NHS
Hampshire and Isle of Wight

Reference: **FOI 42549 HIOW D9Y0V**

Subject: **Population Health Management**

I can confirm that the ICB have now completed the search for the information requested, please see responses below:

QUESTION	RESPONSE
I note with interest your "Population Health Management" programme: (https://www.wessexcarerecords.org.uk/our-programmes/) where clearly identifiable, confidential, medical information is uploaded form contributing data controllers - such as GP surgeries - and likely linked to datasets from other sources (such as NHS Trusts), and then processed for secondary purposes : de-identification, anonymisation (which is processing), linkage, data analysis, planning, commissioning etc. *Your Population Health Management programme is not direct medical care. That is what your shared care record, CHIE, is for. It is data analysis, planning, commissioning, anonymisation, research etc.* *The National Data Guardian has recently written to all ICBs stressing the need for a legal basis to avoid a breach of confidence, misuse of private information, and so breach of GDPR, when confidential medical information is processed outside of the GP surgery (out with "the data controller's boundary") for purposes other than direct medical care: (https://www.whatdotheyknow.com/request/918862/response/2169509/attach/6/FOI.22.KAM245%20Appendix%20A.pdf)* *This follows previous communication from NHSX: (https://www.nhsdatasharing.info/NHSXLetter.pdf)* *A legal basis that avoids an actionable breach might be:* *• Explicit permission from the individual; or* *• A legal obligation placed upon the contributing data controller to process in this way; or* *• HRA/CAG approval under Reg 5 of COPI 2002 (so-called "s251 approval"), such as recently obtained by Nottingham and Nottinghamshire ICB (22/CAG/0101) for secondary uses of information within their shared care record, as obtained by West Yorkshire ICB (22/CAG/0102) for secondary uses of information uploaded form GP surgeries, and as has been applied for by the Greater Manchester Care Record (22/CAG/0169 and 22/CAG/0170).*	

<table>
<tr><td colspan="2">But "implied consent" is not a lawful basis that contributing data controllers - such as GP surgeries - can rely upon when instructing data processors (or sub-processors) to use such information for secondary purposes. Such secondary uses are, in the absence of Regulation 5 COPI 2002 approval, manifestly unlawful, and represents a breach of confidence, a misuse of private information, and a breach of GDPR.

So:</td></tr>
<tr><td>1. Please could you provide me with the legal basis for such processing that avoids a breach of confidence, misuse of private information, and so a breach of GDPR. Please note, I am not seeking the "GDPR" legal bases (Article 6 and 9), but how the common law of confidentiality is met.</td><td>Compliance with the common law duty of confidentiality statement:
The approach within the Hampshire and Isle of Wight (HIOW) Population Health Management (PHM) platform addresses compliance is set out as follows:
Cerner contractually act as the data processor for all parties involved in the PHM programme. A processor is essentially an extension of a controller and is processing data on behalf of the controller(s).
Automated processes within the Controllers systems extract the agreed data to be included into the PHM Platform. The data is transferred securely to the Cerner data environment.
Within the environment automated processes are run on the data to ensure the quality of data (normalisation & standardisation).
The data is then person matched so that data from multiple sources on the same person is correctly linked. This process is automated for all records with the exception of records with incomplete or incorrect demographic information. Where the automated process cannot match two or more records to an individual, there is then a human review. The human review is conducted initially by the processor and if further scrutiny or investigation is required, by the PHM technical team. In order to preserve the confidential health/care related data, this human review is conducted only on the core personal demographics, away from any of the special category health/care related data. So, the individuals conducting the review</td></tr>
</table>

Hampshire and Isle of Wight

	do not see confidential information. • Access by end user to data is controlled on the criteria of organisation and role. Only organisations and roles with a provision of (direct) care relationship are permitted to view identifiable data within any reporting tools. In summary compliance with the common law duty of confidentiality is considered and addressed at each stage of processing the data. The use of automated processing (where there is no disclosure or involvement of a person to whom disclosure could be considered a breach of confidentiality), the use of organisation and role based access controls are the key to mitigating any risk to confidentiality. This is also supplemented by auditing and if required, incident reporting procedures.
2. Please could you kindly send me the latest DPIA undertaken for this secondary uses purposes (processing)	Please see attachment *HIOW PHM DPIA v1.4*
3. Please could you state the data processor used in this scheme, if not clear from the DPIA	All processors are clearly described in the DPIA.
4. The SNOMED or Read Code that GP surgeries can apply to a patient record, that would prevent any such processing from taking place for that individual's confidential information	No consent for electronic record sharing – 414859005 Refused consent for upload to local shared electronic record - 416409005
5. Please could state whether the NHS Data Opt Out applies to such processing	Taken from the DPIA – The National Data Opt-out (NDO) for the NHS [is] 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 [is] implemented when NHS Digital Secondary Use Services (SUS) data is being used in analytics, in line with the requirements of the Data Access Request Service (DARS). The removal of data for NDO [is] 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. There are no use cases for application category 3 in the PHM programme.

The information provided in this response is accurate as of 25th January 2023 and has been authorised for release by Hampshire and Isle of Wight ICB.