POPULATION HEALTH MANAGEMENT
Data protection impact assessment (DPIA)
V1.4

Version number	Updates	Date signed off
V1	First version developed by PHM Information Governance Working group and distributed for sign up	May 2021
V1.1	Minor updates	May 2021
V1.2	Minor updates	June 2021
V1.3	Minor updates	June 2021
V1.4	Review. Standardised coversheet, removal of reference to PHM Development programme and hosting of data in Optum servers, reference to new governance structure, update on user management processes, update on subject access request process, update on opt out process, add ICB as lead controller	October 2022

Date of next review:	October 2023	If not triggered by other trigger event

Project Details

Name of Project
Hampshire and Isle of Wight Integrated Care System, Population Health Management Programme
Brief Summary of Project
Establishment, by providers & partner organisations working collaboratively across the patient journey, of a jointly managed data platform to put existing data to better use, as determined by clinical leaders, by: • Understanding the needs of the care system's population, including health inequalities • Targeting support to where it will have the most impact, using segmentation and stratification toolsets • Identify early actions to keep people well, not only focusing on people in direct contact with services, but looking to join up care across different partners Contracted clinical use cases include: • Identify patients with high resource utilisation or rising risk of high utilisation across and within the health & care system • Identify risks of complication from chronic disease • Identify patients at risk of frailty and adverse events • Identify patients at risk of disease development • Assess patterns of service utilisation, morbidity and mortality across the local population and other segmentations • Case finding services – single condition (i.e. Type 2 Diabetes / Chronic Obstructive Pulmonary Disease / risk of Cerebrovascular event / deterioration of condition) • Gaps in care analysis – (i.e. primary prevention in higher risk groups patients in 'health' groups); condition management; medication review and adherence • Primary care support, enablement, admission and utilisation reduction, COVID; support, recovery and restoration.
Estimated Completion Date
The end point contract with Cerner is a key review point. The PHM programme will continue and evolve but platforms/uses will change and DPIA will need review as part of that.
Name of Project Lead
Faye Brooks, Head of Population Health Management
List all organisations involved in the project
ICS organisations All partners will be invited to participate and sign the Data Sharing

Agreement

Details of person conducting DPIA

Name
Faye Brooks & Adam Horton-Tuckett
Position
Head of Population Health Management & IG Consultancy Lead
Contact Email Address
faye.brooks@nhs.net, adam.tuckett@nhs.net

Step 1: Confirm the need for a DPIA and the main areas to consider

Does the project involve… (mark all that apply)
☐ The collection of new information about individuals
☐ Compelling individuals to provide information about themselves
☒ The disclosure of information about individuals to organisations or people who have not previously had routine access to the information (in this case on a limited basis)
☐ The use of existing information about individuals for a purpose it is not currently used for, or in a way it is not currently used
☐ Contacting individuals in ways which they may find intrusive
☐ Making changes to the way personal information is obtained, recorded, transmitted, deleted, or held
☒ The use of profiling, automated decision-making, or special category data[1] to make significant decisions about people (e.g. their access to a service, opportunity, or benefit).
☒ The processing of special category data[1](which includes health data) or criminal offence data on a large scale.
☐ Systematically monitoring a publicly accessible place on a large scale (e.g. CCTV)
☐ The use of new technologies.
☐ Carrying out profiling on a large scale.

[1] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

☐ Processing biometric or genetic data.

☒ Combining, comparing, or matching data from multiple sources.

☒ Processing personal data without providing a privacy notice directly to the individual.

☐ Processing personal data in a way which involves tracking individuals' online or offline location or behaviour.

☐ Processing children's personal data for profiling or automated decision-making or for marketing purposes or offer online services directly to them.

☐ Processing personal data which could result in a risk of physical or mental harm or distress, identity theft, fraud, financial loss or other detriment in the event of a security breach.

If you answered "yes" to any of these, please proceed to Step 2.

If none of these apply, please tick the box below.

☐ None of the screening statements in Step 1 of this document apply to the project, and I have determined that it is not necessary to conduct a Data Protection Impact Assessment

Step 2: Describe the processing

Describe the purposes of the processing

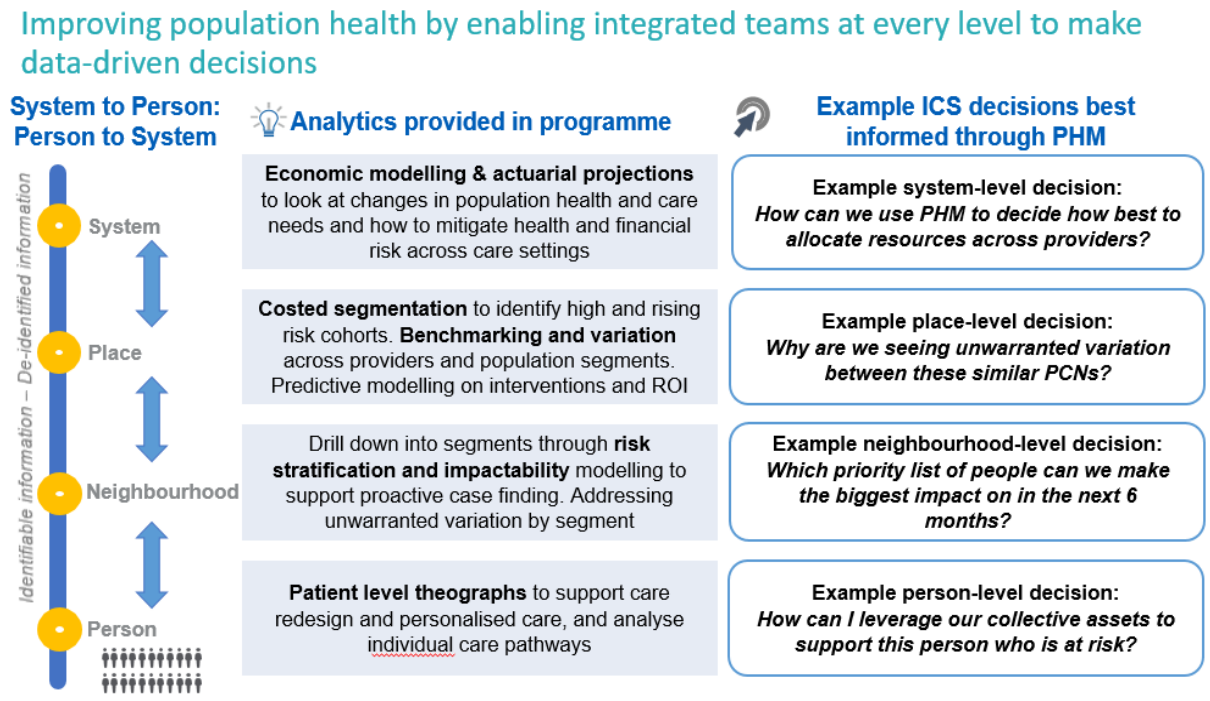
What does the project want to achieve?

Embedding Population Health Management (PHM) in patient care and decision making throughout Hampshire and Isle of Wight ICS is a key goal of the ICS as it works to improve patient care and to improve preventative care.

Having access to high quality data through a PHM approach is also a key system capability outlined in NHSE/I national ICS planning guidance.

The PHM programme seeks to improve understanding of the population's health to provide insights into the needs of the population now, as well as their needs for the future, the impact of services that we put in place and bringing data together to provide a holistic view of individual people in the population.

As described in the diagram below, Hampshire and Isle of Wight ICS's PHM programme seeks to embed PHM approaches into all levels of decision making throughout the region, from GP practice and Primary Care Network level, to supporting strategic decisions across the ICS.



To achieve these goals, the programme will bring together data sources from across health and care into a 'single source of truth', linking data in a safe and secure digital environment. This data will be accessed through a purpose-built platform, displayed through an easy-to-use set of dashboards providing clinical and data analysis.

Users from a range of organisations and roles across health and care in Hampshire and Isle

of Wight will be able to access population data enabling front line users, analysts, commissioners, and financial teams to better understand the impact of changes in the region, from patient to system level.

To get the best out of the improvement in access to high quality data, the programme will also wrap around a programme of training, support, and leadership to ensure that people from across the system have the skills to be able to understand and use the data effectively.

What is the intended effect on individuals? (Directly or indirectly)

The use of high-quality data through a PHM approach will have both direct and indirect impact on individuals across the region.

By bringing together multiple data sources into one, easy to access record, health and care staff caring for individuals will have better access to data supporting improved care, reducing duplication, and improving care targeted more precisely to the needs of individual.

Data driven decision-making across local, neighbourhood, place and system level will also lead to indirect benefits for most of the 1.8 million individuals living and working in the Hampshire and Isle of Wight ICS region. Basing commissioning decisions on high quality data from across a wider pool of sources will enable a more holistic view of the needs of the population, enabling services to be developed to meet those needs with greater accuracy and responsiveness, improving the care for those individuals. Data driven commissioning and prioritisation will also enable a more targeted use of resources, enabling resources to be appropriately allocated to where they are needed most and to reduce waste and inefficiency.

PHM approaches across Hampshire and Isle of Wight will also enable targeted, data driven interventions aimed at improving health and social inequalities across the region thus improving the health and wellbeing of the population of the region.

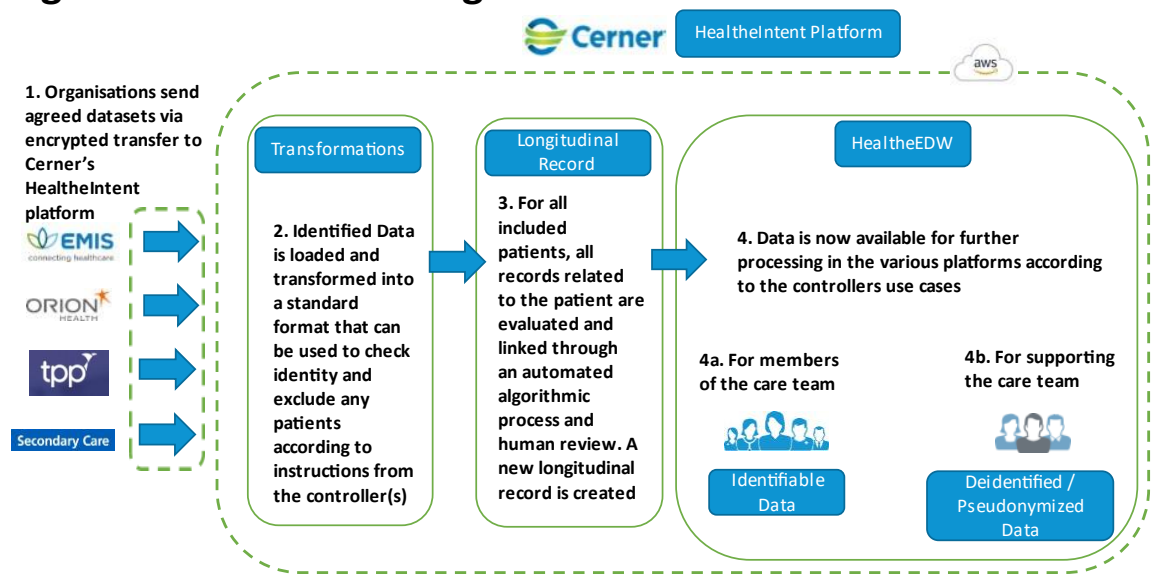
The nature of the processing

(NB the use of detailed data flow maps may well support answers to a number of the questions below).

How will the project collect data?

ICS partner organisations, agreeing to the sharing of data they control, will supply data to the Cerner HealtheIntent platform, via secure file transfers using the HealtheIntent Data Upload Utility (HIDUU). Data collection will be from existing operational systems in partner organisations. The exact method of data extraction differs slightly for general practice and further detail is on page 21). NHS digital Secondary Uses Services (SUS) data is provided by North of England Commissioning Support Unit (NECS) via secure file transfer (sFTP) directly into the Cerner secure server environment.

High Level Data Flow Diagram



How will the project use the data? Will any automated decisions be taken with a significant effect on individuals?

There will not be any fully automated decisions taken. Reports and dashboards will be developed and made available to end users, that is, the professionals currently providing care to individuals or supporting the provision of such care. The development of these will be clinical/care driven. These will be used to support decisions on delivery of care and development of care services.

End user's access (professionals providing care to individuals or supporting care provision)

Two levels of data granularity will be available to end users when accessing reports and dashboards:

1. The executive level displaying overall system numbers and trends with drill down capabilities to an organisation or to cohorts that make up population segmentation. At this level, role-based access control is applied and that allows or restricts a user from accessing a report or a dashboard.

2. The patient level that provides information on persons that make up a particular cohort, stratified by risk or level of care needed, with the aim of improving the health outcomes of those individuals. At this level users can have access to patient identifiable information. A relationship-based access control will restrict the view of the user so that they only see data of those persons holding a legitimate relationship (affiliation or attribution) with their organisation(s).

End user access (no direct care relationship with individual)

Two levels of data granularity will be available to end users when accessing reports and dashboards:

1. The executive level displaying overall system numbers and trends with drill down capabilities to an organisation or to cohorts that make up population segmentation. At this level, role-based access control is applied and that allows or restricts a user from accessing a report or a dashboard.

2. Row level that provides information on persons that make up a particular cohort, stratified by risk or level of care needed, with the aim of improving the health outcomes of those individuals but with hidden identifiable information. At this level users cannot see identifiable information as they have no legitimate relationship with the patient to see this information.

Analyst access (development of reports and dashboards)

Two levels of data access will be in place for analysts and their access to the PHM platform will reflect the form of access they currently have to other data sources.

1. Analysts who are not allowed to see patient identifiable data will still have access to all HealtheAnalytics Tools and Data Models for an unidentified population. This will allow analysts to query data, build data sets and data models and build visuals for end-user consumption without accessing any patient identifiable information.

2. The same tools and Data Models will be available from an identifiable population. This population can be accessible to a smaller pool of analysts for use cases that require that type of access.

In both populations (identifiable and unidentifiable) the role-based access controls apply, allowing or restricting an analyst from seeing, modifying or creating a new report or dashboard.

Additionally, a relationship-based access control can be in place for analysts when viewing reports and dashboards from the identified population, restricting their view to the organisation they belong to.

How will the project store the data?

Data is stored in a cloud-based platform managed by Cerner and hosted within Amazon Web Services (AWS) in the EU West 2 – London Region. Cerner utilises AWS Virtual Private Cloud (VPC) architecture to isolate its infrastructure from the rest of the AWS infrastructure. We are following the established AWS Shared Responsibility Model to establish division of responsibilities between the AWS managed physical infrastructure and the Cerner managed application/platform.

Cerner is responsible for managing the platform, the applications, the Identity and access management as well as the operating system, network and firewall and client and server-side encryption. Cerner employees in the infrastructure team have no access to patient level data. Access to both the infrastructure and data is strictly controlled by a need-to-know access and business operations model.

AWS is responsible for the so-called foundation services, which includes the compute,

storage, database and networking and the AWS global infrastructure which includes the availability zones, regions, and any edge locations.

AWS will not have access to any data, or the encryption keys and they will not process data belonging to Cerner clients. AWS staff cannot access any identifiable data stored within HealtheIntent.

AWS consistently maintains third-party validation for thousands of global compliance requirements and continually monitors many industry sectors (including SOC reporting). Cerner encourages clients to review their documentation that is posted on their website (https://aws.amazon.com/compliance/programs). Documentation available includes industry-recognized security, environmental as well as health and safety certifications. AWS holds the following relevant security certifications for its data centre operations: ISO 27001, ISO 27017, ISO 27018, HIPAA, EU GDPR Compliance, SOC 1 Type II, SOC 2 Type II, and CSA Cloud Security Alliance Controls amongst other relevant regional certifications.

Cerner utilises Amazon's Simple Storage Service (S3) for object storage. All data within S3 is encrypted at rest to AES 256 and in transit to TLS up to version 1.3 with a cypher strength of 256 bits. In addition to encryption, access control is explicit to only Cerner associates who have explicitly been granted permission to specific S3 buckets they have business reason to access. There are so called bucket policies that check and restrict any kind of data transfers that are not using transport layer security (TLS). If there is an attempt to send data to any S3 buckets not using encryption, Cerner has the configuration set up so that the bucket will refuse the transaction/transfer.

Cerner utilises Amazon Elastic Block Store which are attached to Cerner's EC2 instances and use encrypted EBS volumes using industry standard encryption.

How will the project delete the data?

Deletion (following expiry of retention period or on request): Retention of data will follow the NHS Records Management Code of Practice and any other relevant guidance (e.g., Local Government Association) applicable at the time. When a retention period is reached or a specific request is made, then data can be deleted from the system. If data is deleted in one of the systems linked to HealtheIntent, then any 'delete' flag sent during data updates will be picked up by HealtheIntent and that data also deleted from the system.

What are the sources of the data? NB if data from NHS Digital is required, specific advice must be sought to ensure correct permissions are either in place or gained.

Each partner organisation agrees the dataset to be submitted to the platform from their systems. (NB. one common dataset for General Practice, possible variations depending on differing system suppliers).

NHS Digital Secondary Use Services (SUS) data is included following approval via NHS Digital DARS process (DARS numbers DARS-NIC-291482-X5N6H-v0.2 and DARS-NIC-412777-Z2J9N-v0.2) . Cerner are also approved by NHS Digital as a recipients of NHS Digital data for risk stratification purposes. https://www.england.nhs.uk/publication/list-of-risk-stratification-

approved-organisations/
Will the project require the sharing of data with other organisations?
INFO: If yes, please provide details of other organisations
Yes. The aim of the programme is to develop two main uses and benefits of data sharing, namely: Intelligence supported individual care delivery with the use of tools for cohort identification, risk stratification for specific conditions and patient tomographs of care pathways. Data is therefore shared with partners who have a care relationship with the individual. A de-identified data repository supporting the development of care services across the Integrated Care System. The de-identified data from multiple sources is therefore shared with partners whose organisational function is to support the development of care services.
If so, how will the data be shared? For example, will it be exchanged between parties or stored in a shared repository?
Data will be stored in a repository (see diagram above). Access will be to end users accessing the system via reporting tools and dashboards created by analysts/developers.
If the data is being shared, will this be governed by an agreement (e.g. contract, data sharing agreement, data processing agreement)?
The basis for sharing and use by partners in the PHM programme is governed by the PHM Data Sharing Agreement, setting out the legal gateways enabling organisations to share data, the lawful basis for use (related to partners statutory functions) and how uses will be clinical/care led and overseen, and how the arrangement will be jointly managed.

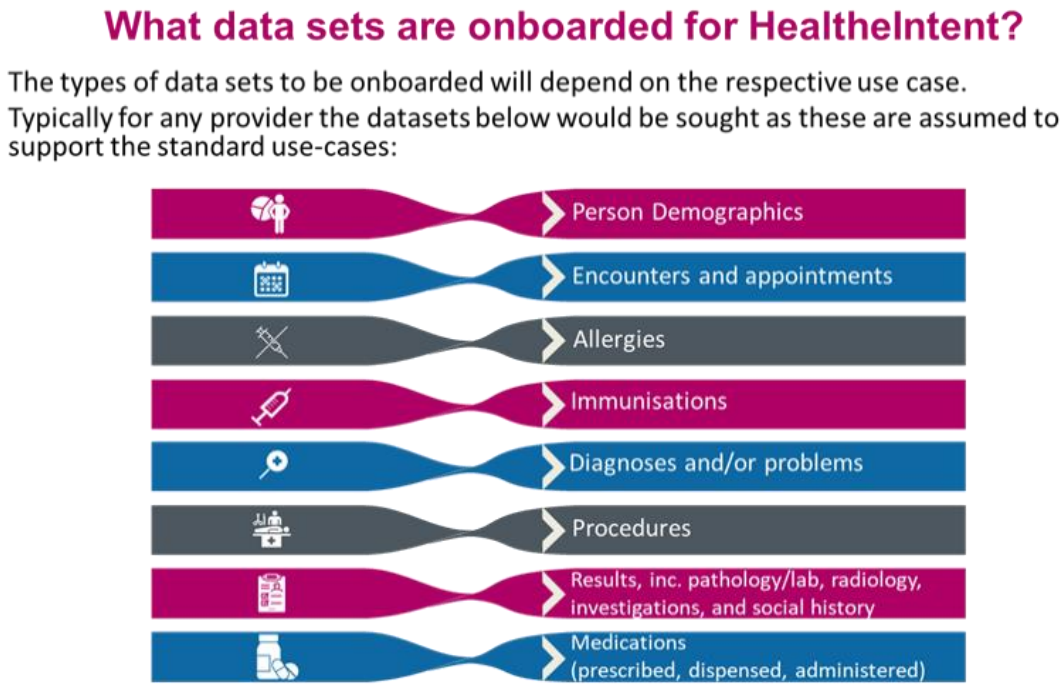
Describe the scope of the processing
What is the nature of the data?
INFO: Detail the type of personal data being processed. List any fields that will be processed (e.g. name, address, data of birth, NHS number, video images)
These sections describing the 'scope' of processing are not intended to be a full list of all data items that will be included as that will develop and change overtime. Each partner contributing data will be in control over the data they agree to provide as part of the 'onboarding' process. Some partners will in time provide data from multiple systems. Cerner maintain a 'wiki' which identifies the sources of data, what data is included from that source and the format. This can act as the core reference point for any queries around specific data items being shared. The partnership Information Asset Owner will liaise with Cerner to ensure this is in place and maintained.

Does it include special category or criminal offence data? Please provide details.

INFO: "Special category" data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special category data will be included in the following ways and for the following reasons:

- Race/ethnic origin – to permit analysis related to health inequalities
- Religious beliefs – to permit analysis related to 'hard to reach' groups as proven necessary during the Covid-19 pandemic
- Data concerning health and care – fundamental to the provision of care or activities to support care provision. (See diagram below for the high-level categories of health & care related data)



In terms of future inclusion of additional data items and management of risk, it is unlikely any other forms of 'special category' personal data, other than the above will be included.

The platform has the functionality to screen and restrict 'sensitive data items' and for any significant development where concerns are raised this will be considered.

How much data will the project be collecting and using? (Describe the scale and scope of the project, i.e. how many individuals are affected? What's the geographical or organisational reach?)

The programme will be collecting data on all residents in Hampshire and Isle of Wight who are in receipt of health and care services from engaged partner organisations.

Filters will be applied so that:

- Data on patients who are not HIOW residents (i.e. not registered with HIOW GP or don't have a HIOW postcode) are excluded
- Patients whose records are coded with an 'opt out' of data sharing for individual care will be excluded from all data sets, and data will not appear in any reports, dashboards or data sets.
- A list of 'sensitive' data items will also be maintained so that specific codes if appearing on records are also excluded.
- Patients who are identified as 'sensitive' on the NHS spine are excluded from all data sets

How often will the data be collected and used?

Data collection ideally will be daily where possible to ensure accuracy, though will vary dependent on the frequency that each data source can provide updates

How long will the personal data be kept?

INFO: Where possible please specify a time period linked to current NHS and Social Care records management and retention schedules.

Data will be held in line with the current version of the NHS Records Management Code of Practice. Any Local Authority data will be held in line with Local Government Association guidance.

Any deletions from data sources, where that system can send a 'delete' flag to HealtheIntent will also see that data deleted from HealtheIntent.

Describe the context of the processing
What is the nature of the relationship with the individuals?
INFO: Detail who the data subjects will be (e.g. patients, clients, service users, staff, professionals)
Subjects will be patients and clients of organisations in the PHM partnership. These are individuals in receipt of health and care services within the scope of the Hampshire and Isle of Wight Integrated Care System. Data on partner staff will also be included in the system but this will only be in relation to their professional role in delivering care services, their user account details and audit trails of their use of the system.
How much control will they have over their data?
Within the Hampshire and Isle of Wight Integrated Care System public engagement is part of a wider activity under the 'Wessex Care Records' programme that is incorporating both shared care records and other uses of data and will be used to gain public views on uses of data across the ICS including the PHM programme. Output of the forum will be considered as required by the PHM programme. Where an individual has an existing 'opt out' of data sharing for individual care on any partner system that feeds the PHM platform, that opt out will be applied. These are generally recorded on GP systems. That will mean their data will be excluded from all data sets, and data will not appear in any reports, dashboards or data sets. Individuals who do not have an opt out noted on their GP record, but subsequently do have one applied, will see that opt out carried through into the PHM platform. The National Data Opt-out for the NHS will also be respected, noting that use cases that trigger the engagement of the NDO are unlikely within the use of the PHM platform as use will either be de-identified data or individual care related. The NDO will be implemented when NHS Digital SUS data is being used in analytics, in line with the requirements of the DARs. The removal of data for NDO will be done at source for this data source. Any proposed use case that supports individual care, and proposes to use confidential patient information (as defined in the NDO policy: Appendix 6: Confidential Patient Information (CPI) definition - NHS Digital) will likely require both support of Section 251 of the Health & Social Care Act (approved by the National Confidentiality Advisory Group) and to ensure that checks with the National Data Opt out are built into the processes. Application of NDO to the PHM platform can be categorised in terms of use as follows: 1. Individual care (direct care) – NDO does not apply 2. Supporting individual care but with de-identified data only – NDO does not apply 3. Supporting individual care with identifiable data – NDO would apply unless that particular use has sought section 251 support that includes an approved NDO waiver. Should any individual make a formal objection to the use of their data (under their UK GDPR article 21 rights), this will be considered on a case by case basis and responded to appropriately. There are a number of technical options to restrict the availability of data,

depending on the uses that are causing concern. The programme will support any organisation dealing with such a case to set out the options available at the time. The 'informing' activities will also emphasise the benefits for individual care and the assurances of other activities using de-identified data.

Would they reasonably expect their data to be used in this way by these organisations?

INFO: Please provide details to support the answer

Requirements on data subject expectations vary for the different uses of the data.

Individual care uses:

For individual care uses, many studies have shown the majority of patients expect their data to be shared between the organisations providing their care to ensure that they are provided with the best possible care. These studies have also shown the majority of patients are surprised when this is not done. This expectation is mainly when the patient is present with a care professional. The PHM platform will use role-based access to ensure that identifiable data is only available to those with an individual care relationship to the individual(s).

Caldicott review 'to share or not to share' (2013) noted:

The Review Panel found a strong consensus of support among professionals and the public that safe and appropriate sharing in the interests of the individual's direct care should be the rule, not the exception. (To share or not to share, executive summary, 2013)

PHM will be used to identify patients 'at risk of' and may see some shift to more proactive care provision activities than is currently the case. Expectations of patients for their data from multiple sources to be analysed to identify them for different beneficial interventions is perhaps not so strong as access to records at the point of providing care but some level does currently take place. The experience of the Covid 19 pandemic will have significantly increased the public's understanding with patients being identified for 'shielding' and also for prioritisation for vaccine provision being similar 'risk assessed' use of data for direct care. This will enable care professionals to:

- Provide best care to people who are already diagnosed with a condition
- Identify those with undiagnosed conditions
- Identify those who are at imminent risk of getting a condition with a view to preventing the condition materialising.

De-identified uses supporting the provision of care

Where the use of data does not need the identity of the individuals, then this also fits with the expectations of patients identified in national studies (e.g. National Data Guardian 'Review of data security, consent & opt-outs' – see section3.2.25 – 3.2.28).

Note, any potential uses of 'confidential patient information' as defined in the National Data Opt out policy, will be specifically considered and assessed by PHM governance structure taking account of any need for S251 support or other specific legal basis to process such data.

Transparency

The above shows that there is a reasonable level of public acceptance about the uses of data in the ways that the PHM platform will provide. However, noting the expectations are derived from national work conducted some years ago, partners in the PHM programme must assess and where required enhance their engagement with the public that support such expectations and deal with any individual concerns raised.

The PHM programme will support partners to ensure that messages they make available as part of engagement activity are accurate and up to date with reference to the PHM programme; and, that feedback from engagement activity is considered by programme leadership.

The PHM programme will align with ICS comms and engagement strategy which is likely to include ICS-wide communication with individuals on the way that data is used in health and care across the ICS.

Do they include children or any vulnerable groups?

INFO: If yes, please provide details

Yes, there is good reason to include children and vulnerable individuals in activities designed to improve either their care or services provided to them. To not do so would be potentially discriminatory to these groups that need support.

Where systems/apps are used to collect, store, share or otherwise process the data, please describe the overall security mechanisms to prevent unauthorised access, damage, loss or other risks to the security of the data.

INFO: please detail items such as access controls (logins, passwords, timeouts), encryption (at rest and in transit), database/data centre security, security accreditations, penetration tests, vulnerability scans etc

Procurement process – security definition and contracted schedules:

The PHM platform has been procured via the HSSF (Health Systems Support Framework) developed via NHS England. The Health Systems Support (HSS) Framework provides a quick and easy route to access support services from innovative third-party suppliers at the leading edge of health and care system reform, including advanced analytics, population health management, digital and service transformation. The suppliers on the framework have passed rigorous selection criteria to ensure their products are of a high quality, their prices fair and their financial position stable.

The procurement process utilising the core HSSF templates set a detailed requirements specification for Information Security and Information Governance and this is now covered in detailed contract schedules. The schedules require the supplier to provide an Information Security Management System (ISMS) to the customer and this has been done by Cerner.

Good Governance

The ICB IG Advisory Panel will consider whether governance and management

arrangements for the programme meet the standards set out in the DSPT and other relevant bodies. It is incumbent on every partner to meet the standards required in order to protect other members of the partnership and maintain confidence in the system.

Information Asset Management

The ICB Chief Information Officer will be the information asset owner on behalf of the partnership.

Data Security and Protection Toolkit, including CyberEssentials+

The IAO will make an annual report on DSPT outcomes of all participants and suppliers to the ICB IG Advisory panel. The panel will advise the PHM Programme Governance of any concerns.

Additional information relating to the suppliers is set out below:

Data centre/hosting security:

Cerner

Cerner's Healtheintent Platform is hosted within the EU West 2- London region in Amazon Web Services (AWS) and utilises virtual private clouds, (VPCs) to isolate from the rest of the AWS infrastructure. A VPC is an on-demand configurable pool of shared resources allocated within a public cloud environment. The AWS hosted solution will utilise multiple, separate VPCs. A Production VPC where all the actual code, hardware and infrastructure will reside in and a separate Management VPC which engineers and operations will use though a bastion host, (a special purpose computer on a network specifically designed and configured to withstand attacks). Cerner will also deploy a management tooling system in the management VPC to help with operational matters. This discourages and limits any manual management of systems in the Production VPC. Cerner also has VPC peering set up between the two VPCs for communication. The AWS Region upon which the Cerner HealtheIntent platform is hosted contains multiple Availability Zones (AZ1, AZ2 and AZ3) which all provide redundant power, networking, and connectivity to reduce the likelihood of two zones failing simultaneously. All AZs within an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fibre providing high-throughput, low-latency networking between AZs. All traffic between AZs is also encrypted. AZs are physically separated by a meaningful distance, many kilometres, from any other AZ, although all are within 100 km (60 miles) of each other. Using AWS does not change the way Cerner manages its security program, nor does it provide AWS with access to Cerner's systems or networks.

NECS

Data is stored within encrypted databases and held within the NECS ISO 27001 compliant data centre. Data is encrypted at rest, and in transit.

Security:

NECS have IT Security accreditation in place governing their current practices (either ISO 270001, CyberEssentials or both). They are also all compliant with the NHS Digital Data Security and Protection Toolkit.

Cerner Compliance with industry standards

Cerner has made significant investments in demonstrating compliance with industry standards and regulatory requirements. Cerner contracts with an organization independent from security to perform an internal assessment of compliance with Cerner policies and procedures, laws, and regulations. Additionally, Cerner regularly undergoes external audits to validate the operating effectiveness of security controls across Cerner's platforms and operations ensuring compliance with relevant legislation (such as HIPAA, the EU GDPR and other applicable privacy or data protection legislation), regulations and standards applicable to the safeguarding of personal, medical, and other sensitive data.

International Standards Organization (ISO)
Cerner's information security management system is compliant with the principles of the ISO 27001, 27017 and 27018 standards. Its policies are applicable to all of Cerner's platforms.

Operational procedures used to deliver Cerner's services are certified against ISO 27001:2013, ISO 27017:2015 and 27018:2019. The certificate scope comprises the Information Security Management System (ISMS) supporting the globally managed security, software development, installation, upgrades, implementation, maintenance, remote hosting and support services for Cerner owned data centres and co-location data centres including public cloud. The ISMS is limited to the controls and supporting justifications described within the organization's Statement of Applicability, which further extends to the additional objectives detailed within ISO/IEC 27017:2015 and ISO/IEC 27018:2019.

Cerner has a dependency on co-location data centres in Canada, Sweden, United Kingdom, France and Australia and public cloud service providers for their physical and environmental security controls. Cerner has in-scope processes that extend to the management of Cerner system residing in the co-location data centres and public cloud.

The departmental scope for this ISMS is comprised of Consulting, Cerner India, Cerner Support Services, CernerWorks, International Consulting, Shared Services Engineering, Strategic Growth, and Technology.

Cerner operations for the United States, Canada, United Kingdom, Ireland, France, Germany, Sweden, India and Australia are included in the scope.

NHS Data Security and Protection Toolkit
In line with the regulatory requirements in the United Kingdom, Cerner maintains compliance with the requirements of the NHS Data Security and Protection Toolkit (DSP Toolkit). Cerner completes annual self-assessments through the DSP Toolkit as required

by NHS Digital to maintain compliance with the 10 National Data Guardian Standards. Confirmation of Cerner's self-assessments can be found on the NHS DSP Toolkit website under https://www.dsptoolkit.nhs.uk/OrganisationSearch/YGM05. Cerner's ODS code is YGM05.

Technical and Organizational Measures (TOMs)
In line with the requirements of the EU GDPR and other relevant data protection legislation, Cerner has developed global Technical and Organizational Measures to protect the processing of personal and sensitive information. The latest version of Cerner's global Technical and Organizational Measures is available upon request.

Access control:

Cerner

Users of the system will be controlled by the following:

- Cerner staff accounts incorporate two factor authentication and automatic time outs. Accounts also closed on staff member's last day of employment.
- Cerner & Optum support access to be kept to a minimum, reviewed regularly and monitored
- Use of strong passwords - not containing part of username, minimum 8 characters (upper/lower case, numerical & special characters) and not used previously

HIOW partner organisation staff:

The identity management solution for staff is in place.

- All users will complete a user registration form for the platform with assurance provided for identity and need for access by line manager
- The vast majority of users will access the platform using nhs.net single sign on process
- Request/approval process for a user account are managed by each partner organisation for their staff access, confirming organisation, role and need for access
- Processes are linked to partner starter, change, leaver processes

In addition the system features a robust audit trail recording the actions of all users, including login activity (successful and unsuccessful). The audit trail has a set of standard reports and a reporting tool that provides the ability to create custom audit reports.

Further guidance is incorporated into PHM Programme 'User Management' Standard Operating Procedure.

Vulnerability scanning & penetration testing:

Cerner conducts continuous production scanning of its platforms, and then scores vulnerabilities based upon the expected impact to the environment and external exposure. Once the vulnerability is scored, a process to mitigate or remediate the

vulnerability is initiated. Identified vulnerabilities are assessed for risk and mitigated or remediated according to their severity level. This analysis includes internal penetration scanning of environments using industry standard tools.

The CSIRC (Computer Security Incident Response Capability) team coordinates and utilises international and technological industry threat intelligence information including the Health Information Sharing and Analysis Centre (H-ISAC) and the British NHS Digital Care CERT Cyber Security Centre to ensure protection of Cerner hosted environments. In addition, the team leverages industry standard tools to systematically analyse logs to identify potential unauthorised activity and focus on potential threats.

Penetration testing

Annually, Cerner hires a reputable (CREST accredited) independent security company to perform an external penetration test on the Cerner environment to check for security weaknesses that would allow a malicious actor into the hosted environments. This test not only gives Cerner's security leadership insight to specific vulnerabilities, but also ensures the security controls and processes implemented are effective at blocking active threats.

In addition to the external penetration testing detailed above, Cerner has hired trained security professionals to perform penetration testing on an ongoing basis. These associates are part of the Enterprise Security organization and report directly to the CSO. These tests also allow real data for Cerner's security and other executives to determine if the controls implemented are operating effectively.

Penetration testing attestation

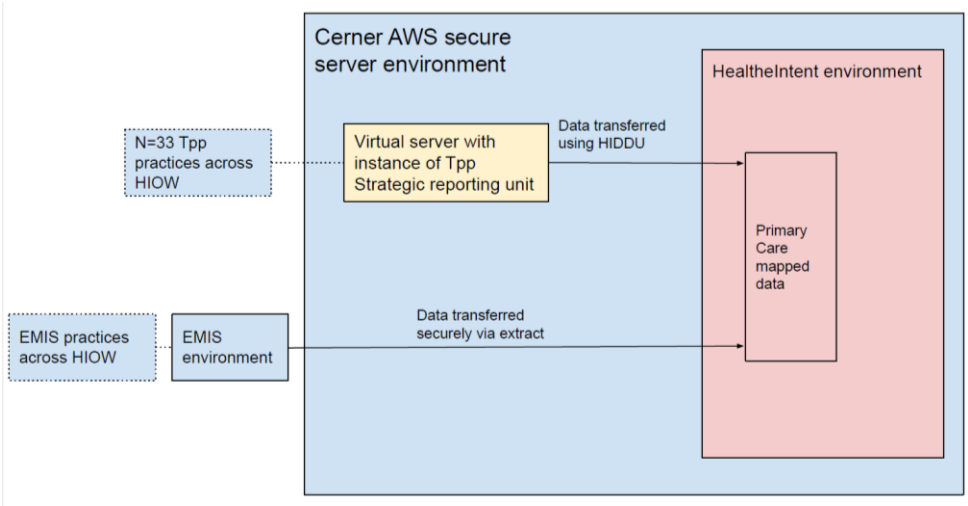
Cerner will provide a "Penetration Testing Attestation Letter," which shall describe the penetration testing that was performed and confirm that an industry standard methodology, testing tools and national vulnerability database were used. Cerner also can, upon request, confirm that identified vulnerabilities have been remediated or are being addressed in a remediation plan and are being actively monitored. Cerner requires a confidentiality agreement to be in place to receive this Attestation Letter.

Secure data transfer:

Cerner

Data sending systems are in control of their data stream via the HealtheIntent Data Upload Utility (HIDUU). The HIDUU is a lightweight, Java-based command-line tool that employs the OAuth industry-sandard security model to create a secure connection between the data sending system and Cerner's HealtheIntent Platform hosted within the EU West 2- London region in AWS, using TLS encrypted channels. The HIDUU provides client-side file validation and logging to ensure clean data files land within the HealtheIntent Data Ingestion Platform. HIDUU also allows data stewards to track their data streams using the HealtheIntent Data Ingestion Tool. This tool provides statistics around file transmission and size with future enhancements allowing more thorough tracing of data through the entire pipeline.

Data from general practices that utilise the TTP Systmone application is extracted in a slightly different way. A version of the TPP Systmone 'strategic reporting extract (SRE) ' tool is hosted in the Cerner data environment. This will be linked to the TPP systems of participating practices. A regular query will be run from the SRE to the systems to extract the agreed data. By being hosted in the Cerner data environment, the data will be transferred directly from the GP system to Cerner secure servers. In this regard Cerner will act as the data processor for the practices. Practices are listed as beneficiaries in the contract that the ICB holds with Cerner for the provision of the overall PHM Platform and specific instructions to Cerner will be set out by the ICB on behalf of the relevant practices. The practices will receive a copy of these before any extraction begins (see below)



NECS

NECS transfer NHS Digital SUS data to Oracle Cerner's SFTP site, which is accessed with a username and password. This data is encrypted in transfer.

Data Backup:

Cerner

Backups (full or incremental) will be conducted daily during off-peak business hours in the client's time zone at a separate site to the main site. This site is also UK based and subject to the same security controls as the main site. Backup jobs will be staggered throughout the window to ensure optimal performance and reliability.

Maintenance Window: a weekly window will be scheduled to perform maintenance on the backup system. Scheduled restores will not take place during this window; however emergency requests will be evaluated as requested.

Full backups will be conducted a minimum of once per week.
Incremental backups will be conducted daily with the exception of the day when a full

backup is conducted.
Snapshots for Images: Snapshots will be performed at a minimum of once per day. Snapshot jobs will be staggered throughout the day and have no impact on the client.

Backup jobs will be checked daily to ensure they completed successfully. Any backup job that has failed will be investigated, resolved; and the job will be rescheduled with the owner of the system.

Malicious code protection:

Cerner uses multiple overlapping security applications and countermeasures within its security program to protect the platforms. The following are some examples of the security technologies Cerner deploys to protect the platforms:

- **Anti-Virus Software** – Anti-Virus (AV) anti-malware software, or other compensating controls are used, as appropriate, throughout the hosted environment and pattern file updates are deployed daily. Inbound data is scanned in real-time and system drives are scanned on a weekly basis. In addition to keeping virus signatures up to date, the AV software and scan engines are updated to maintain and improve their effectiveness.
- **Network Firewalls** – Perimeter network and critical infrastructure connections are protected by industry standard network firewall technologies.
- **Intrusion Detection and Prevention Systems (IDS and IPS)** – Inline appliances are strategically placed within the network infrastructure to identify malicious or anomalistic behaviour. Each connection traversing interfaces of the firewall and each major connection traversing the core network is inspected to ensure validity. In AWS cloud environments Cerner is utilizing host-based Intrusion Detection Systems.
- **Denial of Service** – Cerner works closely with its internet service providers and AWS to detect and defend against denial of service access attacks.
- **System Hardening** – Server deployment templates/images are updated in line with industry standard practices to secure configurations.
- **Patch Management** – Cerner maintains an automated system inventory and patching tool providing visibility of system changes. Cerner obtains up-to-date patch notification through its partner relationships and tests patches using various processes prior to applying the patches within the applicable Platform(s).
- **Separation of Environments** – Cerner maintains appropriate logical and physical separation of its development, test and client production environments.

Is the processing novel in any way?

INFO: If yes, please provide details

No, population health management is a long-standing activity (albeit undertaken at smaller scale hitherto, relative to this programme). There are significant improvements in data analysis processes to Population Health Management in the HIOW ICS programme.

What is the current state of technology in this area?

INFO: i.e. is the technology 'tried and tested' in other areas, or in any way new/innovative?
The technology is tried and tested in other areas including the following health & care systems and communities: North Central London, Lewisham and West Suffolk.
Are there any current issues of public concern that should be considered?
INFO: If yes, please provide details
No specific issues currently identified

Step 3: Consultation process

Consider how to consult with relevant stakeholders (such as organisational partners and data subjects/representative bodies including HIOW Data Trustworthiness Forum)

Describe when and how the project will seek individuals' views – or justify why it's not appropriate to do so

The Population Health Management programme will not be seeking the views of all individuals for the data sharing process for three main justifications;

- there is a clear precedent that system-wide data sharing health records and population health management programmes have not sought views of all individuals
- there is no expectation from patients that individuals be approached for their views and;
- the resources and time required to engage with 1.8 million Hampshire and Isle of Wight residents makes the task untenable.

The PHM programme will align with ICS and local patient engagement methods for exploring views on data sharing and will build in patient communication as part of a wider ICS communication and engagement plan on data sharing, and health and care records.

Who else does the project need to involve, or has already been involved in the health & care community?

INFO: e.g. ICS Data Trustworthiness Forum, Local Medical Committee (other professional bodies)

Partners from across health and care were consulted in the development of the PHM program strategy leading to a broad source of views.

Key strategic partners from the ICS, Integrated Care Board, key health organisations, key local authorities and representative bodies from Hampshire and Isle of Wight have had a direct role in the development of the PHM programme from its inception. This has included decision making on the procurement of the Cerner HealtheIntent system.

The PHM programme is governed through the PHM Strategy Board whose membership includes health (commissioning, primary, acute, community and mental health), care (local authority, county councils), public health and local medical committee representation. The programme is further governed, and delivery assurance provided by the PHM Delivery and Assurance Board with representation from the above organisations in addition to wider health and care representation. Leadership and input from these individuals and organisations will ensure broad consultation in the ongoing programme.

Will the project involve any new data processors? If so what are the contractual arrangements with them (in place or being established)?

INFO: Processors are organisations who will process the personal data on behalf of the data controllers

The suppliers, Cerner and Optum, are data processors. Hampshire, & Isle of Wight ICB

holds the supply contract with Cerner (& Optum as a sub processor) and these identify all potential PHM Partner organisations as beneficiaries of the contractual arrangements.
Is there a requirement to consult information security experts, or any other experts?
INFO: Please provide details to support the answer
Not identified to date. Cerner environment is in use by a number of other health and care partnerships, so is not new to the health and care environment and is subject to rigorous security (see previous sections).

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures

What is the legislation that requires or permits the processing? (Legal gateway)

INFO: Public sector organisation(s) can process personal data to perform a statutory function. Please detail the relevant legislation here. Details to support this can be found in appendix 12 of the HIOW ICS DSA for direct care and in the matrices of the Secondary Use Data Governance Tool - https://data.england.nhs.uk/sudgt/

A number of component activities link up to form the processing for the system, firstly the extraction and loading of data, then the use of data along two main paths, namely individual care and purposes that support individual care. The legal gateways for these activities by organisation category are as follows:

Processing activity	**Organisation category**	**Legal Gateway(s)**
Extraction from organisational system and loading into PHM platform	NHS Provider & organisations contracted to provide NHS services (inc GPs)	Individual care (identifiable): Health & Social Care (Safety & Quality) Act 2015, linked to H&SC Act 2012 (s251b) – duty to share data to facilitate the care of an individual. *(NB objections considered under data subject rights)* Purposes supporting individual care (de-identified): (NHS Act 2006, s.72) - Duty on NHS bodies to co-operate with each other in exercising their functions
Use of data for individual care	NHS Provider & organisations contracted to provide NHS services (inc GPs)	Individual care (identifiable): Health & Social Care (Safety & Quality) Act 2015, linked to H&SC Act 2012 (s251b) – duty to share data to facilitate the care of an individual. *(NB objections considered under data subject rights)*
Use of de-identified data for purposes supporting individual care	Commissioning organisations (individually or collaboratively as ICS)	The full scope of applicable legislation is identified in the NHS England 'Secondary Use Data Governance Tool' activities matrix: Secondary use data governance tool (england.nhs.uk)

How will the processing actually achieve the purpose?

INFO: Please provide details to support the answer

The following is an extract from NHSE PHM website:
(NHS England » Population Health and the Population Health Management Programme)

As set out in the NHS Long Term Plan, local NHS organisations will increasingly focus on population health and local partnerships with local authority-funded services, through Integrated Care Systems.

Therefore PHM is the critical building block for integrated care systems and enables Primary Care Networks (PCNs) to deliver with their local partners true Personalised Care. Together, the three Ps (PHM, PCNs, Personalised Care) form a core offer for local people which ensures care is tailored to their personal needs and delivered as close to home as possible.

PHM enables systems and local teams to understand and look for the best solutions to people's needs – not just medically but also socially – including the wider determinants of people's health.

Many people need support with issues such as housing, employment, or social isolation – all of which can affect their physical and mental health – these solutions are often already available through, or better designed with, local people, the local council or a voluntary organisation.

Better partnership working using PHM to join up the right person with the right care solution helps us to improve outcomes, reduce duplication and use our resources more effectively.

Hampshire and Isle of Wight ICS are prioritising the development of a population health management approach as described in the Long-Term Plan (as summarised above) and outlined in ICS planning guidance. As part of the ICS' intelligence and analytics strategy the data will help by:

- Supporting our understanding and planning for our population's health
- Helping health and care staff to make better day-to-day decisions
- Tracking performance of NHS and social care services and understanding where and how they could be improved
- Supporting the development and rapid deployment of new medical products or clinical services that can benefit our population

To achieve the ICS aims to:

- Improve our population's health and wellbeing, the quality of care we deliver, and access to that care
- Do more to prevent ill health and be proactive about providing good quality

preventive care in people's homes and communities

Is there another way to achieve the same outcome?

INFO: Please details to support the answer

The processing of data for population health already takes place, albeit on a scale limited by current means and with limited data.

An alternative to using a platform such as HealtheIntent, would be to continue to conduct data gathering and extractions across partner agencies for specific activities on a one by one basis. In addition to the significant increase of time and resource utilisation to increase the scale to the HIOW partnership, this will only give limited benefits as any 'picture' achieved for each analysis will be, by default, narrow in scope. This will also result in large volumes of data being periodically extracted, sent between numerous partners, compiled into numerous different datasets and arguably significantly more data being transferred, shared, stored in multiple places.

Therefore as well as the 'big picture' benefit of this approach, the data feeds, storage and overall use will be significantly more secure and controlled than if data uses develop in a piecemeal and unstructured fashion to meet the multiple requirements of partners across the ICS.

How will the project prevent function creep?

INFO: Function creep is where data collected for one purpose is used for another purpose over time.

The Data Sharing Agreement sets out the agreed scope of use of the data. This is set around the initial contracted use cases. It is expected that uses will develop further over the lifetime of the programme, where necessary facilitating review of the Data Sharing Agreement.

The overall use of data within the platform will be directed and overseen by the PHM Programme Governance. For example it is noted in the PHM Strategic Board Terms of reference that:

[The Strategy Board is required to]:

Develop an understanding of the current and future needs of the system at practice, PCN, place and system that will supported by a PHM approach

Act as joint controllers of the data shared into the HealtheIntent platform with the Integrated Care Board taking a lead role

Assess proposed use cases for the shared data from organisations against the established purposes as defined in the data sharing agreement

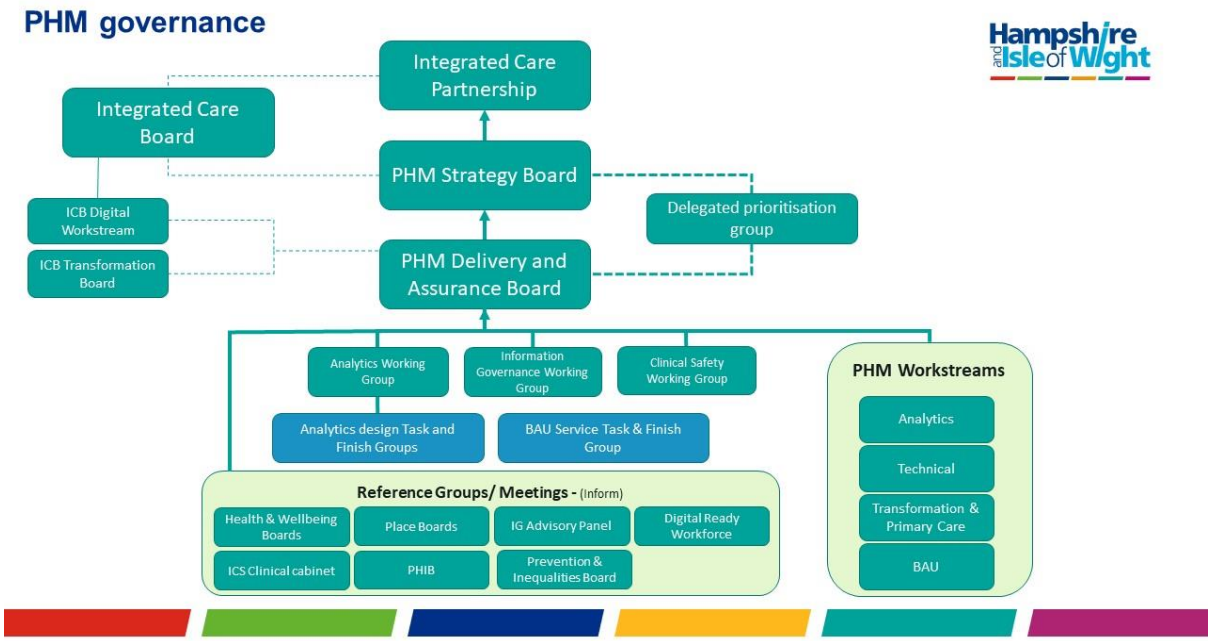
Assess against the defined purposes where use cases are novel, or where new data sources are available

The PHM Strategy Board and Delivery and Assurance Board is responsible for ensuring that use of data is clinical/care driven and aligned to the priorities of the health and care system

long term plan.

Furthermore, access controls on analysts who are able to create and modify reports/dashboards will be in place, limiting the scope of what they can create, linked to their role, employment and level of function.

The HIOW PHM Governance Structure:



Detail on operational IG management is set out in the data sharing agreement.

How will the project ensure data quality and data minimisation?

INFO: We should only use the minimum amount of personal data possible to achieve the purpose(s). Where the processing is for purposes other than direct care (see HIOW ICS DSA section 7), please detail how the identity factors will either be anonymized or pseudonymised. Note, data should only be pseudonymised if there is a need to link multiple data sources, prior to either full anonymisation or for re-identification only for direct care purposes to staff providing such care.

Data minimisation:

Initial data collection from each partner organisations will be a defined dataset for their current patient records (including those not actively receiving care). As each organisation is on boarded the specific details will be worked through and agreed.

Whilst these datasets will be large in the number of data items gathered and the number of patients that data is gathered on, the following are applied to ensure the data collected is adequate, relevant and limited to that which is required for the overall strategic purposes and aims:

- Population scope: Patients with a HIOW Postcode as either their Home or temporary address will be included (i.e. patients resident outside HIOW but treated by HIOW partners will not be included, except where the patient is registered with a HIOW General Practice)
- Patients with addresses of 'no fixed abode' will be included
- Records of patients who have died will be included, subject to NHS retention periods
- Patients marked as 'sensitive/S-Flagged' on the NHS Spine will not be accessible
- Patients whose whole primary care record is marked as 'confidential' will not be accessible
- Patients with an opt out code preventing sharing of their data for individual care will not be accessible.
- A list of 'sensitive' codes will be developed and maintained. Any record that has a sensitive code from the list on it will not have that code accessible.

Data minimisation will also be applied in the use of the platform as follows:

- Development of reports and dashboards will be conducted on the 'de-identified' data set during the development processes using the minimum data in terms of query and output.
- Reports and dashboards will be transferred to the identifiable dataset when they have been developed.
- Access control for end users will limit them to reports/dashboards created for their organisation (or where the organisation is in a group).
- Access control will also limit whether end users can see identifiable data, based on their organisation type and whether the individual has data related to that organisation, i.e. GPs would see patients of their practice, but would not see patients from other practices.

Data Quality:

When loading the data extracts, the platform will go through a number of stages to support the quality of the data:

- Structural mapping – this will map entities and data fields from the source systems to the HealtheIntent data models to ensure consistency where possible
- Code standardisation – mapping source codes from multiple systems to industry standard codes in PHM platform where required
- Concept normalisation – grouping of industry standard codes with the same clinical meaning to 'concepts' within HealtheIntent
- Person Matching – Auto linking on set of defined data items, with human review if required by Cerner/Client

Additional quality checks are performed by the Cerner Data Intelligence team following code standardisation. These include Unmapped Codes, Validated Mapping Analysis, Qualifier Analysis and Unexpected Data Analysis reports.

Any issues identified as source data quality issues will be highlighted to the relevant partners for addressing.

Analysts developing reports and dashboards will follow their standard processes for assessing and assuring the quality of data within the reports as they do now with existing

work.

How will individuals be informed about the processing of their data in this project/initiative?

INFO: Please detail either specific informing activities or how the programme will ensure any reliance on existing informing activities are sufficient.

Partner organisations should already make available 'fair processing' notices to their patients/clients. These should detail that data is shared with partner organisations to support the delivery of effective care to the individual (direct care) and that de-identified data is used and shared by the health and care system to improve overall services.

A key statement related to the PHM platform will be produced and shared with all partners to either include in their notices or to assess the sufficiency of their current notices.

Further related work to engage with the public will be part of the wider Wessex Care Record engagement programme.

How will the project help to support their data protection rights?

INFO: Data subject's rights include the right to access, correct, erase, object and restrict their data. Where a project has joint controllers, a specific arrangement will need to detail how data subject rights are upheld.

Access: The information held on the platform is a reduced version of existing information held by the individual organisations that hold patient information. No new or detailed information is created. In line with the Data Protection Act 2018, each organisation that has provided care and provided information to the Population Health Management platform would have to check the information before release and this would take significant time to co-ordinate. Therefore it is more appropriate and faster for individuals to contact each providing organisation for subject access requests.

Rectification: Correction requests will need to be actioned on data source(s) and feed through to the HealtheIntent platform during the next data extract and load. Any partner organisation who receives a request to rectify data where they are not the original source must ensure the request is directed to the source organisation. Should the error be found to have arisen within the processing undertaken to load and analyse data on the HealtheIntent platform, it is the responsibility of the lead controller (contract holder) to facilitate any necessary investigation and correction with Cerner.

Erasure: As data on the platform is processed on the basis of article 6 condition 'exercise of official authority' then the right to erasure does not apply.

Restriction: An individual with concerns over the use of their data will have the right to restrict the use of such data within the HealtheIntent platform, in particular with regard to objections or rectification requests. A process to manage such requests will be developed, so that any partner in receipt of a request is supported in providing a sufficient response.

Portability: The right to portability does not apply to the processing of data on the HealtheIntent platform as it is not processed on the basis of consent from, or a contract

with the individual.

Objection: An individual has the right to object to the use of data in the PHM platform. A process for managing objections and opt-out is in place.

Any patient who has a code on their GP record preventing their data from being shared for individual care (i.e. via the Care and Health Information Exchange – CHIE) or for any electronic record sharing will not have their data used for any reporting, dashboards or any other use within the PHM platform.

Patients whose GP record is coded with their 'dissent from secondary use of patient identifiable data' (a.k.a a 'type 1' opt out) will have their data processed for individual care and also where the use on the PHM platform is of de-identified data.
Further detail is available in the published HIOW Population health Management Subject Legal Rights Pack.

Automated decision making: No function exists within the HealtheIntent to make an automated decision about an individual so this right does not apply.

How will the project safeguard any international transfers of personal data?
INFO: If there are no international transfers involved, please state this
No transfers of data outside of the UK.

Step 5: Identify legal basis under GDPR/Data Protection Act 2018

Condition(s) for Processing
Personal Data – please indicate the basis for processing from the list below (NB condition on vital interests not included on the basis that any circumstance it would relate to would be covered by other conditions for public sector related work).
☐ The data subject has given consent ☐ The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ☐ The processing is necessary for compliance with a legal obligation to which the organisation(s) is subject ☒ The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the organisation(s) ☐ The processing is necessary for the purposes of the legitimate interests pursued by the organisation(s) or by a third party
Further Information, please detail why the above basis has been chosen
The above basis is the standard basis for public sector organisations when carrying out processing relating to their statutory functions for provision of individual care or exercising functions to support the overall health and care service in the area. The 'necessity' requirement is covered in section 4 'How will the processing achieve the purpose'
Special Categories of Personal Data. Where the initiative is processing special category data, one of the following basis must be applied:
☐ The data subject has given explicit consent ☐ The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law ☐ The processing is necessary for reasons of substantial public interest (on the basis of UK law identified in section 4 – legal gateway) ☒ The processing is necessary for the purposes of preventive 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 (on the basis of UK law identified in section 4 – legal gateway) ☐ The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high

standards of quality and safety of health care and of medicinal products or medicinal devices (on the basis of UK law identified in section 4 – legal gateway)

☐ The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (on the basis of UK law identified in section 4 – legal gateway)

☐ No special category data being processed

Further Information, please detail why the above basis has been chosen.

The main uses for the PHM platform are individual care or activities to support the provision of individual care.

Data Protection Act 2018 Schedule 1 Condition, please mark the relevant condition below (http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted)

☐ Employment, social security or social protection

☒ Health or social care purposes

☐ Public Health

☐ Research

☐ Substantial public interest, supported where required by appropriate policy document *(for example: shared policy on safeguarding vulnerable adults)*

Common law of confidentiality – describe how the processing of data will comply with the common law of confidentiality

Info: The generally recognised approaches to comply are: consent (can be implied or confirmed as a 'reasonable expectation'), or justification, this includes: overriding public interest (e.g. safeguarding individuals), specific legal duty, approval of national Confidentiality Advisory Group (via section 251 of Health & Social Care Act), or where the processing activities present either no risk of disclosing confidential information inappropriately, or where such risk has been reduced to 'rare/extremely low'.

HIOW partners, individually and when working jointly, are fulfilling their legal duties to deliver individual care under the Health and Social Care Act, and associated acts.

As and when the PHM programme determines that data is needed from, or to be shared with, sources other than in the health and social care partners, eg housing or environmental data, National Confidentiality Advisory Group (CAG) approval may be required; CAG approval may also be required where data is to be shared beyond the confidentiality of the usual care team.

The common law duty of confidentiality needs to be considered in the following ways to ensure compliance.

Data extraction & loading:
Identifiable data is extracted from agreed source systems and loaded into the Cerner PHM platform. Identifiable data is required as it will be used to support individual care use cases. For other purposes it will be de-identified by automated processes in the platform. The extraction and loading processes are automated processes that do not require system administrators to have sight of and manipulate the data.

For individual care use cases:
Access controls will be used to ensure that identifiable data, from the identifiable database (identified tenant) is only available to users:

- That work for an organisation that has a legitimate care relationship with the individual(s); or
- Have a documented and approved legal basis to access such data, e.g. an approval under section 251 (NHS Act 2006) from the national Confidentiality Advisory Group.

For purposes supporting individual care:
Data brought into the Cerner PHM Platform for the identifiable database will be processed through a 'de-identification' tool and held in a de-identified database (de-identified tenant).

The demographic data items are treated as follows:

Demographics	Transformation
EMPI Person ID	Pseudonymise
givenName	Remove
surname	Remove
Prefix	Remove
Medical Record Number	Remove
NHS Number	Remove
Date of Birth (DOB)	Month/Year
Gender	Retain
Ethnicity	Retain
Phone Number	Remove
Street	Remove
City	Remove
Postcode	Transform to LSOA
RecordId (source-specific identifier)	Retain

The data in this format is classed as 'pseudonymised'. It is still 'personal data' so Data

Protection legislation still applies, however pseudonymisation is a recognised approach to ensure confidentiality is maintained, whilst separate data sources remain linkable. It also permits re-identification in controlled circumstances where those ensure compliance with common law duty of confidentiality

Analysis activities e.g. build of analytical products such as dashboards will be developed on the de-identified database as a default.

All developed analysis products (i.e. dashboards, regular reports etc) will then run on the identified tenant, but access to identifiable data will be controlled by the following means:

- Queries developed to support analysis will select the minimum data (particularly in terms of identity factors) for the activity
- Outputs of analysis will be designed so that identifiable data is only included where necessary in relation to provision of direct care
- Role based access controls for the end user will determine whether they have a legitimate basis to access identifiable data based on role and organisation

The reasons for running all end user analysis products on the identified tenant, even where the analysis output does not include identifiable data is to maintain sufficient and effective access control are:

- Many reports will allow access down to identifiable data where the user's permissions are appropriate but will also be used at a non-identifiable level by end users who do not have permission to see identifiable data.
- Such reports need to run on the identifiable tenant to function, even if a large portion of the users of those reports do not need to see identifiable data (and will not be permitted to).
- The alternative of creating the report essentially twice (once for each tenant) and then managing user access to different tenants creates duplication of effort and also potential for mistakes to be made either granting too much access or too little.

Step 6: Identification of controllers & processors

Controller – organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. Identify & list below each organisation involved that will be classed as a controller, in addition noting any organisations that are joint controllers. Where organisations are joint controllers a 'joint controller arrangement' will be required (see appendix 10 of the HIOW ICS DSA).

All partner organisations submitting data to and using data from the HealtheIntent platform will be data controllers.

Controllers for individual care uses:

Provider organisations using the PHM Platform for 'intelligence supported' individual care will be able to access data on patients that they have a care relationship with and will be controllers of the use of the data for those purposes. This is in line with the statutory functions of provider organisations.

Where more than one provider is working together to provide the care of individuals, supported by outputs from the PHM Platform, such as information to support Multi-Disciplinary team activities, then the providers are **joint controllers** of the use of that data and must satisfy themselves that they have sufficient joint controller management arrangements for such activities. The PHM output is likely to be one part of the data they process to deliver such multi-party care services.

Controllers for purposes supporting direct care:

Typically, this data will be pseudonymised (pseudonymised data falls under GDPR). Integrated Care Boards and Local Authorities have numerous legal powers (see step 4) to use data to improve services, monitor quality, design new models of service delivery and in general promote and support the well-being of the population.

These powers extend to the residents of the geographical area that each organisation covers. The Data Sharing Agreement supporting the use of data on a whole system wide basis, sets out the basis on which partners **act as the joint controllers needed to permit processing of data across the whole HIOW population for such purposes, where a use requires it**.

For each identified controller, please confirm their current submission status to the Data Security & Protection toolkit. Please also list any other accreditations they have related to data protection & information security (such as ISO27001, Cyber Essentials)

As part of the process to bring an organisation into the partnership, their current DSPT status will be checked- Organisation Search (dsptoolkit.nhs.uk)

Partners will be asked as part of signing the Data Sharing Agreement to confirm they have achieved 'standards met' in the DSPT. Where a partner has not achieved 'standards met'

then they will be asked to detail the area(s) they are not compliant with and the HIOW IG Advisory Panel will advise the PHM Programme Governance whether the non-compliance presents any risk to the PHM Programme.

Processor – processes personal data on behalf of a controller (or joint controllers).
Identify & list below each organisation that is a data processor for the project/initiative. Confirm that a data processing agreement/contract, compliant with GDPR article 28, has been or is being established.

Info: In a situation where multiple controllers are sharing data and one supplier is a data processor, the contract with the supplier can be between one controller and the supplier, with the other controllers listed as 'beneficiaries' either directly or by clear organisation type under the Contracts (Rights of third parties) Act 1999.

It will also be useful to identify any external accreditations that a processor has with regard to information security and their compliance with the Data Security & Protection Toolkit.

Processor	**Purpose(s)**	**Contract Management entity**	**DSPT Status**
Cerner	Provision of HealtheIntent PHM Platform and associated SME, analytical, and technical support for the programme	Hampshire & Isle of Wight Integrated Care Board (all parties listed as potential beneficiaries)	21/22 standards met (23/06/2022) Cerner has achieved ISO 27001:2013, ISO 27017:2015 and ISO 27018:2019 accreditation
Optum (sub processor of Cerner)	Analytical support for wider PHM programme	Hampshire & Isle of Wight Integrated Care Board (Optum as sub-contractor)	21/22 standards exceeded (29/03/2022)
NECS (NHS England as host legal entity)	Provision of Secondary Use Services (SUS) data from NHS Digital	Hampshire&Isle of Wight Integrated Care Board	2122 standards exceeded(24/06/2022)

Hampshire& Isle of Wight ICB holds the contracts with Cerner, Optum & NECS which contains the core contractual requirements between the ICB as controller (with all other controllers listed as beneficiaries) and the supplier(s) as data processor. Any signatory to this agreement is, via agreement with the ICB able to enforce any contractual data processing aspect of that contract upon Cerner & Optum.

For each identified processor, please confirm their current submission status to the Data Security & Protection toolkit. Please also list any other accreditations they have related to data protection & information security (such as ISO27001, Cyber Essentials)

See above

Step 7: Identify and assess risks - DPO(s) to review and advise

Table 1 – Risk assessment **before** any mitigating controls are considered. See appendix A for examples of common risks and some suggested mitigating controls. Do not assume the appendix includes all possible risks, nor copy risks from the appendix unless confirmed that risk applies.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. Breach of confidentiality – unlawful access to record (by partner or supplier staff)	Possible	Significant	Medium
2. Breach of confidentiality – unlawful access by external party	Unlikely	Severe	Medium
3. Loss of data (temporary or permanent), due to technical / security failure	Unlikely	Moderate	Low
4. Incorrect alteration of data during on boarding process due to system process failure or technical security failure	Unlikely	Moderate	Low
5. Poor quality data impacting on quality of care delivery or service development	Possible	Significant	Medium
6. Unlawful processing or sharing of data	Possible	Significant	Medium
7. Excessive processing of data	Possible	Significant	Medium
8. Individuals are inadequately informed and compromised in exercising their rights	Possible	Moderate	Medium
9. Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	Unlikely	Significant	Medium

Identify additional measures that could be take to reduce or eliminate risks identified as medium or high risk in step 7			
Risk	**Options to reduce or eliminate risk (detail on many of these is included earlier in the DPIA)**	**Effect on risk**	**Residual risk**
1. Breach of confidentiality – unlawful access to record (by partner or supplier staff)	• Access controls to data, as defined earlier in the DPIA via PHM platform access control policy • Training for all staff, established in DSPT and specifics for the PHM programme • Employment contracts • Professional registration • Audit trail & disciplinary action – deterrent & define any useful proactive auditing	Reduced	Low
2. Breach of confidentiality – unlawful access by external party	• Physical access restrictions to data centre, network security features, penetration testing, vulnerability scans • System log on security	Reduced	Low
3. Loss of data (temporary or permanent), due to technical / security failure	• Supplier resilience arrangements, backups, & organisational fall back plans	Reduced	Low
4. Incorrect alteration of data during on boarding process due to system process failure or technical security failure	• Data extraction & upload process testing and checks • Training of support staff	Reduced	Low
5. Poor quality data impacting on quality of care delivery or service development	• Checks during design, collection and sharing of data • Visibility of data to wider number of users • Reporting of queries	Reduced	Low
6. Unlawful processing or sharing of data	• Governance processes including DPIA, Data Sharing Agreement and IG workstream, linked to Health & Care Reference Group, reviewing all developments and ensuring all uses of data are conducted lawfully	Reduced	Low

7. Excessive processing of data	• Data used in reporting and dashboard development to be subject to clinical review and are identified as necessary for the effective delivery of care across the health & care community • Role Based Access to reduce access to data in repository to data items identified as needed by user role	Reduced	Low
8. Individuals are inadequately informed and compromised in exercising their rights	• Qualifying standard requiring participating organisations to meet baseline 'informing' requirements. • Audits on compliance by partners • Common statements shared, common web resources	Reduced	Low
9. Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	• Processes for items such as SARS to be set out where required in joint controller agreements • Requirement on all organisations to have sufficient process as part of compliance with the Data Security & Protection toolkit.	Reduced	Low

ANY RISKS THAT REMAIN HIGH AFTER MITIGATION WILL REQUIRE CONSULTATION WITH THE INFORMATION COMMISSIONER'S OFFICE – to be facilitated by the lead DPO for the project
Comments from Data Protection Officer(s) for each identified controller organisation
Comments have been requested and provided during the consultation phase. All comments have been responded to either as amendments or points of clarity and discussed with DPOs across the partnership attending the weekly Information Governance Working Group.
Comments from the Records Management lead(s) (as required)
Not required
Comments from Cyber Security lead(s)
Not required (due to procurement due diligence)

Step 8: Sign off

The DPIA is presented to all partners of the programme and managed via the Information Governance Working Group. Partners should follow any internal organisational approval process they have. The PHM programme will not be requesting individual records of approval to the DPIA from each partner. Partners of the programme who are willing to participate will be required to

sign the Data Sharing Agreement. The DPIA supports the Data Sharing Agreement, so it is taken that signing the agreement to share the data they control, a partner is confirming that they are sufficiently assured by the DPIA to share the data they contribute.