation to host and process IL2 and OFFICIAL data, assured against the UK G- Cloud 14 Cloud Security Principles. |
| Who will be able to access identifiable data? | All members of the GP Practice team, Extended Access Hubs, Urgent Treatment Centres, Primary Care Networks and Clinical Commissioning Groups can be granted access to the APEX system. This is agreed and set up by each practice individually depending on their local practice requirements and how the practice intend to use the system. This is decided on a practice by practice basis depending on the local landscape and internal way of working.  Individuals are granted access by a system administrator at that healthcare organisation and can only see data visible to that organisation and with role-based permissions configured for them. Identifiable data only relates to healthcare professionals registered in the Principal Clinical System and APEX end users. All patient related data held in APEX is de-identified through pseudonymisation. |
| How will you ensure the accuracy of the personal data (including their rectification or erasure where necessary)? | APEX processes data directly from the Principal Clinical System on behalf the Primary Care Organisation so any amends or removal of information would be completed via the Principal Clinical System environment, with changes then reflected in APEX. |
| How will you monitor and maintain the quality of the personal data? | APEX processes data directly from the Principal Clinical System on behalf the Primary Care Organisation so any amends or removal of information would be completed via the Principal Clinical System environment, with changes then reflected in APEX. |
| Will the data be linked with any other data collections? | APEX does not complete any data linking. |
| How will this linkage be achieved? | N/A |
| Is there a legal basis for these linkages? i.e. is the Controller/s responsible for the data expected to co-operate/link data to carry out their legal obligations. | N/A |
| How have you ensured that the right to data portability can be respected? i.e. Data relating to particular people can be extracted for transfer to another Controller, at the request of the person to which it relates, subject to:   * Receipt of written instructions from the person to which the data relates. * Including data used for any automated processing,   And  The transfer of the data has been made technically feasible.  **N.B.** Transferable data does not include any data that is in the public domain at the time of the request.  No data that may affect the rights of someone other than the person making the request can be included. | The right to data portability does not apply in this circumstance. Consent is not the legal basis for processing and neither is the processing by automated means. |
| What security measures will be used when the data is in transit? | All data in transit is encrypted using either HTTPS (TLS) or SFTP. In addition to the communication security provided by TLS or SFTP, data payloads are also encrypted using PGP for data extracted by the EMIS Extract Service and 256-bit AES encryption for data extracted by the EMIS Web API. |
| What confidentiality and security measures will be used to store the data? | Data in transit is payload encrypted/cryptographically signed and transmitted over a secure connection.  Aggregated and pseudonymised data is stored using an encrypted-at-rest model in the APEX Data Centre. This is a secure environment with restricted access to authorised Edenbridge staff. Services are hosted in a UK data centre which complies with the ISO: IEC 27001 standard and has been awarded an accreditation to host and process IL2 and OFFICIAL data, assured against the UK G- Cloud 14 Cloud Security Principles. |
| How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed? | The processing duration will be for the period of the SaaS License deployed to each healthcare organisation. Once the processing period has expired or in the event that the agreement is terminated, all Data and Personal data remains the property of the Controller and shall be either returned or destroyed by the Processor within a three-month period post contract. We could however instigate this immediately post contract if requested by the Data Controller.  The Principal Clinical System remains the source of all data processed by APEX so remains fully available to the Data Controller, but is able to be returned securely in line with the General Data Protection Regulation before being destroyed in line with the Edenbridge Healthcare Limited Data Destruction Policy and Microsoft Azure guidelines, available at: <https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data>  The GP practice has a statutory obligation to undertake service evaluation and local audit, this may include data related to ‘deceased’ or ‘left’ patients. APEX will continue to process data for ‘deceased’ or ‘left’ patients for a period of 12 months. This is to provide accurate local audit and service evaluation. Following this period all data relating to the deceased’ or ‘left’ patient is removed. |
| What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis? | APEX does not process any identifiable data outside of the Primary Care Organisation context. The Primary Care Organisation always remains the Controller as outlined in the APEX Data Processing Agreement. |
| Please confirm you have a System Level Security Policy (SLSP) for the project/service.  This policy needs to identify the technical controls that enable you to demonstrate that you have ensured privacy by design has been addressed by ensuring you have information on the controls required to protect the data. | Edenbridge Healthcare has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.  The data protection impact assessment will include:   * Consideration of how personal data will be processed and for what purposes * Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s) * Assessment of the risks to individuals in processing the personal data * What controls are necessary to address the identified risks and demonstrate compliance with legislation   Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate. |
| If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA?  Is there functionality to respect objections/ withdrawals of consent? | The APEX Data Processing Agreement attached below fully outline the General Data Protection Regulation compliance in relation to Subject Access Requests.  APEX only holds personal identifiable data in relation to user data. |
| Are there any plans to allow the information to be used elsewhere either in the NEL, wider NHS or by a third party? | N/A |
| Will the privacy notices in relation to this data be updated and ensure it includes:   * ID of controller * Legal basis for the processing * Categories of personal data * Recipients, sources or categories of recipients of the data: any sharing or transfers of the data (including to other countries) * Any automated decision making * Retention period for the personal data * Existence of data subject rights, including access to their data and/or withdrawal of consent and data portability | Edenbridge Healthcare Limited does supply all Primary Care Organisations with a sample GP Privacy Notice as attached below to use as a baseline or to use in addition to current Privacy Notices. |
| Where consent is the legal basis/there is automated processing. The data must be able to be easily separated from other datasets to enable data portability (see previous questions), audit of data relating to specific organisations and to facilitate any requirements for service transitions.  Please describe how you will meet this requirement. | N/A |

1. **Access and reporting**

|  |  |  |
| --- | --- | --- |
| What access controls will you have in place to ensure there is only authorised access to the location the data is stored? Please include your procedure for enabling, monitoring access and identifying any inappropriate access. | | |
| Access to APEX and user account creation is controlled by an administrator within the practice. The APEX team only have access to the product for the provision of support and training as per the SaaS License agreement. In certain circumstances Edenbridge Healthcare’s operations staff, who have all completed data security training through the organisation’s DSP Toolkit Accreditation, may need to access personal information in order to diagnose a system issue. Access to the production system is strictly controlled and audited through Identity Access Management (IAM) and Role Based Access Control (RBAC). Only authorised personnel, with appropriate security training, can access data held in Production systems and they may only do so if they have legitimate reason. | | |
| **Are there any new or additional reporting requirements from the system/software being used for this project/service?**  **If “No” move to section 5 below: Business Continuity planning** | |  |
| No |
| What roles will be able to run reports? E.g. service activity reports, reports on individual people. | | |
| None | | |
| What roles will receive the report or where will it be published? | | |
| N/A | | |
| Will the reports be in person-identifiable, pseudonymised or anonymised format? | | |
| N/A | | |
| Will the reports be in sensitive or redacted format (removing anything which is sensitive) format? | | |
| N/A | | |
| If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of? | Yes/No | |
| N/A | |
| What plans are in place in relation to the internal reporting of a personal data breach?  (NB Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual(s), it will normally need to be reported to the ICO within 72 hours.) | | |
|  | | |
| What plans are in place in relation to the notification of data subjects should there be a personal data breach?  (NB Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s), they should be notified as soon as reasonably feasible and provided with any recommendations to mitigate potential adverse effects.) | | |
|  | | |

1. **Business continuity planning**

|  |  |
| --- | --- |
| How will the personal data be restored in a timely manner in the event of a physical or technical incident? | Edenbridge Healthcare Information Security Continuity Plan is produced by Edenbridge Healthcare Senior Management Team and reflects considered plans that ensure information security continuity in the event of any of the occurrences identified in the Information Security Continuity Risk Assessment process. All critical information security processes are identified in the plan, together with the responsibilities for restoration of service in the event of a continuity event.  The plan identifies the extent – for each of the critical services – to which service interruption is allowed before the continuity plan is invoked.  Information security continuity plans are verified, reviewed and evaluated in accordance with our internal audit and review procedures.  In the event of any physical or technical the Principal Clinical System remains the authoritative source of information and where necessary can be reextracted from the Principal Clinical System to APEX. |

1. **Direct marketing[[8]](#footnote-9)**

|  |  |  |
| --- | --- | --- |
| Will any personal data be processed for direct marketing purposes? |  | No |
| If Yes, please describe how the proposed direct marketing will take place: | N/A | |

1. **Automated processing**

|  |  |  |
| --- | --- | --- |
| Will the processing result in a decision being made about the data subject solely because of automated processing[[9]](#footnote-10) (including profiling[[10]](#footnote-11))? |  | No |
| If Yes, is the decision:   * necessary for entering into, or performance of, a contract between the data subject and a data controller * authorised by law * based on the data subject’s explicit consent? | N/A | |
| Please describe the logic involved in any automated decision-making. |  | |

1. **Risk Management and action plan**

The risk score will determine the level of authorisation needed for any DPIA completed that requires a full DPIA. Any risk score that is verified by the IG team to be in the upper range of a medium risk score (9 to 12) or in the range of high risk will require referral to the NEL Data Protection Officer for review and approval. Any DPIA risks that score as high risk will only have the processing of the data approved once the risk has either mitigated to reduce the risk to medium as a minimum or where this is not possible, a high-risk score will require escalation to NHS England and approval from the Information Commissioner’s Office before any processing can commence. The escalation process also includes a review to enable the risk to be lowered to within tolerance, if possible. The table below identifies the ranges for the scores and the risk level associated with each range of scores.

|  |  |
| --- | --- |
| Risk level | Score |
| Low Risk | 1 to 6 |
| Medium | 7 to 12 |
| High | 13 to 25 |

The risk assessment tool used is dependent on the data processed and the source of the risk involved. There is an information asset risk scoring tool available, a security risk assessment tool is available where the ICT infrastructure poses the highest risk. If the dependency of the service/project is strongly linked to a particular service with its own risk scoring tool, such as Clinical Services, then that tool will be used to assess the risk and include the information asset risk score as a factor to the assessment.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Data Protection Risks**  List any identified risks to Data Protection and personal information of which the project is currently aware.  Risks should also be included on the project risk register. | | | | | | |
| **Risk Description**  **(to individuals, to the NEL CSU or to wider compliance)** | **Current Impact** | **Current Likelihood** | **Risk Score (I x L)** | **Proposed Risk solution (Mitigation)** | **Is the risk reduced, transferred, or accepted? Please specify.** | **Evaluation: is the final**  **impact on individuals**  **after implementing each**  **solution a justified,**  **compliant and**  **proportionate response**  **to the aims of the project?** |
| **Data breach of APEX hosted Environment** | Moderate | Rare | Very Low | All Patient Data is De-identified  All staff have IG training. Data access is limited to technical support staff only by request only.  APEX environment adheres to standard security regulations.  All data is encrypted at rest.  APEX environment uses threat detection technology.  The APEX Data Centre is a secure environment with restricted access to authorised Edenbridge staff. Services are hosted in a UK data centre which complies with the ISO: IEC 27001 standard and has been awarded an accreditation to host and process IL2 and OFFICIAL data, assured against the UK G- Cloud 14 Cloud Security Principles. | Reduced | Accepted |
| **Data breach while transporting data to APEX environment** | Moderate | Rare | Very Low | All channels are secured with either HTTPS (TLS) or SFTP.  Data content is additionally encrypted. | Reduced | Accepted |
| **Pseudonymisation software compromised**  Persons with malicious intent may be able to call the EMIS API | Moderate | Rare | Very Low |  | Accepted | Accepted |
| **Bug in pseudonymisation software** | Moderate | Rare | Very Low | Software fully tested. Any new fields added by supplier will cause the software to abort. | Reduced | Accepted |
| **Apex website compromised** | Moderate | Unlikely | Low Risk | Website uses HTTPS communication and current browser standards.  Password minimum strength, hashing and user disabling algorithms.    APEX environment uses threat detection technology.  External independent penetration tested. | Reduced | Accepted |

|  |  |  |  |
| --- | --- | --- | --- |
| Approval by IG Team/Information Security | | | |
| Risk Description | Approved solution | Approved by | Date of approval |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Actions to be taken** | | |
| **Action to be taken** | **Date of Completion** | **Action Owner** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Conclusions**

|  |
| --- |
| **Consultation requirements**  Part of any project is consultation with stakeholders and other parties. In addition to those indicated “Key information, above”, please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information. Where a lead Commissioner/Controller has been identified that organisation must consult with, capture actions from and gain approval from all collaborating partners.  It is the project/service lead’s responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations. |
|  |

|  |
| --- |
| **Further information/Attachments**  Please provide any further information that will help in determining Data Protection impact.  See Appendix 2, note 5 for examples |
|  |

|  |
| --- |
| **IG Team comments:** |
| The DPIA has been reviewed and no significant IG risks in the process have been identified in relation to personal information as it is di-identified at source before any processing takes place using Apex. The CCG’s SIRO and Caldicott Guardian will need to review and sign off the DPIA. |

Following review of this DPIA by the Information Governance Team, a determination will be made regarding the Data Protection impact and how the impact will be handled. This will fall into three categories:

1. ~~No action is required by IG excepting the logging of the Screening Questions for recording purposes~~.
2. The questionnaire shows use of personal information but in ways that do not need direct IG involvement – IG may ask to be kept updated at key project milestones.
3. ~~The questionnaire shows significant use of personal information requiring IG involvement via a report and/or involvement in the project to ensure compliance.~~

**IG review**

**IG staff name**: Ben Tunmore

**Signature**: 

**Date**: 17/04/2020

Please email entire completed document to [nelcsu.Information-Governance@nhs.net](mailto:nelcsu.Information-Governance@nhs.net)

The Information Asset Owner identified as co-ordinating projects/services involving multiple partners must present the completed DPIA to the management group with oversight of the project/service to obtain their approval before signing on behalf of the partners.

**Information Asset Owner (IAO) approval (for low to medium risk processing)**

**IAO name:**

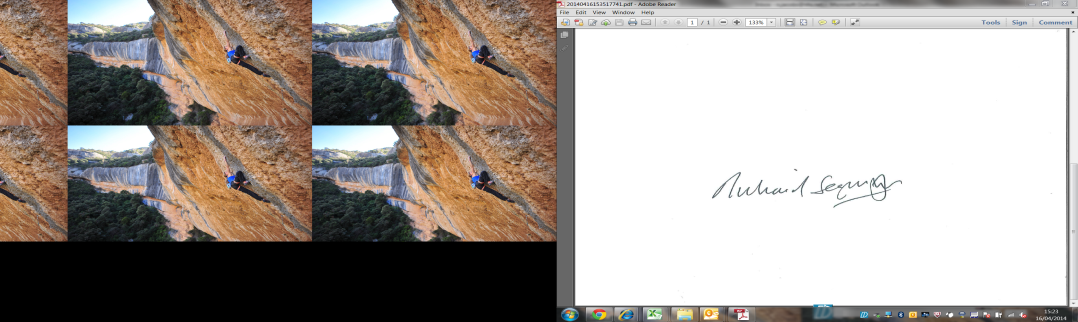
**Signature:**

**Date:**

The lead Commissioner/Controller SIRO is responsible for ensuring all collaborating partner SIROs have approved the DPIA before signing on their behalf (if needed) below. If in doubt, the procurement or project manager must consult with the SIRO from each collaborating partner. Consultations that relate to risk mitigation must be reflected in the action planning section and capture actions and related approvals from all stakeholders, to capture the collaborative view of risks and issues before signing the DPIA below.

**SIRO approval (for high risk processing)**

**SIRO name: Richard Segall Jones**

**Signature:** 

**Date: 4 May 2020**

**Data Protection Officer (DPO) approval (for high risk processing)**

**DPO name: Helen O’Neil**

**Signature:** 

**Date: 4 May 2020**

1. anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable [↑](#footnote-ref-2)
2. 'Controller' means alone or jointly with others, the organisation that determines the purposes and means of the processing of personal data – for example, this is the case where an organisation is obliged by law to carry out a specific function [↑](#footnote-ref-3)
3. ‘Processor’ means alone or jointly with others, the organisation is processing personal data under the instruction of a Controller and **does not** determine the purposes and means of the processing of personal data – for example, NEL is always a Processor [↑](#footnote-ref-4)
4. The [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/) is a self-assessment tool provided by NHS Digital to assess compliance to the 10 National Data Guardian Security Standards. [↑](#footnote-ref-5)
5. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [↑](#footnote-ref-6)
6. 'pseudonymised' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [↑](#footnote-ref-7)
7. See [NHS Confidentiality Code of Practice](https://www.digital.nhs.uk/cop) Annex C for guidance on where consent should be gained. NHS Act 2006 s251 approval is authorised by the National Information Governance Board Ethics and Confidentiality Committee and a reference number should be provided [↑](#footnote-ref-8)
8. direct marketing is “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals” - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations [↑](#footnote-ref-9)
9. examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention [↑](#footnote-ref-10)
10. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements [↑](#footnote-ref-11)