

Data Protection Impact Assessment
Covid-19 Vaccination Roll-Out
PharmOutcomes/Outcomes4Health/OcularOutcomes

Project Manager:	Name:	Jamal Syed on behalf Community Care Hall Green
	Title:	IT Manager
	Department:	Managers
	Telephone:	0121 325 5545
	Email	Jamal.syed@nhs.net

Background

Where a proposed new system or process uses personal or sensitive data, or significantly changes the way in which personal data is handled, a Privacy Impact Assessment should be carried out to ensure compliance with the General Data Protection Regulation.

This assessment in this document follows the recommendations of the Information Commissioners Office (ICO) for NHS bodies and helps meet the mandated requirements of the Data Security and Protection Toolkit.

Some of the considerations that need to be taken into account are whether a new system or process will:

- allow personal information to be checked for relevancy, accuracy and validity;
- incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required;
- have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage;
- enable the timely location and retrieval of personal information to meet subject access requests.






Further guidance on specific items can be found on the Information Commissioner's website.

www.ico.org.uk

Information directly from Pinnacle is supplied with evidence where possible or a link to the IG and Technical Specification where more complete information is supplied.

Name: of the system used for data collection	<i>Outcomes4Health</i>
Objective:	Use of Outcomes4Health (O4H) to record patient Covid-19 vaccination details and ensure that the GP record is updated
Background:	There is currently a national programme to roll out the 'flu and covid-19 vaccinations and to support the programme, NHS England(?) has mandated the use of O4H within the STP footprint. This DPIA covers the processing of patient data by PCN's using O4H.
Describe the purpose or main aims of the new system / change in process / policy or system	<p>The 'vaccination programme' within the STP will deliver a staged roll-out the Covid-19 vaccine to patients, according to need. The roll-out needs to factor in the requirement for health professionals to know whether and when the patient has received the 'flu vaccination and the national systems being mandated to capture this data by NHS England and Digital.</p> <p>The following systems are being used to rollout the 'flu and covid-19 vaccinations:</p> <ul style="list-style-type: none"> • NIVS – Nationally mandated system under the COPI regulations. Used for checking and reporting child and staff vaccination uptake. Does not connect back to GP record; • NIMS – System being constructed nationally to support call/recall for flu/covid. Design and technical specifications not available until mid-December. All systems advised to utilise a local plan B; <p>Outcomes4Health (O4H) - The local 'plan B' for the above, which has been mandated for use by NHS England and writes results to the GP direct as part of direct care. Use is mandated for <u>all</u> COVID vaccinations</p> <p><i>The System is a secure, web-based clinical and service management data collection and communications platform that allows patient facing entry of service information and special category personal data. Encryption levels and system design make The System suitable for recording and storing special category patient data and meets the requirements of Data Protection Regulations, including GDPR, and the Data Security and Protection Toolkit.</i></p> <p><i>Service Data, Personal Data and Special Category Personal Data is collected about recipients of health and social care services directly or transferred from other healthcare providers to allow for provision and continuity of care. All data is processed and stored on secure servers to record patient/client interactions then stored for the appropriate retention period set under the current NHS guidelines Records Management Code of Practice for Health and Social Care or as otherwise directed by the Data Controller.</i></p>

	<i>The system also allows the secure transfer of Patient/Client Identifiable Data to other healthcare providers using N3 or HSCN connections and secure NHS mail (e.g. nhs.net).</i>
What are the intended outcomes?	
Benefits:	<p><i>Secure website access to PharmOutcomes/ Outcomes4Health/OcularOutcomes</i></p> <ul style="list-style-type: none"> <i>• Assign provider accreditations according to competencies</i> <i>• Live monitoring and recording of activity</i> <i>• Automatic anonymisation or pseudonymisation for reporting purposes</i> <i>• Automatic invoicing</i> <i>• Live service reporting</i> <i>• Monitored provider communications through system with outcome tracking</i>
Relationships:	<p><i>Service Commissioner: <Service Commissioner></i></p> <p><i>Data Processor: Pinnacle Systems Management Ltd</i></p> <p><i>Service Providers: <Accredited Providers></i></p>

PharmOutcomes/Outcomes4Health/OcularOutcomes System Provider	
Who supplies the system?	<i>Pinnacle Systems Management Ltd</i>
What is the supplier's registered address?	<i>Fulford Grange Micklefield Lane, Rawdon, Leeds, England, LS19 6BA</i>
What is the supplier's contact address and telephone number?	<i>86-88 High Street Newport Isle of Wight PO30 1BH 01983 216699</i>
What is the supplier's Data Protection Officer's (DPO) name and contact email?	<i>Pamela Bowes dpo@phpartnership.com Tel: 01983 216699 Ext 202</i>
Is the DPO suitably qualified?	<i>The DPO is a qualified EU GDPR Practitioner</i>  Adobe Acrobat Document
Is the supplier of the system registered with the Information Commissioners Office (ICO) for data protection (https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/)? If so, please provide details of the registration number and expiry date.	 PSM ICO Registration Certificate.pdf Reg No: ZA112333
Has the supplier of the system implemented ISO27001? If so, please provide a copy of the ISO27001 certification.	 PSM ISO27001 Certificate.pdf Yes.
Has the supplier implemented any other security certification?	 Cyber Essentials Plus Certificate.pdf Yes, Cyber Essentials Plus
Does the contract include clauses related to data protection, confidentiality, consent and freedom of Information?	 PharmOutcomes Commissioner Multipl Yes.

1. INFORMATION ASSET REGISTER AND DATA FLOW MAPPING	
Who is the Information Asset Owner?	<i>(Name, title, department and contact details)</i> Jamal Syed, IT Manager, Hall Green Health, 0121 325 5545, jamal.syed@nhs.net
Who is the Information Asset Administrator/s?	<i>(Name, title, department and contact details)</i> John Hood, Practice Manager, Hall Green Health Marie Quinn, Practice Manager, Swanswell Medical Centre Emma Frost, Practice Manager, Northbrook Group Practice
Has this system been added to the relevant Information Asset Register?	<i>To be confirmed by PCN</i>
What is the Information Asset Register risk rating level?	Risk Rating: Recommended (Medium)
If personal, sensitive or business sensitive data is being processed by the system, has this been added to the relevant Data Flow Mapping document?	Yes
Has a process map been developed which details the process? If so, please provide a copy.	<p><i>For details of various processes please see</i></p> <p>Link to Pinnacle Technical and IG Specification https://phpartnership.com/latest/igfaq</p> <p><i>Pinnacle can help you put together a process specific to your service -</i></p>

2. DATA PROCESSING		
Whom is the information processed about? (please tick ✓ all the related options)		Employees
	✓	Patients
		Partner businesses or organisations
		Other
What are the Data Classes that will be held or processed as part of the implementation or change? (please tick ✓ all the related options)	✓	Person-sensitive details (Patient Demographics – e.g. name, address, postcode, date of birth, NHS number and Vaccination Details – <i>please delete as appropriate</i>)
		Family, lifestyle and social circumstances (marital status, housing, travel, leisure activities, membership of charities – <i>please delete as appropriate</i>)
		Education and training details (qualifications or certifications, training records – <i>please delete as appropriate</i>)
		Employment details (career history, recruitment and termination details, attendance details, appraisals, other – <i>please delete as appropriate</i>)
		Financial details (income, salary, assets, investments, payments, other – <i>please delete as appropriate</i>)
		Criminal proceedings, outcomes and sentences
		Goods or services (contracts, licenses, agreements etc.)
		Racial or ethnic origins
		Religious or other beliefs of a similar nature
		Political opinions
		Physical or mental health conditions
		Offences including alleged offences
		Sexual health
		Trade Union membership
		Other

Will this system include data which has not previously been collected as part of the system or process / policy? If yes, have you amended the existing privacy notice?	Yes Yes
What checks have been made regarding the adequacy, relevance and necessity of data used?	
Are you transferring any personal, sensitive or business data to a country outside the European Economic Area (EEA)? (https://www.gov.uk/eu-eea) If yes, please provide the name of the country.	<i>PharmOutcomes/Outcomes4Health/OcularOutcomes does not store or transfer information outside of the UK unless specifically requested by the service commissioner.</i>

3. Human Resource Security	
Are background verification checks conducted on all employees?	<i>Official documents are checked and references are taken up for all Pinnacle employees.</i>
Are employee's information security and governance responsibilities defined in their employment contract?	<i>Yes these are included in all Pinnacle employee contracts</i>
Do you have and maintain an information security awareness program?	<i>Yes, this is included in Pinnacle staff induction and is regularly updated through staff training meetings</i>
How often are your staff knowledge on data security and confidentiality tested?	<i>Staff are required to do this at least annually based on their role requirements</i>
Are employees mandated to return all information systems assets at the end of their employment?	<i>Yes – this is part of the exit process</i>
What is the time frame for revoking the IT access rights of all employees, contractor and third-party users once they leave your organization?	<i>This happens before employees leave the office on their final day</i>

4. TECHNOLOGY	
Can the system use pseudonyms or work on anonymous data?	<i>PharmOutcomes/Outcomes4Health/OcularOutcomes has the ability to pseudonymise and anonymise data depending on service requirements.</i>
Is Cloud Technology being used? If yes, provide the data centre location.	<i>PharmOutcomes/Outcomes4Health/OcularOutcomes is held on a secure server infrastructure hosted entirely within the UK by Memset Ltd, Building 87, Dunsfold Park, Stovolds Hill, Cranleigh, GU6 8TB and Unit 2, Smallmead Road, Reading, RG2 0QS.</i>
Does the cloud hosting data centre (s) meet appropriate security standards?	<i>Memset operates an ISO 27001 certified Information Security Management System that provides mature, scalable and audited management of security policy, issues and continual improvement.</i> https://www.memset.com/about/security-compliance/accreditations/
How will we be alerted to any possible cloud system or other breaches?	<i>Pinnacle staff will alert data controllers of any possible breaches within 24 hours of them becoming aware.</i> <i>The DPO email address listed on your organisation page for the system is the email address that will be used.</i>
Does the system include new technology that might be perceived as intrusive? (i.e. the use of biometrics or facial recognition etc.)	<i>No</i>
Will the system require access to any Commissioner networks or systems?	<i>The system is accessed via the internet and does not require access to any other systems.</i>
How is the system accessed?	<i>PharmOutcomes/Outcomes4Health/OcularOutcomes is an internet-based system. It will run on any currently supported full featured browser with JavaScript enabled. This includes:</i>

	<ul style="list-style-type: none"> • <i>Internet Explorer 8 or greater</i> • <i>Chrome</i> • <i>Opera</i> • <i>Edge</i> • <i>Firefox</i> • <i>Safari</i>
What encryption standards are applied to communications, data at rest and in transit?	<p><i>PharmOutcomes/Outcomes4Health/OcularOutcomes uses transparent data at rest encryption to aes-128-ctr standard (this is the recommended encryption method for MariaDB), all data is transmitted within a private vLAN and over a VPN.</i></p> <p><i>External connections to PharmOutcomes/Outcomes4Health/OcularOutcomes are encrypted using standard https protocol, and we only accept TLSv1.2 and TLSv1.3.</i></p> <p><i>Backups are stored on an encrypted disk and are GPG encrypted before being stored offsite.</i></p>

5. CONSENT

<p>Is there a legal basis for holding and processing the data?</p> <ul style="list-style-type: none"> Please list any statutory or legal requirements, including localised policies and procedures that are relevant. 	<p>Processing will be on a lawful basis (Article 6 of the GDPR) as Records of Medications and Services provided must be recorded under the Terms of Service in the NHS (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013 Link to regulations</p> <p><i>A Privacy Notice should be given to the patient, detailing how their information will be used. This can be linked to the service within PharmOutcomes/Outcomes4Health/OcularOutcomes</i></p> <p>Link has been put into Hall Green Health's website under Privacy Notice</p> <p><i>Services outside of this remit should capture consent.</i></p> <p>Data sharing agreement already in place between PCN practices. This is covered by direct patient care. Consent to share information with other organisations should be captured.</p>
<p>Do you require the individuals' ("data subjects'") consent to process or hold their data?</p>	<p><i>Consent should be captured where information is to be shared with other organisations. Consent will be given to receive direct care – processing of personal data will be referenced within the privacy notice</i></p>
<p>If an opt-out option is available, how will this be managed?</p>	<p><i>If patients do not consent to their information being shared, notifications will not be generated and/or reports will not contain this patient's information. No opt-out available – direct care purposes</i></p>
<p>How will you tell the data subjects about the use of their data?</p>	<p><i>Privacy Notices can be attached to PharmOutcomes/Outcomes4Health/OcularOutcomes to be printed off for the patient.</i></p>
<p>Have you assessed the likelihood of the use of the data causing unwarranted distress, harm or damage to data subjects concerned?</p>	<p><i>The data being captured is only data around the patient's COVID vaccination status. As such it the likelihood of distress or harm being caused is low.</i></p>
<p>Have you assessed the likelihood of the loss or damage of the data causing unwarranted distress, harm or damage to data subjects concerned?</p>	<p><i>Pinnacle regularly carries out a full security risk assessment, and appropriate processes and</i></p>

	<p><i>procedures are put in place to protect the information held.</i></p> <p>Link to Pinnacle Technical and IG Specification https://phpartnership.com/latest/igfaq</p> <p>Data Processed relates to health but would not have a <i>serious</i> impact on privacy if compromised.</p>
<p>Could the project result in making decisions and / or taking action against the data subjects in ways that can have a significant impact on them?</p>	<p><i>No, the processing is intended to assist direct care and recording vaccination details – it should not lead to significant decisions being made about them.</i></p> <p><i>This data will not affect significant decisions about patients. This will similar to previous vaccination programs within the public health domain.</i></p>

6. ACCESS TO THE DATA	
Who will use the system or process and have access to the data?	<p><i>PCN staff will have access to Pinnacle for the direct purpose of direct patient care. All staff provided access will have signed confidentiality agreements for their respective practices.</i></p> <p><i>Service Providers – Full patient and service information</i></p> <p><i>Commissioners – anonymised patient and service information</i></p> <p><i>Where PID access is required this can be granted subject to a written justification and confirmation that appropriate patient consent is in place.</i></p> <p><i>Pinnacle staff and their partners will have access to provide support and resolve any technical issues. As far as possible, support is given without accessing patient-identifiable information.</i></p>
What training have users had in patient confidentiality?	<p><i>Service Providers – PCN staff are being deployed from Practice staff. These staff are covered by their practices DSP Toolkits.</i></p> <p><i>Commissioners -</i></p> <p><i>Pinnacle staff have full training in information governance using nationally recognised and internal training courses.</i></p>
How will the users access and amend data?	<p><i>Through secure access to PharmOutcomes/Outcomes4Health/OcularOutcomes online system.</i></p>
Is there a secure password policy in place on the system?	<p><i>All passwords must adhere to the rules for construction as defined in our Password Policy.</i></p> <p><i>Access to patient-identifiable information also requires a six-letter word generated by the</i></p>

	<p>system. Users are required to use this every time they wish to access PID.</p> <p>The security word is also used to re-access the system if it times out during any periods of inactivity.</p>
How often do users have to change their password?	<p>Password Term: We are moving away from forcing password changes following the guidance of the National Cyber Security Centre which has determined that this makes systems less secure. This can be changed at the request of the commissioner to meet their own policy.</p>
Is there a usable audit trail in place for the information asset?	<p>For security and audit purposes, the system retains a full log of log-ins and service provisions; the records are auditable given an appropriately authorised and legal request to do so.</p>
How often will the system or process / policy be audited?	<p>Live service auditing is available on PharmOutcomes/Outcomes4Health/OcularOutcomes.</p>

7. STORAGE OF THE DATA		
Where will the data be stored?	<p><i>PharmOutcomes/Outcomes4Health/OcularOutcomes live data is held entirely within the UK by Memset Ltd, Building 87, Dunsfold Park, Stovolds Hill, Cranleigh, GU6 8TB and Unit 2, Smallmead Road, Reading, RG2 0QS.</i></p> <p><i>Pinnacle uses Amazon Web Services (AWS) for our DNS and Database Backups. All communication with S3 is over secure HTTPS and the data stored is encrypted to AES-256 on Pinnacle Servers before being transferred to S3.</i></p> <p><i>AWS is ISO27001 accredited and restricted to the London region to ensure data never leaves the UK.</i></p>	
Does the system or process change the way data is stored?		
Which format will the data be stored in? (please tick V all the relevant options)	<input checked="" type="checkbox"/>	Electronic
	<input type="checkbox"/>	Paper
	<input type="checkbox"/>	Verbal
	<input type="checkbox"/>	Other

8. DATA SHARING	
<p>Will the data be shared with any other organisation/s?</p> <p>If yes, please list the names of the organisation/s.</p>	<p>Anonymised data is shared with <Service Commissioner and National Immunisation Service></p> <p><Notifications> <i>Notification are sent from the system to the registered GP practice</i></p>
<p>How will the data be shared?</p>	<p><i>Any patient-identifiable data will be sent via PharmOutcomes/Outcomes4Health/OcularOutcomes securely over an N3 or HSCN connection or via secure email (eg nhs.net).</i></p>
<p>Are there any Information Sharing Agreements or Protocols in place to support the sharing of data? If so, please provide a copy.</p>	<p><i>Terms of service include a data processing agreement as part of the national mandate</i></p>
<p>Is there a Data Processing Agreement in place?</p>	<p><i>A Data Processing Agreement (DPA) must be in place between Data Controllers and Data Processors (Pinnacle) as there are specific clauses determined by GDPR. Pinnacle licence agreement has a DPA built in</i></p> <p><i>There are Data Processing Provisions within the service level agreement which practices accept when using the system.</i></p>

9. PHYSICAL SECURITY OF DATABASE HOSTING	
Please describe the physical access control mechanism in place within your organization's work area and data centers?	<p>The physical security baseline of Memset data centres is aligned to most commercial security standards, including ISO 27001:2013, PCI-DSS v3.2, PSN CoCo and the requirements of data marked OFFICIAL.</p> <p>The data centres individually exceed normal commercial good practise with controls such as IL4 alignment, Class 3 strong-room construction, ANPR vehicle entry controls or the use of vibration sensors on exterior walls.</p> <p>https://www.memset.com/about/security-compliance/accreditations/</p>
Do you monitor/log all access to data center?	Every system within the data centre is monitored and controlled from the on-site control room and maintained 24 x 7 x 365.

10.DATA SECURITY	
What security measures have been undertaken to protect the data?	<i>Pinnacle has an Information Security Management System in place which is certified to ISO27001.</i>
What security controls are in place to keep data separate from other client data?	<p><i>Our system rely's on role based authorisation to access any data. All users start with the minimum amount of privileges, needing to request for elevated access.</i></p> <p><i>The system checks at multiple stages to see if a user is allowed to access information, and will always default to "not allowed" if it's unable to ascertain a positive outcome.</i></p> <p><i>The only time your information will be viewable by someone else is if you have actively sent it to them or granted consent (e.g. via a service template / referral to pharmacy).</i></p>
<p>What business continuity plans are in place in case of data loss or damage?</p> <p>(i.e. as a result of human error, virus, network failure, theft, fire, floods etc.)</p>	<p><i>Pinnacle has a comprehensive Business Continuity Plan in place which is tested on a regular basis.</i></p> <p><i>The disaster recovery and business continuity arrangements for PharmOutcomes/Outcomes4Health/ OcularOutcomes are part of the core design of the system. Failover protection is provided by dual load-balancing servers and multiple (three) web-servers. As soon as records are saved by a contractor on the platform, e.g. by clicking a 'Save' button, a record is made on the</i></p> <p><i>PharmOutcomes/Outcomes4Health/ OcularOutcomess database system which is located in England, and an identical copy is replicated onto another three servers in two distinct data centres.</i></p>

How often are your servers patched with critical and security updates?	<i>Pinnacle has a program that scans for critical and security updates every morning and identifies which can be applied safely without human intervention and which should be reviewed before updating. The latter are then reviewed by our development team and updated where appropriate.</i>
How often is external penetration testing carried out on the system?	<i>Independent penetration testing is carried out on the system at least twice a year. Follow-up testing also ensures that any issues raised by the testers have been addressed effectively.</i>
How are changes to the system managed?	<p><i>Pinnacle has internal procedures which ensure development and testing takes place in a secure environment before being uploaded to the main system. Our processes and procedures meet the requirements of ISO 27001 and are regularly reviewed and updated where necessary.</i></p> <p><i>As the system is accessed via a web portal, no software updates are required. Updates are planned to take place outside of main working hours and to cause minimal disruption. Changes are managed and tracked through a shared issue tracking system. Staff record changes required and can track progress through prioritisation, development, testing and completion.</i></p>
How often is information backed up?	<p><i>There is a regular programme of backups for the system using the following timetable:</i></p> <p><i>10 x 4-hourly + 7 x daily per week</i> <i>Offsite backups 7 x daily per week</i></p> <p><i>Data backups are retained for 90 days before being overwritten in rotation. Data backups are only used for system failures, but Pinnacle receives a restore image once a month which is verified and actively restored on a secondary server to assure the disaster recovery process.</i></p>

11. DATA QUALITY	
Who provides the information for the asset?	<p><i>The service commissioner determines the information to be collected, and the accredited service providers enter the information requested from patients.</i></p> <p><i>For some services the initial data may be received into the system via secure N3 or HSCN Connection from another healthcare system such as referrals from a hospital, GP or NHS111 Call centre</i></p>
Who inputs the data into the system or process?	<p><i>Data is entered directly into the system at point of service by the accredited service providers.</i></p>
How will the information be kept up-to-date and checked for accuracy and completeness?	<p><i>This is the responsibility of the service provider and the service commissioner.</i></p> <p><i>PharmOutcomes/Outcomes4Health/OcularOutcomes can assist in this process with the use of mandatory fields and drop-down lists.</i></p>
Can an individual (or a court) request a copy, amendments or deletion of data from the system?	<p><i>This is easily accommodated by the system given an appropriately authorised and legal request to do so.</i></p> <p><i>This will only be done with the full knowledge and permission of the Service Commissioner.</i></p>

12. ON-GOING USE OF DATA	
Does the system or process / policy involve changing the standard disclosure of publicly available information in such a way that the data becomes more readily available than before?	No
What is the data retention period for this data? (please consult the detailed retention schedule (appendix 3) in the link below) https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016)	<i>Details of the vaccination processed through Pinnacle will be read to the GP system and retained within the patient record held by the GP.</i>
Please describe your hard copy data destruction process?	<i>No hard copies are held by Pinnacle. If any sensitive information is sent to us this is destroyed using a secure destruction service which supplies us with certificate of destruction.</i>
How will the data be securely destroyed when it is no longer required?	<i>See deletion process in attached documentation</i> Link to Pinnacle Technical and IG Specification https://phpartnership.com/latest/igfaq
Will the data be used to send direct marketing messages?	<i>PharmOutcomes/Outcomes4Health/OcularOutcomes will never use the information for this purpose.</i>
If direct marketing messages will be sent, are consent and opt-out procedures in place?	<i>There will be no direct marketing activity taking place</i>