



Data Protection Impact Assessment

What is the name of the project, system or process that this DPIA document relates to?	Eyecare electronic Referral and image sharing To implement an Eyecare electronic Referral System (EeRS) Coventry and Warwickshire.
Key contact name:	Julia Markham
Key contact details – email, landline and mobile	julia.markham2@nhs.net
IG Project No.	N/A
DPO Consulted	26/03/2024
DPO Reviewed	27/03/2024
SIRO Consulted	N/A
SIRO Approval	N/A
Caldicott Consulted	N/A

This questionnaire is a mandatory document requiring completion as part of a project, procuring and implementing a new system or a change in business process for example, to identify any impact on the handling of personal confidential data (PCD) irrespective of whom it relates to, e.g. patients, service users, staff, or third party contractors.

A DPIA should be completed at the beginning of any project or change of process.

*Please note that once completed, it can take time to for approvals and signing off of the DPIA therefore any project/process **SHOULD NOT** be started until all risks have been reviewed and approved as it could put the organisation at risk.

Table of Contents

1. Introduction	3
2. Data Protection Impact Assessment	3
2.1 Contact details	3
2.2 Project/Process Outline	4
2.3 Data Types	6
2.4 Assessment Questions	6
2.5 Appropriate Policy Documents	10
2.6 Procurement / development of data collection system	12
2.7 Data Retention and Disposal	17
2.8 Legal Basis/bases	18
2.9 Common Law Duty of Confidentiality (CLDC)	19
2.10 Third Party Partner Organisations	21
3. DPA 2018 / UK GDPR	23
4. Risks	26
5. Statement of Assessment (completed by IG Leads)	28
6. SIRO or Caldicott Guardian Statement of Assessment – for Full scale Data Protection Impact Assessments only	28
Appendix 1 – High level workflow options considered	31
Appendix 2 – Identification of how to receive booking requests	36
Appendix 3 – Example of high level flow at Shropshire, Telford and Wrekin ICS	37
Appendix 4 – Service Providers Checklist for understanding steps involved in EeRS deployment	38

1. Introduction

This document details the process for conducting a Full Data Protection Impact Assessment (DPIA) and the involvement of Information Governance through a project lifecycle to ensure that, where necessary, personal and sensitive (special category) information requirements are complied with, and risks are identified and mitigated.

2. Data Protection Impact Assessment

2.1 Contact details

Please complete with as much information as possible as this will assist in assessing whether further action is required.

Information Asset/Project Name	Cinapsis referral system/ Eyecare electronic Referral System (EeRS)
Directorate/Department	Transformation - Elective
Organisation	Coventry and Warwickshire ICB
Is this a change to an existing process?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
DPIA form Completed By: <i>If completion is by the IAA, please copy and paste into the IAA section too.</i>	Name: Julia Markham
	Job Title: Transformational Project Manager
	Dept.: Planned care
	Contact No: 07971647309
	Email: julia.markham2@nhs.net
Date completed	21/12/2023
Information Asset Owner(s) <i>The senior person(s) responsible for the system/process – Director/ AD or Senior Manager level</i>	Name: Click or tap here to enter text.
	Job Title: Click or tap here to enter text.
	Dept.: Click or tap here to enter text.
	Contact No: Click or tap here to enter text.
	Email: Click or tap here to enter text.

2.2 Project/Process Outline

Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required.

NHS E Midlands have commissioned Monmedical Ltd t/a Cinapsis (Cinapsis) to provide an Electronic eyecare Referral System (EeRS) across 11 Integrated Care Systems (ICS). Cinapsis provides optometry (Optom) practices with a secure online platform (web and or mobile app) that enables optometrists to submit referrals. Optometrists can include images or supporting files with the referral.

The ICB is to establish Coventry and Warwickshire Ophthalmology Coordination Service (OCS) to manage routine referrals. The OCS will be able to access Cinapsis on the secure platform and are able to review the demographic data and the referral for completeness and appropriacy. The OCS will issue an outcome on the EeRS platform, which will result in a summary outcome letter being returned to the referrer within Cinapsis, as well as to a nominated generic email address (if the practice email address is not NHS.NET, the Optom practice would be required to click on a secure link and log into Cinapsis to access the outcome letter and any PID). If the outcome indicates a booking is required, patients will be phoned and offered a choice of provider and the referral will then be forward to that provider. Cinapsis are able to utilise the Electronic Referral Service (ERS) interface to submit the referral and any data across to the relevant ERS endpoint – e.g. to be retrieved by the Booking Team. Additionally, on raising a referral, the optometrist will be able to select an option to copy the patient's registered practice into the outcome. The GP will then be informed via their designated Message Exchange for Social Care and Health (MESH) endpoint (or alternate address if provided to Cinapsis) that the referral has been made and accepted/declined.

The host of the OCS will be the South Warwickshire GP Federation.

The management of non-routine referrals will be considered in phase 2 of the project, the DPIA will be updated at this point. In phase 1 signposting and advice on the management of urgent and emergency referrals will be included on EeRS reflecting the current referral pathways.

Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system/process being implemented as part of the project.

The Cinapsis referral system affords a highly effective patient referral methodology. A handshake takes place with the NHS Spine and returns patient demographic and GP practice Registration details. A presenting complaint and, if necessary, additional information such as documents or pictures may be added, which creates a 'Case'.

Cinapsis features include synchronous (telephone and video) and asynchronous (e-mail/messaging) communications, which are tailored on a per-specialty basis. It enables secure and auditable communications; operating via connectivity to the Personal Demographics Service (PDS) and supports integration with external clinical systems.

Cases and outcomes, are all stored securely within the core application, hosted, and managed as part of the NHS HSCN.

The principal benefits of the Cinapsis referral system are summarised here:

- Provides a quick and easy route for optometrists to make referrals
- Optometrists will be able to view the outcome of the referrals made and will be able to access the booking number enabling them to contact the NHS and independent service providers to discuss their patients care if required
- Supports investment planning for online care pathways
- Creates more sustainable services.
- Provides clinical and activity data for audit, research, and development purposes.

Implementation of OCS would streamline routine eye referrals across the ICS where currently there are legacy pathways from the previous division into 3 CCGs. Establishing OCS should help ensure patient equity and choice across the ICS and fulfil the recently published patient choice guidance.

What is the purpose of collecting the information within the system/process? For example patient treatment, patient administration, research, audit, reporting, staff administration etc.

The implementation of the Cinapsis system will support existing processes in managing patient care, including referrals, and no new information or increased levels of information are collected or processed. The system deployment is requested to improve efficiencies in how data are shared between the healthcare team.

The primary objectives of the programme are:

1. take maximum advantage of evolving technologies to bring about improved patient care.
2. improve accessibility of data for health care professionals.
3. enhance information flows with targeted messages to the right person at the right time.
4. avoid/remove the risk of potential delays in patient interventions.
5. improve safety for patients and health carers through better use of patient information.
6. support drive towards better outcomes and more efficient healthcare delivery for patients.

What are the potential privacy impacts of this proposal - how will this change impact upon the data subject? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing.

The planned implementation introduces no new material impact upon data subjects. The programme is controlled by contracts that strictly govern the actions of data controllers and processors. All processing has been assessed to be compliant with data protection legislation.

Provide details of any previous Privacy / Data Protection Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system/process, a DPIA may have been undertaken during the project implementation.

This is a new Initiative for the data controllers within the Midlands EeRS Programme

If as part of a National initiative, technical specs etc. are required for review please embed in the below area:

Click or tap here to enter text.

2.3 Data Types

In order to understand the potential privacy risks, it is important to know the types of data that are proposed to be held and/or shared.

Personal	Please Tick All that Apply	Special Category (Sensitive)	Please Tick All that Apply
Name	<input checked="" type="checkbox"/>	Racial / ethnic origin	<input checked="" type="checkbox"/>
Address (home or business)	<input checked="" type="checkbox"/>	Political opinions	<input type="checkbox"/>
Postcode	<input checked="" type="checkbox"/>	Religious beliefs	<input type="checkbox"/>
NHS No	<input checked="" type="checkbox"/>	Trade union membership	<input type="checkbox"/>
Email address	<input checked="" type="checkbox"/>	Physical or mental health	<input checked="" type="checkbox"/>
Date of birth	<input checked="" type="checkbox"/>	Sexual life and/or sexual orientation (e.g. gender etc)	<input checked="" type="checkbox"/>
Contact number	<input checked="" type="checkbox"/>	Biometrics; DNA profile, fingerprints	<input type="checkbox"/>
Age	<input checked="" type="checkbox"/>	Health and Social Care data	<input checked="" type="checkbox"/>
Additional data types (if relevant)	<p>The provision of direct care by clinicians requires full, appropriate access to the healthcare record.</p> <p>The referral process and the processing envisaged are compliant with data protection legislation and meets tests on proportionality measures.</p>		

2.4 Assessment Questions

Please answer the questions below as fully as possible. If you are unsure of how to answer the question, please contact an IG Team member.

If there is supporting information that relates to any of the questions, which you feel would be informative, indicate within the comments section and send this along with the completed assessment.



Assessment Questions		
	Yes/No	Comments
Is it likely that the project will involve processes that are subject to Dept. of Health (DH) guidance/legislation/ Caldicott	<input checked="" type="checkbox"/> Yes	The system will be used to manage and monitor patient pathways, and report on local and national requirements.

principles/Medical Record Standards? (If you are unsure, please look at the list below, as examples of what process types would be included).	<input type="checkbox"/> No	
If you have answered 'Yes' to the above, please indicate (with an X) if the following activities are included within the project:		
		Comments
Recording of Demographic data	<input checked="" type="checkbox"/>	An initial referral on Cinapsis will include demographic data
Sharing of Patient information	<input checked="" type="checkbox"/>	An initial referral on Cinapsis will include the sharing of patient data
Diagnostic activity results	<input checked="" type="checkbox"/>	An initial referral on Cinapsis will include any diagnostic tests already undertaken.
Reporting of patient activity	<input checked="" type="checkbox"/>	
Transfer of Patient Identifiable Data to other systems, Patient, GP or other Third parties.	<input checked="" type="checkbox"/>	The referral will be transferred to the e-RS system, and responses and following communication will be transferred into Optom systems.
Other, Please state below:	<input checked="" type="checkbox"/>	
The Cinapsis system will be used to manage and monitor patient pathways, and report on local and national requirements.		
Category		
Technology	Yes/No	Comments
Does the project involve new or inherently privacy-invasive technologies e.g. biometrics or facial recognition?	<input type="checkbox"/> Yes	The Cinapsis system does not have biometrics or facial recognition ability.
	<input checked="" type="checkbox"/> No	
<p><i>NB: In order to answer this question, considerations include:</i></p> <ul style="list-style-type: none"> <i>whether all of the information technologies that are to be applied in the project are already well-understood by the public</i> <i>whether their privacy impacts are all well-understood by the organisation, and by the public</i> <i>whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected</i> <i>whether all of those measures are being applied in the design of the project.</i> 		
Justification	Yes/No	Comments
Is the justification for the new data-handling unclear or unpublished?	<input type="checkbox"/> Yes	
	<input checked="" type="checkbox"/> No	
<p><i>NB: Individuals are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed 'for security reasons', or 'to prevent fraud', are much less likely to calm public disquiet.</i></p>		

Identity	Yes/No	Comments
1. Will the project require anyone to contact individuals in ways that they may find intrusive?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	All parties will be contacted in agreed or existing methods of communication.
2. Does the project involve an additional use of an existing identifier?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	All patients' identifiers currently used will be used within the new system. Primarily the NHS number, but also the Acute Trust hospital number may be used, if required, in the future.
3. Does the project involve use of a new identifier for multiple purposes?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
4. Does the project involve new or substantially changed identity/ authentication requirements that may be intrusive or onerous?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
5. Will the project result in anyone making decisions or taking action against individuals in ways which could have a significant impact on them?	<input type="checkbox"/> Yes <input type="checkbox"/> No	By using the system, patients will be offered a choice of provider.
<p><i>The public understands that an identifier enables an organisation to collate data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.</i></p>		
Data	Yes/No	Comments
1. Will the project involve the collection of new information about individuals?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
2. Will the project compel individuals to provide information about themselves?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
3. Will the project result in the handling of a significant amount of new data about each person, or are there plans to use the information for a purpose it is not currently used for, or in a way it is not currently used?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
4. Will the project result in the handling of new data about a significant number of	<input type="checkbox"/> Yes	

people, or a significant change in the population coverage?	<input checked="" type="checkbox"/> No	The cohort of patients in the project will be the patient population of the ICS.
5. Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages?	<input type="checkbox"/> Yes	
	<input checked="" type="checkbox"/> No	
6. What considerations have been made regarding the adequacy, relevance and necessity for the collection of each field of personal confidential data for the project? Please describe what has been done and the outcome.	<p>The system chosen has a field for patient consent and training will incorporate a section which deals with patient consent for referrals.</p> <p>The configuration of the data fields will reflect what is currently collected for referrals,</p>	

NB: The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g. to support so-called 'front-end verification'), and the matching of personal data from multiple sources.

Data Handling	Yes/No	Comments
1. Does the project involve complex joint data controller arrangements that may prove difficult to administer? (If unsure then the IG team can discuss with you)	<input type="checkbox"/> Yes	Data Processing Agreements will be put in place to be signed by all Parties.  DPP_Version 3_6June2023_NHS_Er
	<input checked="" type="checkbox"/> No	
2. Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?	<input type="checkbox"/> Yes	
	<input checked="" type="checkbox"/> No	
3. Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?	<input type="checkbox"/> Yes	
	<input checked="" type="checkbox"/> No	
4. Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?	<input type="checkbox"/> Yes	The chosen supplier who is supplying the software has completed the following ICYT Assurance at BSOL ICB.:  Assurance%20Frame work%20for%20supp
	<input checked="" type="checkbox"/> No	
5. Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?	<input type="checkbox"/> Yes	
	<input checked="" type="checkbox"/> No	

6. Does the project involve new or changed data retention arrangements that may be unclear or extensive?	<input type="checkbox"/> Yes	
	<input checked="" type="checkbox"/> No	
7. Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?	<input type="checkbox"/> Yes	
	<input checked="" type="checkbox"/> No	
8. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	<input checked="" type="checkbox"/> Yes	Data will be made available to the digital supplier (Cinapsis) as part of providing the digital solution rather than shared directly with them. Some data may be visible during technical investigations, but assurances and checks have been undertaken on Cinapsis. Data Processing Agreements will be put in place to be signed by all Parties.
	<input type="checkbox"/> No	

2.5 Appropriate Policy Documents

An appropriate policy document should be produced outlining compliance measures and retention policies for **special category data**, if indicated in 2.3 above. The Data Protection Act states that an organisation should have one in place for almost all substantial public interest conditions (and also for the employment, social security, and social protection condition) as a specific accountability and documentation measure.


<p>What Schedule 1 condition (or conditions) of the DPA 2018 are you relying on to process special category data</p>	<p>DPA 2018 Schedule 1, Part 1 (2) – (1) condition is met as the processing is necessary for health and social care purposes, (2) means the purposes of (c) medical diagnosis, (d) provision of health care or treatment, (e) provision of social care and (f) management of health care systems or services or social care systems or services.</p> <p>The lawfulness of sharing/processing of Shared Personal Data set out in Article 6(1)(e) of the UK GDPR is also permitted under Section 8(d) of DPA 2018:</p> <p>Processing is necessary for the exercise of statutory functions.</p> <p>The lawfulness of sharing/processing special category personal data set out in Article 9(2)(h) of the UK GDPR (as above) is permitted under DPA Section 10 (health and social care purposes): Obligation of professional confidentiality and secrecy.</p> <p>For the purposes of Article 9(2)(h) of the UK GDPR, the circumstances in which the processing of special category personal data is carried out is subject to the “conditions and safeguards” referred to in Article 9(3) of the UK GDPR. Therefore, in accordance with the Data Protection Act 2018 s.11(1), these “conditions and safeguards” include circumstances in which it is carried out:</p>
---	---

	<ul style="list-style-type: none"> • by or under the responsibility of a health professional or a social work professional, or • by another person who, in the circumstances, owes a duty of confidentiality under an enactment or rule of law. <p>Access to patients' data will be carried out by "registered and regulated" health/social care professionals, and non-registered health/care professionals (e.g., analysts), who owe a duty of confidentiality as a result of their employment by health or social care organisations. The terms "health professional" and "social work professional" are defined in Section 204 of DPA 2018 and include a broad range of different professionals.</p>
<p>What procedures are in place</p>	<p>All organisations working within the health and social care sector are required to submit to a minimum of 'Standards Met' to the Data Security and Protection Toolkit (DSPT). The DSPT encompasses the National Data Guardian's 10 data standards and ensures accountability can be evidenced and holds organisations accountable for the way that they handle, share and process personal data. The submission is annual and is mandatory. The GP Practices, acute trust, Community Care and Cinapsis are all required to complete this and be compliant with the current DSPT.</p> <p>All organisations are required to have comprehensive information governance policies and procedures in place and ensure they meet the UK GDPR Article 25 requirement of having processes in place that meet data protection by design and default. Any organisation implementing a new software, system, platform etc. must ensure confidentiality is built into everything and be able to evidence this through effective and key documentation. As such all staff must be trained on an annual basis as a mandatory requirement in Information Governance, employment contracts must contain clauses that relate to confidentiality, staff must be issued with an Information Governance Handbook and sign a key code of conduct to ensure the organisation has accountability built into their everyday operations.</p> <p>The Cinapsis platform is hosted by Hicom Technology (https://www.hicom.co.uk/) who operates a scalable, high availability data centre based in Surrey. A tiered storage solution is in place, with resilience against multiple disk failures, controller failure, power failure and connectivity failure. The storage environment is rated at 150,000 IOPS and provides low latency storage via redundant fibre switching. The data centre has redundancy throughout all critical infrastructure components i.e. cooling, networking, perimeter defences, compute etc., all external connectivity is provided by diverse providers to ensure redundancy in the event of complete supplier failure, multiple levels of power redundancy are provided by UPS and external generators. The Hicom data centre has multiple levels of monitoring and alerting in place which are continuously monitoring the health, resources and availability of the various servers and services, this allows Hicom to pro-actively support these servers and services ensuring maximum uptime.</p> <p>The Hicom data centre is secured against physical and cyber threats, all external connections coming in to the Hicom data</p>

	<p>centre are protected by enterprise grade redundant firewalls, all Hicom systems are secured with a minimum of two layers of malware/virus protection, the physical environment is located in a secure location and protected with bio metric security systems.</p> <p><i>3rd-Party Cloud Supplier</i></p> <p>Hicom uses Redcentric to provide HSCN connectivity, Redcentric are one of the core providers selected by the NHS to provide backbone technology and services to the HSCN network. The physical connectivity is provided by BT & Virgin (diverse providers). Hicom are ISO 9001:2015 Quality Management System (FS33136) and ISO/IEC 27001:2013 Information Security Management System certified (IS 535638)</p> <p><i>Controls in place with infrastructure partners</i></p> <p>The third-party providers have no access to the application, all physical devices i.e. firewalls/servers (excluding the router) are managed by Hicom and no other parties have access, all external connections to the application utilise encryption.</p>
Retention and deletion Policy	All organisations, as part of the DPIA, will follow the Records Management Code of Practice 2021 (RMCoP)
Retention Period for specific documents	No specific documents are highlighted but the RMCoP will be followed appropriately.
<p><i>If you process special category data for a number of different purposes, you don't need a separate policy document for each condition or processing activity – one document can cover them all.</i></p>	

2.6 Procurement / development of data collection system

This section relates to work that may be included within the overall project plan however if some planning has already taken place, it should still be recorded here.

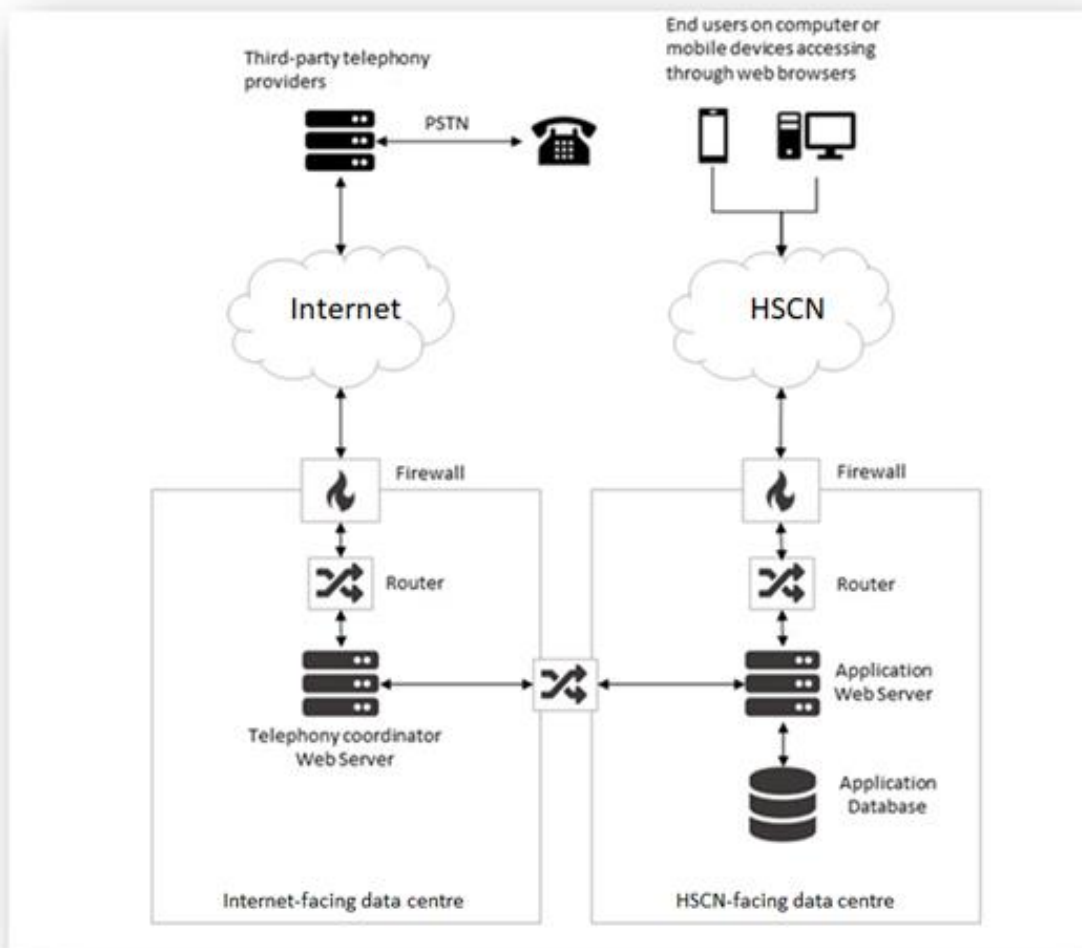
Questions for the procurement / development of a data collection system.	
<p>1. Has a data flow mapping exercise been undertaken? <i>If yes, please provide a copy</i> <i>If no, please ensure one is included within the overall project plan</i></p>	<p>YES</p> <p> Cinapsis Technical Architecture.pdf</p>

Data Flow

The diagrams below depict the data flow design, using the Cinapsis application:

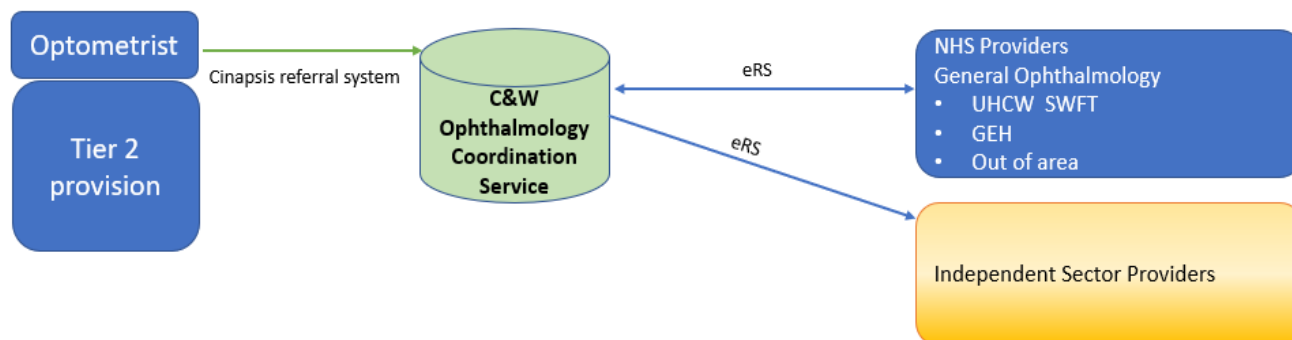


System topology



Coventry and Warwickshire ICB Referral process with eRS Interface:

Coventry and Warwickshire Ophthalmology Process – Future routine referrals




<p>2. Does the system involve new or changed USER access controls and/or authentication requirements?</p>	<p>Yes – the system’s access will be controlled by local admin teams within the Partner organisations.</p>
<p>3. Does the system allow different levels of access for different job roles?</p>	<p>YES - RBAC is in place and will be matched against staff requirements, as part of the Design and Develop Stage.</p>
<p>4. Are there any new or additional reporting requirements for this project? <i>If yes, please provide full details</i> <i>If not yet considered please confirm it will be included in the overall project plan.</i></p>	<p>The Reporting requirements at Region and secondary care and will be scoped out and agreed by Project Board as part of the Design and Develop Stage.</p> <p>The reporting requirements will be based on numbers of referrals and the percentage which is returned to Optom as requiring further information to progress the referral.</p> <p>No new Patient Identification Data will be reported from what is currently collected.</p>
<p>5. Does the system affect any current policies in relation to the collection and management of PCD – in so far as it may require changes to policy?</p>	<p>No</p>

6. Who provides the data that will populate the system?	Clinicians enter patient data at the time of referrals and when communicating with specialists.
7. How will you ensure that the individuals whose information will be processed have been informed of all the processing ¹ and disclosures that will take place?	Optom Practice information and privacy notices confirm use of patient information. For example, the DATA CONTROLLER website privacy notice should state: It may also be necessary, where the latest technology allows us to do so, to use your information and health data to facilitate digital consultations and diagnoses and we will always do this with your security in mind.
8. Will individuals be asked for consent for their information to be accessed, collected and/or shared?	Yes.
9. If NO to Q8, provide or list the reason(s) for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has Section 251 approval or another legal basis.	N/A
10. If data is to be shared outside of the organisation will individuals be able to opt-out? How will the opt-out be recorded e.g. on the system, manual	Data is shared as part of a referral to secondary care services so the patient will not have opted out of sharing their data if accepting that referral.
11. If this project relates to the disclosure of information, how will obligations to share be met?	Data Sharing Agreements will be used within the ICS demographic where required.
12. Who will have access to the identifiable information from the system/process and how?	Optoms (to include nominated admin staff) Ophthalmologists (in Secondary Care)
13. Have you considered an audit trail and what information it will capture? Examples include: all changes made to a record, who made the changes, who has viewed the record.	The Cinapsis solution provides clinical and activity data for audit, research, and development purposes
14. What procedures are in place or planned for the rectifying of inaccurate data, preventing the use of data by individual request or court order?	Under Article 16 of the GDPR data subjects have the right to have inaccurate data rectified. The Optom Practice in their role as data controller must ensure that they have robust policies in place to ensure patients can request rectification of their information and forms part of the Data Quality process each practice must implement to ensure records are accurate and kept up to date. In relation to erasure, this must only be done in cases where clinical validation has been received and only when full assessment has been undertaken and must only be done on a case-by-case basis.

¹ Processing (as defined in the Data Protection Act 2018) in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as (a) collection, recording, organisation, structuring or storage, (b) adaptation or alteration, (c) retrieval, consultation or use, (d) disclosure by transmission, dissemination or otherwise making available, (e) alignment or combination, or (f) restriction, erasure or destruction.

<p>15. Is the new system/process replacing a system/process which is currently in use? <i>If YES, what is the name of the old (legacy) system/process?</i></p>	No – this is a new digital referral system to replace the current pathway which uses nhs.net email, or letter.
<p>16. If yes to Q15, is all the data being migrated to the new system/process? <i>If yes, what has been done/will be done to ensure that the data is of good quality, appropriate, adequate and not excessive.</i></p>	N/A
<p>17. If no to Q15, what arrangements have been/will be made to ensure that controlled access is still available to records which have not reached their retention period.</p>	N/A
<p>18. What arrangements are in place to manage the legacy system/process – is it being decommissioned, what is happening to the data it contains, do some staff need to continue to have access to it, how long will it be maintained etc.</p>	<i>N/A – This is a new system to streamline the Eyecare referral pathway.</i>
<p>19. What considerations have been made/planned regarding the destruction of any records as part of this project?</p>	Records will be held/destroyed in line with the NHS Records Management Code of Practice 2021
<p>20. What is the proposed model for the storage of, and access to, records? <i>NB some of the options listed may go against our policy(s) and so will be highlighted in the report produced from this questionnaire.</i></p>	<input type="checkbox"/> Paper
	<input type="checkbox"/> Networked database, stored on organisations own server and access via network.
	<input type="checkbox"/> Separate system with data saved on network
	<input type="checkbox"/> Separate system with no network (standalone)
	<input checked="" type="checkbox"/> Hosted on a third party server and accessed via internet/portal
	<input type="checkbox"/> Other – please specify: Click or tap here to enter text.
<p>21. If any information will be stored off-site (off-site means outside the organisation and its computer network) please provide details of information security arrangements</p>	Cinapsis store data in cloud based storage on 2 sites within the UK
<p>22. Will information be sent off-site (off-site means outside the organisation and its computer/storage network)?</p>	Yes – see above response (Q21)
<p>23. Please state by which method the information will be transferred.</p>	<input type="checkbox"/> Email (nhs.net/NHSMail)
	<input type="checkbox"/> Email (not nhs.net mail)
	<input checked="" type="checkbox"/> Website access (i.e. a website portal with authentication/log in)
	<input type="checkbox"/> Post (external) <input type="checkbox"/> Post (internal)
	<input type="checkbox"/> Telephone

	<input type="checkbox"/> Courier
	<input type="checkbox"/> Wireless Network (Wi-Fi)
	<input checked="" type="checkbox"/> Secure internet connection (please specify) Click or tap here to enter text.
	<input type="checkbox"/> Other – please specify: Click or tap here to enter text.
24. Is any personal information of any kind being transferred outside of the UK?	No data is transferred outside of the United Kingdom.
25. If yes to Q24, Specify the data that is to be transferred abroad (even if the EU)	N/A
26. Is the system/process to be covered by existing Information Security and other policies?	Yes
27. Is disaster recovery and contingency planning being put in place to manage the effect of any unforeseen events?	Yes – the supplier has a robust DR and Contingency plan. Acutes and Optom Practice will have their localised DR in place as part of EPPR.
28. Are there procedures in place to recover data which may be damaged through the following: <i>Human error Computer virus Network failure Theft Fire Flood Other disaster</i>	Yes, these are detailed within the Call off Contract with NHS E.
29. Has the requirement to apply clinical risk management to the deployment of patient based systems/processes been addressed and in what ways?	NHSE Midlands EeRS Programme have commissioned eTHOS to undertake Clinical Safety assessment. But Cinapsis DCB0129 assessed:  C1.1.1%20-%20Cinapsis%20Clinical%20R
30. What assurances will be received to ensure Mandatory Staff Training is in place for the following: <ul style="list-style-type: none"> • Data collection: • Use of the System or Service: • Collecting Consent: • Information Governance? 	All organisations have mandatory IG training in place. Training of the system will cover data collection, using the system, and collecting consent as well as explaining the processes of the system.

2.7 Data Retention and Disposal

2.7.1 How long is the process/project/initiative expected to last?		
End of contract period	<input type="checkbox"/>	Click or tap here to enter text.
A specific time period (<i>Please specify</i>).	<input checked="" type="checkbox"/>	Cinapsis has been procured under an initial four year contract.

Lifetime of system (where the initiative or project relates to a new or revised ICT system)	<input type="checkbox"/>	Click or tap here to enter text.
Other (please specify)	<input type="checkbox"/>	Click or tap here to enter text.

2.7.2 How long does the data need to be retained?

In line with the Contract and returned/deleted at the end of the contract other than what is required for legal and regulatory reasons required by the supplier.

The retention period is 8 years. Upon reaching 8 years, data are reviewed and purged from the system under instruction from DATA CONTROLLER. Cinapsis has been procured under an initial four-year contract, and information will be deleted or returned to the DATA CONTROLLER at the end of this period if the contract is not extended.

What retention period is suitable for the data you will be processing (e.g., following a Record and Information Lifecycle Management).

If following the [Records Management Code of Practice 2021](#), please quote minimum retention and disposal from the guidance in the text above. If Medical Device retention guidance is being followed please state as such and how long etc.

NB: Please note that all records should be reviewed at regular intervals.

2.7.3 If the data is held electronically, does the process/project include a facility to flag records for review/deletion?

Yes	<input type="checkbox"/>
No	<input type="checkbox"/>
Not applicable	<input checked="" type="checkbox"/>

2.7.4 Are there any exceptional circumstances for retaining certain data for longer than the normal period?

Yes	<input type="checkbox"/>
If Yes, please provide details of how this is conducted and why	Click or tap here to enter text.
No / Not Applicable	<input checked="" type="checkbox"/>

2.8 Legal Basis/bases

To collect and use the data you must have a legal basis for doing so, please indicate which basis below (it can be more than one):

Explicit Consent <i>Has the individual(s) to whom the information relates given explicit consent to process for one or more specific purposes? If so, please provide copies of any consent documentation being relied upon for review.</i>	<input type="checkbox"/>	Contract <i>Is the processing necessary for a contract the ICB has or has been asked to take specific steps before entering into a contract?</i>	<input type="checkbox"/>
--	--------------------------	--	--------------------------

Legal Obligation <i>Does the ICB have a legal duty to process information?</i>	<input type="checkbox"/>	Vital Interests <i>Is the processing necessary to protect a data subject's life?</i>	<input type="checkbox"/>
Public Task (Article 6(e)) <i>Is processing necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller (e.g. scientific research, public health)?</i>	<input checked="" type="checkbox"/>	Legitimate Reason <i>Is processing necessary for the purposes of the legitimate interests of the ICB or a third-party? (Please note that this basis cannot be used for clinical purposes.) If relying on this as a legal basis then a Legitimate Interest Assessment form will need to be completed (contact the IG Team).</i>	<input type="checkbox"/>
Special Categories (Article 9 (h)) <i>Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State Law.</i>			<input checked="" type="checkbox"/>
Other <i>Either supply free text in the text box provided opposite or check the below explanations</i>	<input type="checkbox"/>	Click or tap here to enter text.	
An overriding public interest <i>An overriding public interest, where it is judged that the benefit of providing the information outweighs the rights to privacy for the individual concerned and the public good of maintaining trust in the confidentiality of the service</i>	<input type="checkbox"/>	**Legal support: <i>for the use of confidential patient information without consent under Health Services (Control of Patient Information) Regulations 2002, under section 251 of the NHS Act 2006. Legal support such as S251, PBPP (Scotland), PAC (N. Ireland). If you are relying on Legal Support, then please seek advice from IG</i>	<input type="checkbox"/>
<p><i>** NB Where the disclosure of PCD relates to groups rather than individuals, e.g. for clinical audit or medical research where identifiers are required and consent is genuinely not practicable, then support under Section 60 of the Health and Social Care Act 2001 may be sought through application to the Patient Information Advisory Group.</i></p> <p><i>Legal support such as Section 251 (England), PBPP (Scotland), PAC (N. Ireland). If you are relying on Legal Support, then please seek advice from the IG Team.</i></p>			

2.9 Common Law Duty of Confidentiality (CLDC)

Common Law is also referred to as “judge-made” or case law, so common law is also said to be based on precedent.

(For further information or guidance speak to a member of the IG Team as there is a mandatory requirement to complete this section – it cannot be left blank.)

To meet the requirements of CLDC there must be one of the following conditions:

Requirement	Guidance	
CLDC is covered under Legal Basis as not relying on consent	<p><i>If consent is not the legal basis for the processing of data then CLDC does not require assessment.</i></p> <p><i>The use of Personal Data via the application is for the purposes of Direct Care and Administration, therefore a</i></p>	<input checked="" type="checkbox"/> N/A

	<i>patient's consent to such sharing/Processing can be implied.</i>	
Legal requirement	<i>A mandatory legal requirement or power that enables the CLDC to be set aside, such as the Children Act 1989 which requires information to be shared in safeguarding cases, statutory powers etc.</i>	<input type="checkbox"/>
Court order	<i>A court order where a judge has ordered that specific and relevant information must be provided and to whom</i>	<input type="checkbox"/>
Explicit consent	<i>Explicit (written permission that is fully informed) consent</i>	<input type="checkbox"/>

N.B. The general position is that if information is given in circumstances where it expected that a duty of confidence applies, that information cannot be normally disclosed without the data subject's consent.

Please provide any documentation that you are relying on for this data, such as a Court Order, mandatory legal requirement or the explicit consent documentation used to record any data subject's consent.

2.10 Third Party Partner Organisations

Will data be accessed, stored or processed by a party external to the organisation?	
Yes	<input checked="" type="checkbox"/>
<i>If Yes, please request that they complete the technical security questionnaire but list the organisations in the table provided below, NHS/3rd party/external suppliers etc.</i>	Monmedical Limited T/A Cinapsis
No / Not Applicable	<input type="checkbox"/>
<p>Will the named partner subcontract any part of the work? (i.e. for data capture or entry, systems support or for contacting patients/service users)</p> <p>If Yes, what due diligence has been carried out and evidence of assurance be provided?</p>	<p><input checked="" type="checkbox"/>Yes <input type="checkbox"/>No</p> <p>The data hosting centre is managed by Hicom Technology Ltd.; these arrangements are covered under contract with the Supplier.</p> <p>Hicom, under data protection legislation is regarded as a Sub-processor of personal data.</p> <p>Two additional specialist companies provide applications to the Supplier; these are used to manage voice and video communications. The Supplier has in place contracts with Twilio Ireland Ltd., and Aculab PLC, which under data protection legislation are regarded as Sub-processors of personal data.</p>

Organisation name and Data Protection (ICO) Registration number. https://ico.org.uk/ESDWebPages/Search	Are they a Data Controller (DC) or Data Processor (DP)? (If Joint Controller check both boxes)	Compliance with the Data Security & Protection Toolkit	
		Status Stds = Standards	Date Published
Monmedical T/a Cinapsis ZA288593	DC <input type="checkbox"/> DP <input checked="" type="checkbox"/>	Stds Exceeded	<input checked="" type="checkbox"/>
		Approaching Standards	<input type="checkbox"/>
		Not Published	<input type="checkbox"/>
		23/03/2023	

Coventry and Warwickshire Optoms (Various)	DC <input checked="" type="checkbox"/> DP <input type="checkbox"/>	Stds Met	<input checked="" type="checkbox"/>	Click or tap to enter a date.
		Approaching Standards	<input type="checkbox"/>	
		Not Published	<input type="checkbox"/>	
Coventry and Warwickshire ICB ZB342926	DC <input checked="" type="checkbox"/> DP <input type="checkbox"/>	Stds Met	<input checked="" type="checkbox"/>	29/06/2023
		Approaching Standards	<input type="checkbox"/>	
		Not Published	<input type="checkbox"/>	
South Warwickshire GP Federation ZA104695	DC <input type="checkbox"/> DP <input checked="" type="checkbox"/>	Stds Met	<input checked="" type="checkbox"/>	19/05/2023
		Approaching Standards	<input type="checkbox"/>	
		Not Published	<input type="checkbox"/>	
		Approaching Standards	<input type="checkbox"/>	
		Not Published	<input type="checkbox"/>	
Exemptions	Yes/No	Comments		
Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?	<input type="checkbox"/> Yes			
	<input checked="" type="checkbox"/> No			

3. DPA 2018 / UK GDPR

Does the DPIA meet the following legal requirements?

	Assessment of Compliance
<p>Principle 1 – Lawfulness, fairness and transparency</p> <p><i>(Use of personal data is fair, lawful and transparent)</i></p>	<p>It is the responsibility of every Partner to ensure that as data controllers, they inform their patients under the ‘Right to be Informed’ detailed in the Data Protection Act 2018. They must ensure the use of Cinapsis is detailed in their privacy notice and uploaded both to the website and within practice. Any easy-to-read privacy notices, notices produced in other formats or notices translated into other languages, must also contain this information. Partners may wish to produce information leaflets on the use of Cinapsis or signpost patients to the Cinapsis website for additional information, but the information cascaded to patients must be transparent, easy to understand and specific. Cinapsis have a data security & privacy notice on their website which may also be referenced.</p> <p>The Partner will process any subject access requests made by patients adhering to their Subject Access Request policies. Any information updated into the records following a Cinapsis consultation will form part of the release of records and will also adhere to the stipulations of the Cinapsis data processing agreement. Patients have the right to request their information in any accessible format in relation to their right to data portability and it is the partner responsibility to meet their requested format as far as practically possible.</p>
<p>Principle 2 – Purpose limitation</p> <p><i>(Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose)</i></p>	<p>The purpose of processing personal data in this manner is to deliver safe and effective care in an alternative approach to traditional face-to-face consultations within Secondary/Community care. Consultation is for medical purposes, and the patient can dissent to a referral to the Secondary Care Partner if they so wish.</p>
<p>Principle 3 – Data minimisation</p> <p><i>(Use of personal data is adequate, relevant and no more than necessary)</i></p>	<p>Cinapsis initially uses the NHS number of the patient to link via the PDS to the NHS Spine. This will provide key demographic data to the Optom enabling the communication with the specialist consultant in the Secondary care arena– the Optom Practice will need to share key data relating to the clinical presentation and any key documents/images facilitate the specialist direct care needs of the patient, but at all times only the minimal amount of data would be shared and only within the realms of the professional capacity of the clinicians involved.</p>
<p>Principle 4 – Accuracy</p>	<p>The consultation will be summarised onto the Optom record of the patient. Healthcare professionals</p>

<p><i>(Personal data must be accurate and kept up to date)</i></p>	<p>should ensure that this is done as soon as possible if not contemporaneously. It remains the responsibility of the Optom Practice, in their role as data controller, to ensure records are maintained accurately and kept up to date at all times. They must therefore have robust Data Quality procedures implemented with all staff trained on how and when to update records, and regular audits must be undertaken to ensure the practice records remain accurate and up to date.</p>
<p>Principle 5 – Storage limitation <i>(Personal data must be kept in an identifiable format for no longer than necessary)</i></p>	<ul style="list-style-type: none"> • The data retention period is 8 years as per NHS Digital Retention Schedule. • Data to be reviewed and if no longer needed to be destroyed after this period. • Data ingested by partner clinical systems will be subject to local data retention schedules.
<p>Principle 6 – Integrity and confidentiality (security) <i>(Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction)</i></p>	<p>Cinapsis can:</p> <ul style="list-style-type: none"> • Demonstrate that the manufacturer/developer of the Clinical Communication Tool system has applied and met the NHSD DCB0129 clinical safety requirements. • Demonstrate knowledge and understanding of clinical frameworks and referral management protocols across healthcare settings. <p>Cinapsis are fully DTAC accredited, which as well as a review of overarching application security, includes a requirement to have annual PEN testing undertaken by an independent third party, demonstrating the security of their web based app over HSCN and internet</p> <p>Hosted environment is ISO270001 accredited.</p> <p>Cinapsis are accredited with Cyber Essentials Plus.</p> <p>Cinapsis are also accredited separately as part of their integration with several NHS API's e.g. NHS spine, etc.</p> <p>Log in to the Cinapsis app is subject to 2 Factor Authentication (2FA) on first login up until the session is marked as trusted by the end user (or thereafter every 90 days). The user password must also meet a minimum security criterion.</p> <p>New users must be added and/or authenticated by a nominated administrator before being added to the server.</p>
<p>Principle 7 – Accountability</p>	<p>Cinapsis have a data processing protocol in place that aligns with key legislative requirements, so will be used for Optom Practices to demonstrate accountability in their key activities.</p>



DPP_Version
3_6June2023_NHS_Er

The above embedded document is for use within each ICS to obtain signatures from the Trusts involved and for Optoms to sign up to the Processing of their data by Cinapsis.

4. Risks

Project Ref Number: EeRS2023

Please list the risks identified during assessment, scores and any actions that must be undertaken.

Risk Identified	Consequence Score 1 = Low 2 = Medium 3 = High	Likelihood Score 1 = Low 2 = Medium 3 = High	Risk Score (C x L)	Action <i>(The action is the mitigation or processes in place to reduce the risk)</i>	Owner
Optometrists not able to provide digital output from their equipment	3	2	6	Programme team to carry out capability and explore solutions	EeRS Project Team
Hosted service and Voice and Text services by contracted external system suppliers – adequate cyber security controls	2	2	4	Reviewed applicable supplier/subcontractor certification – ISO 27001 / Reviewed supplier's Statement of Applicability. ISO certification evidenced. Cinapsis has achieved, and consistently maintained, NHS Data Security and Protection Toolkit standards, evidence of compliance. NHS DSPT ODS Ref: ARX02. Cinapsis possesses Cyber Essentials Plus certification.	Data Controller and ICB
System supplier does not respond adequately to requests for change and correction of reported bugs in the system.	3	1	3	Ensure support process prioritises significant defects. Initial pilot tested the support process. Service levels have been agreed as part of contract relationship and monitored at weekly project meetings.	Cinapsis
Risk of inaccurate data being shared i.e. Sharing data relating to the wrong patient	2	2	4	It is the responsibility of the Optom Practice to maintain accurate records of each patient registered and to ensure rectification protocols are timely and appropriate and regularly	Data Controllers

				audited to maintain the quality of the data that links with the PDS to inform the NHS Spine	
<p>Cinapsis can be used on the following devices:</p> <p>On a mobile, browser and as a desktop app (in the form of a floating toolbar)</p> <p>NHS Mail credentials can be used to log into Cinapsis</p> <p>Biometrics enabled on a sharded device could cause issues if staff save credentials on a shared device</p>	3	2	6	<ul style="list-style-type: none"> • Training and Education given to Optom Practices and Practice staff and relevant documentation. • Save the login page https://app.cinapsis.org as a bookmark on preferred browser for easier access. • Staff are informed “NOT” to save credentials or biometrics on a shared device 	Data Controllers

5. Statement of Assessment (completed by IG Leads)

Statement: Please select the appropriate statement and delete the words in bold that do not apply. The other statements should then be deleted.	Assessed By	Date
The privacy risks for this project/change have been assessed, based upon the information provided, and it is felt that there is a low risk of any impact to the privacy of the data subjects. Recommendations have not been made within this section which should be actioned to further reduce or restrict the privacy risks.	Kelly Huckvale, Senior Information Governance Manager, AGEM CSU	26/03/2024

6. SIRO or Caldicott Guardian Statement of Assessment – for Full scale Data Protection Impact Assessments only


Statement – Please remove text in bold that is not applicable	Please choose	Date
<p>Having reviewed the privacy impact risks, assessment recommendations and/or DPIA Report, I confirm that this project/change can/cannot proceed:</p> <p>The reasons for this are:</p> <ul style="list-style-type: none"> • It is crucial to the service delivery within the Organisation / The privacy risks identified would impact negatively on the service delivery within the organisation • The mitigating recommendations, once completed, will/will not reduce the likelihood of the privacy risks occurring • Reassurance has been sought from the Information Commissioners Office and/or NHS England Transformation Team (where applicable), who have confirmed that we are able to proceed/should not proceed with this project/change. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Click or tap to enter a date.

Frequently Asked Questions

<p>What is a DPIA?</p>	<p>Data Protection Impact Assessments (DPIA) is a process that assists organisations in identifying and minimising the data protection risks of new projects or policies.</p>
<p>What is a data protection risk?</p>	<p>This is the risk of harm arising through an intrusion into an individual's physical or informational privacy.</p>
<p>Do I need to consult with other individuals?</p>	<p>Yes, the completion of a DPIA involves working with people who may be affected by the project within the organisation, partner organisations and/or the people directly affected.</p> <p>For example: If the people affected could be patients, it may be useful to include a patient experience group within the consultation process.</p>
<p>Do I need to consult about the DPIA separately if I have already completed this in relation to the Project Documentation?</p>	<p>No; it is expected that information impacts would have been raised as part of the initial project review/documentation</p>
<p>Why do we need to complete a DPIA?</p>	<p>This will highlight any risks or unidentified risks associated with the new project, processes or policies.</p> <p>The ICO (Information Commissioner) may request organisations DPIAs when reviewing incidents or completing audits as this is the most effective way for an organisation to demonstrate to the ICO how they comply with the Data Protection Act.</p> <p>Completing a DPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.</p>
<p>What Projects could require a DPIA to be completed?</p>	<p>The core principles of a DPIA should be completed with all projects. The DPIA is suitable for a variety of situations including (but not limited to):</p> <ul style="list-style-type: none"> • Introduction of a new IT System for storing and accessing personal data. • a data sharing initiative • using existing data for a new and unexpected or more intrusive purpose • a new or change of process involving data (personal/corporate) • implementing a new surveillance system • using a new database that consolidates information from various parts of the organisation • where new or revised policies, strategies will impact on privacy through the collection and/or use of information.

When should I complete a DPIA?	DPIAs should be completed at a time when it is possible to have an impact on the project or process. This is usually near the start of the process.
Does this link with other processes within the ICB?	Yes, the DPIA incorporates any other Information Governance or Data Protection requirements.
Who approves the DPIA?	<p>Any risks raised must be confirmed and accepted by the 'risk owner'.</p> <p>The Data Protection Officer (DPO) will review and approve for submission of the DPIA to the SIRO and/or Caldicott Guardian.</p>

High level workflow options to consider

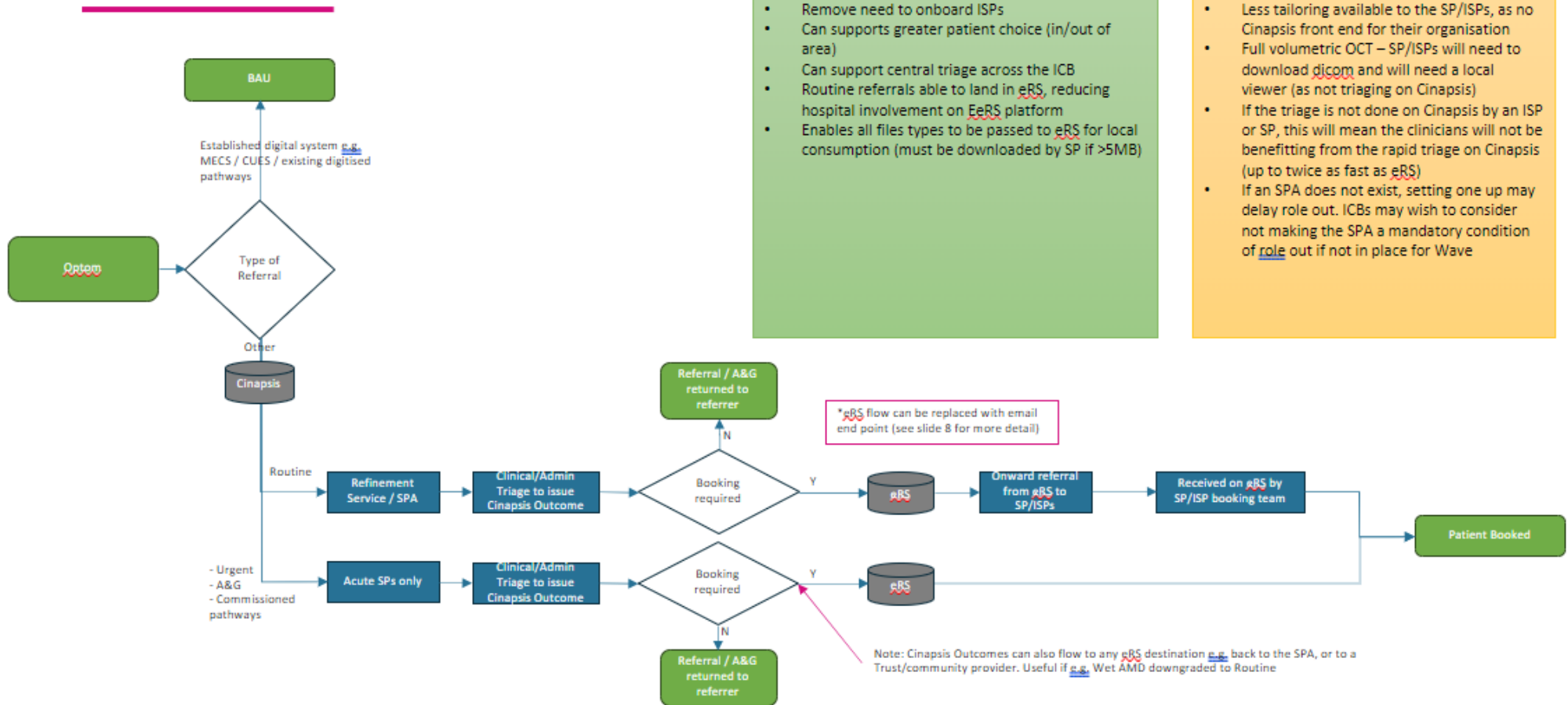
- 
-
- 1** **REFINEMENT SERVICE (SPA) & ACUTE TRUSTS USE CINAPSIS EeRS**
 - All routine referrals directed to SPA for onward referral to relevant SPs/ISP via eRS or NHS Mail
 - Only urgent pathways (e.g. WetAMD), existing A&G and hospital commissioned pathways direct to Acute SPs
 - 2a** **ORGS USE CINAPSIS EeRS – Clinical Triage on Cinapsis to issue outcome**
 - Direct connection to all SPs and ISPs
 - Digitise all current referral and A&G pathways
 - Clinicians review and outcome in Cinapsis, which then flows to eRS or email if accepted
 - 2b** **ORGS USE CINAPSIS EeRS – Administrative stage on Cinapsis to issue outcome**
 - Direct connection to all SPs and ISPs
 - Digitise all current referral and A&G pathways
 - Triage step is undertaken by an admin e.g. accept only, which then flows to eRS
 - 3** **Some SPs/ISPs do not participate in EeRS (with no SPA)**
 - Current: Pathways would remain as is, with no use of EeRS into or out of SPs/ISPs who do not participate
 - Future: Potential to use Cinapsis to present an SP on a DOS and just pipe to an email end point with SP having no EeRS front end (in development – est. late summer 2023)

Roll out can be staged if required to bring in SPs/ISPs when ready

Models can be mixed to use a mix of 1-3

Note: All flows in the following slides demonstrate a linear path for simplicity. See previous slide for indicative data flow back to referrer

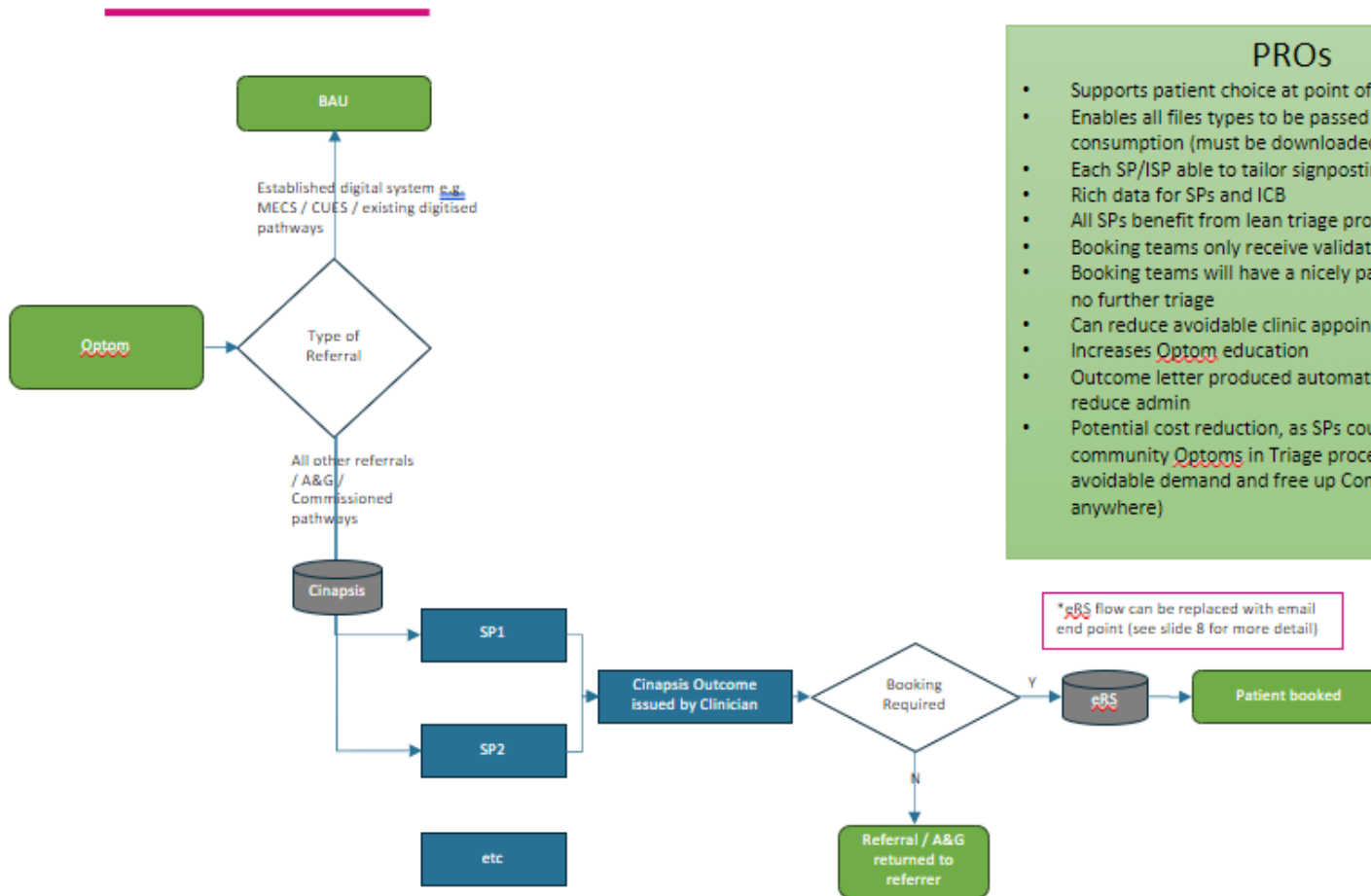
Option 1 - REFINEMENT SERVICE /SPA & ACUTE TRUSTS USE CINAPSIS



- ### PROs
- Remove need to onboard ISPs
 - Can supports greater patient choice (in/out of area)
 - Can support central triage across the ICB
 - Routine referrals able to land in eRS, reducing hospital involvement on eRS platform
 - Enables all files types to be passed to eRS for local consumption (must be downloaded by SP if >5MB)

- ### CONs
- Less tailoring available to the SP/ISPs, as no Cinapsis front end for their organisation
 - Full volumetric OCT – SP/ISPs will need to download **dicom** and will need a local viewer (as not triaging on Cinapsis)
 - If the triage is not done on Cinapsis by an ISP or SP, this will mean the clinicians will not be benefitting from the rapid triage on Cinapsis (up to twice as fast as eRS)
 - If an SPA does not exist, setting one up may delay role out. ICBs may wish to consider not making the SPA a mandatory condition of **role** out if not in place for Wave

Option 2a - ALL ORGS USE CINAPSIS – Clinical Triage on Cinapsis to issue outcome



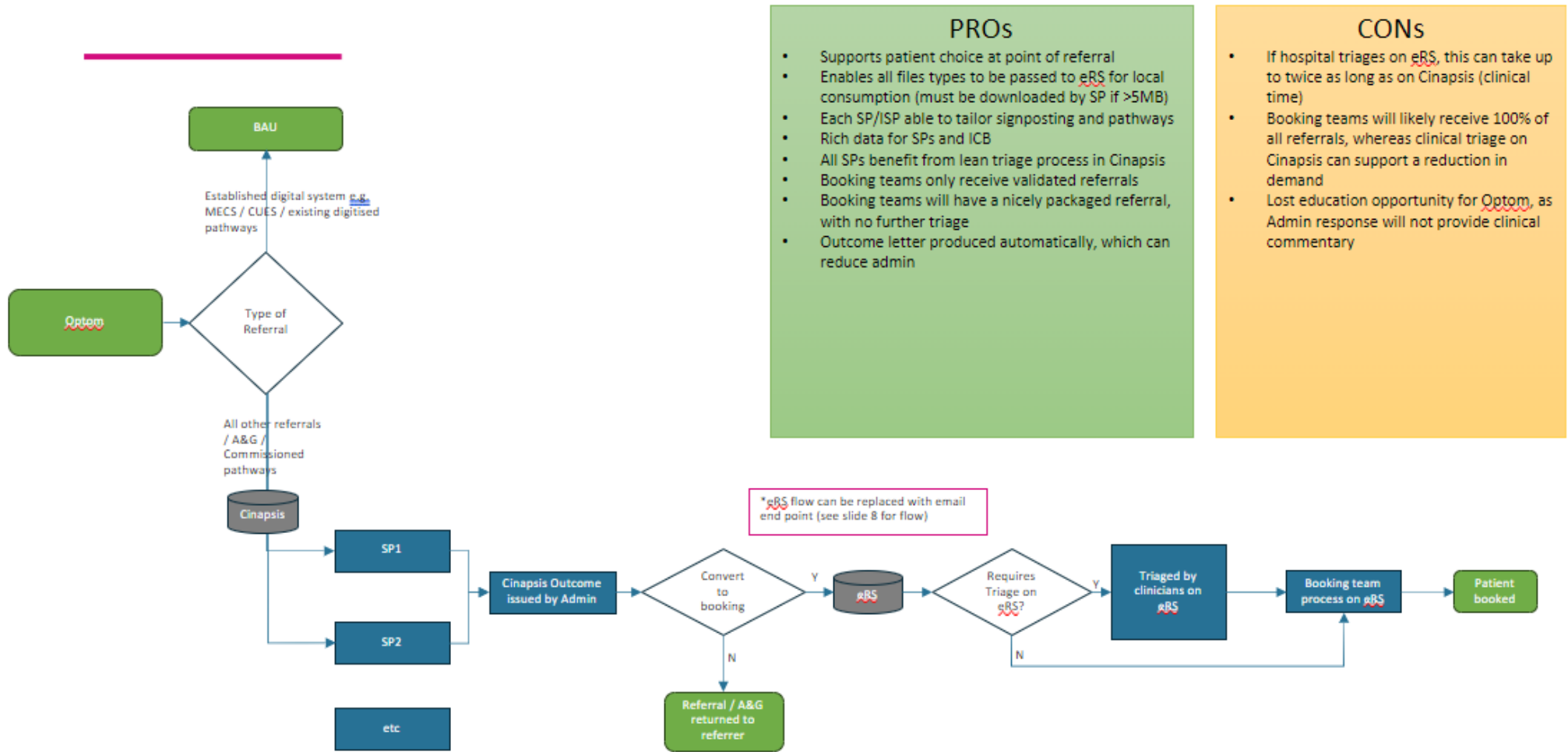
PROs

- Supports patient choice at point of referral
- Enables all file types to be passed to eRS for local consumption (must be downloaded by SP if >5MB)
- Each SP/ISP able to tailor signposting and pathways
- Rich data for SPs and ICB
- All SPs benefit from lean triage process in Cinapsis
- Booking teams only receive validated referrals
- Booking teams will have a nicely packaged referral, with no further triage
- Can reduce avoidable clinic appointments
- Increases Optom education
- Outcome letter produced automatically, which can reduce admin
- Potential cost reduction, as SPs could make use of community Optoms in Triage process to reduce avoidable demand and free up Consultants (work from anywhere)

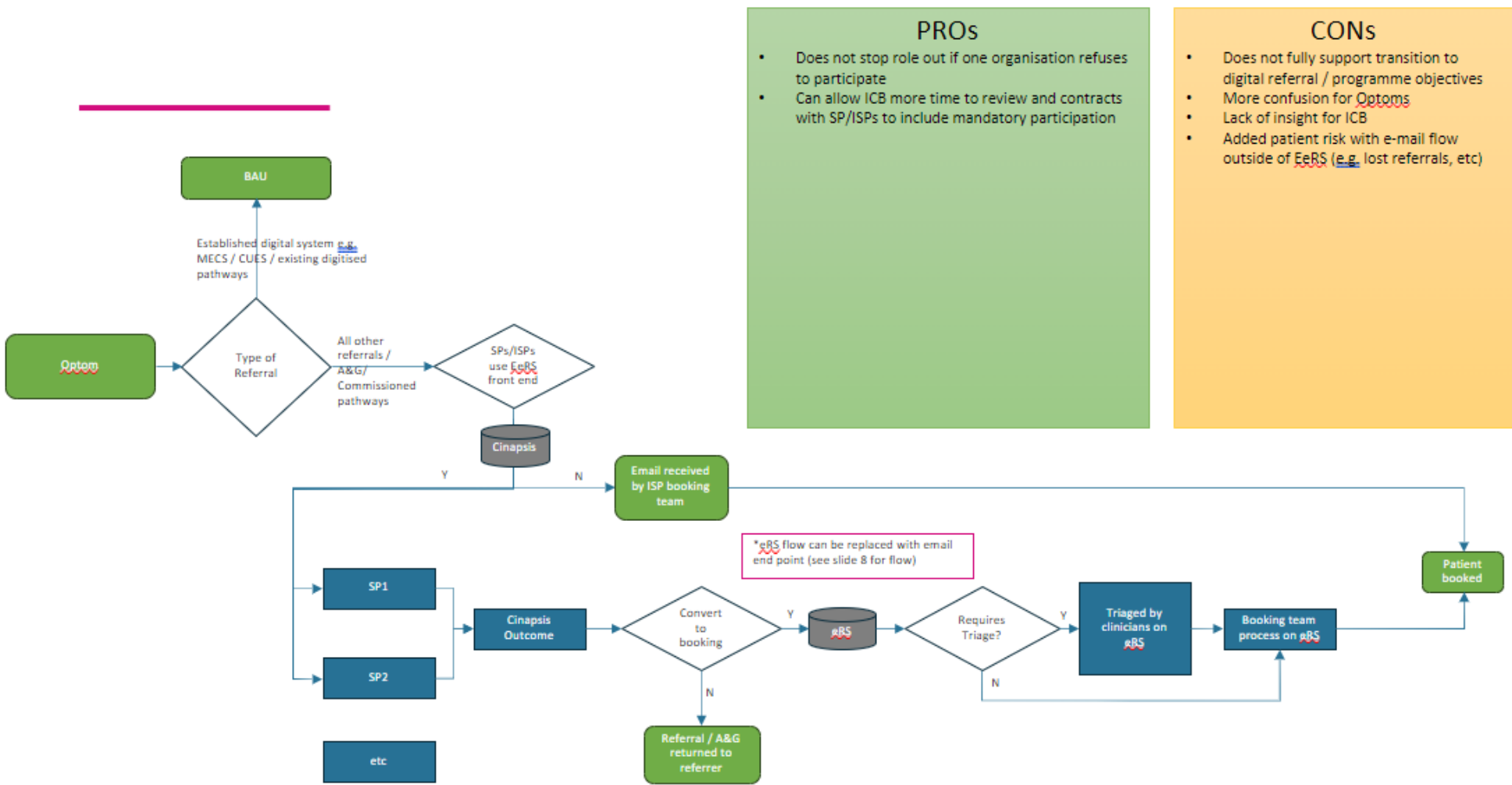
CONs

- All ISPs/SPs need to be engaged in the process to onboard
- Risk of ISPs/SPs not participating
- Required job planning for clinicians to triage

Option 2b - ALL ORGS USE CINAPSIS – Administrative stage on Cinapsis to issue outcome



Option 3 – Some SPs/ISPs do not participate in EeRS (with no SPA)



PROs

- Does not stop role out if one organisation refuses to participate
- Can allow ICB more time to review and contracts with SP/ISPs to include mandatory participation

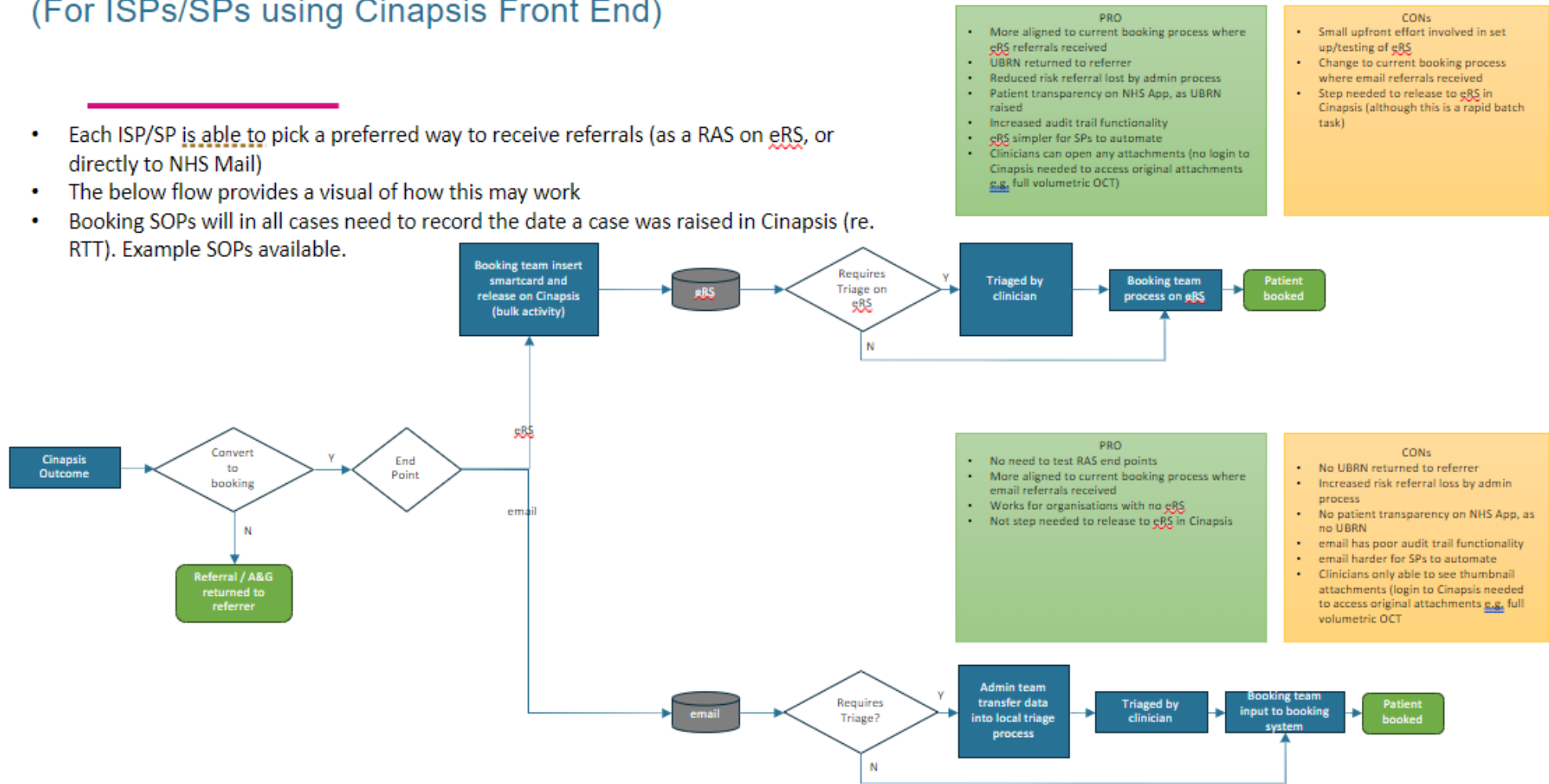
CONS

- Does not fully support transition to digital referral / programme objectives
- More confusion for Optoms
- Lack of insight for ICB
- Added patient risk with e-mail flow outside of EeRS (e.g. lost referrals, etc)

Appendix 2 – Identification of how to receive booking requests

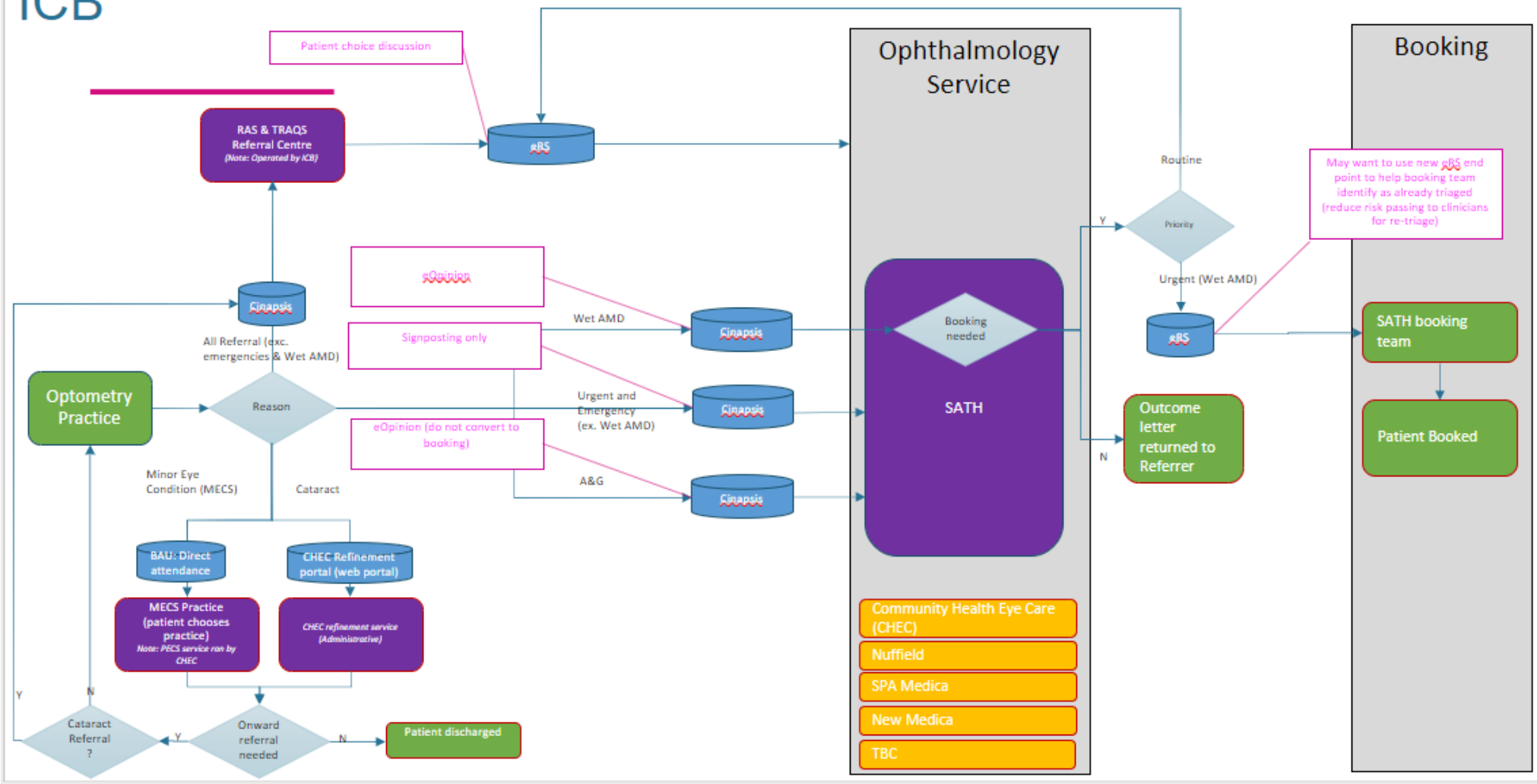
Identifying how to receive booking requests - eRS Vs email (For ISPs/SPs using Cinapsis Front End)

- Each ISP/SP is able to pick a preferred way to receive referrals (as a RAS on eRS, or directly to NHS Mail)
- The below flow provides a visual of how this may work
- Booking SOPs will in all cases need to record the date a case was raised in Cinapsis (re. RTT). Example SOPs available.



Appendix 3 – Example of high level flow at Shropshire, Telford and Wrekin ICS

Example: High Level Flow – Shropshire, Telford and Wrekin ICB



Checklist - Service Providers (1/3)

Core Project Team Resource

- The success of your local project will require you to provide resources from your organisation. Your ICB PM will reach out to identify a **local SRO, Clinical Lead, Operational Lead, Booking Lead, IT lead and BI Lead**. The team will be responsible for keeping other local stakeholders informed.
- Cinapsis will walk each Service Provider through the build decisions and testing process via a **series of short workshops**

Information Governance Resource

- As a data controller, you'll be required to **sign the Cinapsis Data Processing Protocol**. This provides Cinapsis with consent to store & process your data for the purposes of patient care
- Your ICB IG lead will co-ordinate the completion of an DPIA for your area and will authorise the use of the DPP in your region (required before we share)
- Please identify the relevant authorised IG lead to work with the ICB IG lead & also to sign the Cinapsis DPP

IT Assurance

- The Midlands programme team have already been in regular communication with local Digital leads across the Midlands. Agreement has been reached to **utilise the same IT assurance document across all ICBs**, which will be based on the BSOL template
- In the event you operate a process which is separate to the ICB IT Assurance, please engage with your IT leadership at the earliest opportunity to share the IT Assurance Template and gain advanced approval
- Questions should be directed through the Midlands Programme team

Cinapsis Contact

- Pre-Project – Cinapsis will be available via Midlands wide forums from now forward. The Midlands programme team will also be in continual contact with your ICB Project lead
- Project Start Up – Formal contact with Cinapsis will be initiated by waves sequence, beginning with the Early Adopter wave, then wave 1, 2, 3, etc. Each wave will be engaged typically 1 month from the scheduled initial go live of the proceeding wave

Pathways

- Cinapsis recommend you **identify any pathways that you wish to include in scope** e.g. Advice and Guidance, Cataract referrals, Glaucoma, Low Vision, Emergency, etc. It is likely each area will leave existing digital referral routes in place e.g. from MECS. Focus should therefore be on pathways which are undertaken by email, post and fax.
Note: Cinapsis can send referrals to you via a form (eOpinion), or can present an Optom with Signposting into an existing process (e.g. referencing an emergency phone number). Cinapsis can also provide call routing directly into your service if required (e.g. connecting to a baton phone or providing you with tools to manage on call rotas).
- Think in advance about the **desired end points to receive booking requests** to e.g. eRS RAS / email inbox (see briefing booking teams checklist note on the next slide)
- Cinapsis have template forms for most pathways, which will reduce effort in the build process (tailoring is also possible if needed). These can be tailored if changes are required

TBD

Checklist - Service Providers (2/3)

Clinical Safety Resource

- NHSE Midlands have engaged Ethos to undertake a review and assessment of Cinapsis' DCB0129 Hazard Log and Clinical Safety Report. Ethos will be in touch to share the output of their DCB0160 risk management template with each ICB
- Your ICB will nominate a local Clinical Safety Officer to co-ordinate the review & approval of the new EeRS solution
- Please **identify a representative from your organisation to participate** in this process

c3
hrs
total

General IT Readiness Tasks – IT Tasks involved

- Review Cinapsis WES to **ensure min Req's met** e.g. Whitelisting

30m

Booking Team Scope and Resource – IT Tasks involved if eRS used

- Operational leads to **consider in advance how they wish to direct work to their booking teams** (e.g. eRS RAS or email end points). If you currently triage on eRS, ew restricted RAS end points can be helpful to reduce risk of passing triaged cases back to clinicians on eRS to re-triage
- Managing RTT – The date that the Optom raised the referral should be recorded, not the date the UBRN is generated following triage. Future SOPs need to reflect need to input the correct start date by booking teams. This is commonly this is done by manually entering the booking details, or permitting the booking team to adjust the start date in your EPR/PAS (you may alternatively want to consider a scripted approach using supplier data).

Note: This is a limitation of the NHSE API, which isn't able to allow a 3rd party supplier to provide an alternate start date into eRS. NHSE are aware and have an improvement in their backlog to look at this in the future. Example SOPs can be shared to reduce effort

- **Technical Requirements for eRS:** "Referring clinician role" added to Smartcard of booking teams; Deploy Cinapsis Desktop to booking team machines to permits recognition of Smartcard.

Installer: <https://downloads.cinapsis.org/installer/release/cinapsis-desktop-app.msi>

2hrs

Integration Scope and Resource – IT Tasks involved if integration used

- **Integration into your EPR/PAS or into Medisight is optional** and Cinapsis can function without this in the event you have insufficient IT resource, or you wish to add at a later date
- Please **ensure you engage IT leads to assess resource availability** for deployment and testing
- Cinapsis files encounters to the EPR/PAS (generally sent via the Trust TIE). An integration lead is available for questions if needed. Work would normally commence in line with your Wave if integration is required

Note: If integrating into a Medisoft product, you'll need to be upgraded to the latest version of Medisght. Please liaise with Medisoft to discuss if you have any questions

- **GP Connect viewer can also be deployed if needed**, allowing clinicians to see patient allergies, medications and history during the triage process (no IT effort)

TBD

Checklist - Service Providers (2/3)

Testing Resource - IT Tasks involved if integration used

- Your Clinical, Operational, Booking and IT Leads will be required to **support testing**. We recommend an eRS administrator is available to check/update any eRS setting during testing (if the booking manager does not already have rights)
- IT/Interoperability teams will also be needed to support testing if integration is included in scope
- This should be a good opportunity for you to review **and finalise your SOPs**

1-
2hrs

BI Scope and Resource

- Cinapsis data can be accessed and downloaded by an authorised user if required. Additionally, Cinapsis can flow data on a monthly basis to a secure location (IP and port required), or via NHS Mail. Cinapsis can also send data to the Data Landing Portal (DLP) if this is preferred by the BI Lead
- Cinapsis can provide a data dictionary and sample report for your BI team in advance if this is useful
- **Your BI lead will be responsible for confirming your reporting preferences** in order to support local reporting requirements

30m