The Private Healthcare Information Network
11 Cavendish Square
London W1G 0AN
020 7307 2862
www.phin.org.uk

PHIN's Legal Framework

Date: 06 August 2018

Background

The Private Healthcare Information Network (PHIN) is the independent, government-mandated source of information about private healthcare.

PHIN operates with a legal mandate to work with all hospitals and consultants providing private healthcare across the whole of the UK. That mandate comes from the Competition and Markets Authority (CMA) and imposes a legal duty on hospitals and consultants to submit data to PHIN as the new Information Organisation (IO) for private healthcare.

The CMA's Order[1] is issued under the Enterprise Act 2002[2] and specifies 11 performance measures (see paragraph 21 of the Order) for PHIN to publish, by procedure, at both hospital and consultant level. The Order also specifically requires providers of private healthcare to send PHIN patients' NHS numbers (or equivalent patient identification number) (see 21(2)(b) of the Order). These performance measures are also listed on PHIN's website at https://www.phin.org.uk/about/our-mandate

The Order places specific legal obligations on providers and consultants including:

- providers to provide the required information concerning performance quarterly from a date no later than 1 September 2016 (see paragraph 21.1);
- consultants to provide information concerning their fees no later than 31 December 2018 and thereafter from time to time on a regular basis (see paragraph 22.1 of the Order[3] (as amended);
- requiring both providers and consultants to ensure relevant information is provided to patients from the date the Order came into force (1 October 2014) (see paragraph 22.2).

Providers that do not submit complete and accurate information concerning performance to PHIN are failing to meet their legal obligations. The Secretary of State has also emphasised the importance of providing complete and accurate data to PHIN in his recent letter[4] to providers.

General Data Protection Regulation 2016/679

1) Data Controller Status

PHIN's processing of personal data (and each provider's disclosure of such data to PHIN) is necessary for compliance with a legal obligation as explained in further detail below. Where personal data are processed for purposes for which such data are required by law to be processed, the entity on whom the obligation to process the data is imposed will be a data controller for the purposes of that processing.

PHIN and the providers are each data controllers. Therefore, providers do not need to put in place arrangements to comply with Article 28 of the GDPR as this only applies to processors that are working on a data controller's behalf.

PHIN will continue to put in place a Subscription and Information Sharing Agreement to clarify responsibilities as a matter of good practice and which reflects the controller to controller arrangement.

2) Consent under the GDPR

PHIN has, to date, purported to rely on consent for the processing of patient data in connection with its obligations as the Information Organisation. However, in light of recently published GDPR guidance, PHIN no longer considers this approach appropriate – see below for further detail on (i) PHIN's lawful bases for processing patient data under its remit as the Information Organisation and (ii) the ICO's guidance on when to seek consent from data subjects.

PHIN's decision to change its position on seeking consent has been informed by the following guidance:

- The ICO's GDPR guidance cautions controllers against purporting to rely on consent where another lawful basis applies.
- The European Data Protection Board guidance on consent also specifically notes that "sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals."

This decision has been reinforced by the fact that PHIN's reliance on consent to date has adversely affected its ability to produce and publish the required performance measures.

PHIN received consent for only 47.3% of 187,362 eligible records. There was also significant variation on the proportion of consenting patients across different providers for that period, ranging from 11% to 100%. This resulted in 52.7% of records being excluded from the measures that PHIN is legally responsible for publishing and this approach has therefore been deemed to be ineffective.

On the basis set out above, providers must not be requesting consent from patients in respect of the disclosure to PHIN of patient data under the Order. Please note that PHIN does not intend to re-instate consent as it is not an appropriate approach (in terms of lawful bases) or an effective approach (in terms of collection of data).

PHIN has issued on its website[5] an updated privacy notice explaining PHIN's lawful bases for processing under the GDPR.

3) Private patient data

PHIN's lawful bases for processing private patient data (which are also appropriate in respect of a provider's disclosure of such data to PHIN) are as follows:

- **Article 6(1)(c) of the GDPR**: As PHIN has obligations under a CMA Order to publish performance measures, its lawful basis for the processing of personal data in its role as the Information Organisation is "necessary for compliance with a legal obligation". The same lawful basis will apply to providers who have obligations under the CMA Order to disclose patient data to the Information Organisation. The Information Commissioner's Office (ICO) recognises CMA Orders as a legitimate legal basis and an example of a CMA Order is used in the ICO guidance covering Article 6(1c).[6]
- **Article 9(2)(i) of the GDPR**: PHIN's lawful basis for processing special categories of data (i.e. health data) is that the processing is "necessary for reasons of public interest" in "ensuring high standards of quality and safety of health care".

4) NHS patient data

There is a clear benefit from publishing performance measures on both the private work and the NHS funded workload of providers and consultants. PHIN collects NHS activity data to enable it to consider all the treatment carried out by a particular consultant or provider with a view to forming a complete and fair picture of the nature and quality of their services. Whilst submission of NHS data is not expressly required by the Order, PHIN ask for this data to be included pursuant to Article 11.486(d) of the CMA's Final Report[7] which stated that the Information Organisation would be expected "to report performance measures for

the whole of consultants' practices, both NHS and private, since this is the relevant basis on which to judge performance.

PHIN's lawful bases for receiving (directly from providers and NHS Digital), and processing, NHS activity data are as follows:

- **Article 6(1)(f)** – the "processing is necessary for the purposes of legitimate interests pursued by the controller or third party";
- **Article 9 (2)(i)** – the "processing is necessary for reasons of public interest" in "ensuring high standards of quality and safety of health care".

Note to consultants on NHS patient data

PHIN will provide, prior to publication, secure access to the pseudonymised patient records underpinning the consultant level performance measures for consultant assurance and sign-off (subject to terms and conditions of use).

Consultants can choose to have their NHS activity excluded from their published measures but this will not affect the processing of their professional profile data (including personal details in a professional capacity) or the publishing of performance measures relating to private patient activity as this is required by the Order. For clarity, the use of the assurance and sign off process in respect of private activity data is a quality assurance mechanism.

The benefits that including NHS activity data will offer are substantial and wide ranging and will be of use to the general public, patients and consultants themselves. PHIN anticipates that the measures will be of significant benefit not only in terms of quality, safety and regulation but also to consultant's re-validation and appraisal processes.

5) Data linkage

Specific performance measures listed in the CMA Order include "unplanned patient transfers (from either the private healthcare facility or NHS Private Patient Unit (PPU) to an NHS facility)" and "re-admission rates". There is a clear benefit in also including NHS re-admissions in these figures. As such a need arises to link the data collected from providers to information held by the NHS.

The Department of Health, NHS Digital, NHS England, NHS Improvement and the Care Quality Commission all recognise the need for PHIN's linked performance measures to be created and are supporting its endeavours to bring this information into existence.

PHIN is currently consulting with NHS Digital on the appropriate lawful basis for conducting data linkage.

Therefore, although the Order expressly requires providers to submit NHS numbers (or their equivalent) to PHIN, providers should continue to refrain from sending NHS numbers (or their equivalent) to PHIN until notified otherwise. Whilst PHIN does have a legal basis to receive and process the NHS numbers (or equivalent), PHIN is not currently using this data (due to the currently unresolved issues around data linkage) and so has decided to exclude it until in a position to produce relevant and useful information. This is part of PHIN's data minimisation processes and it intends to collect this data again in the future.

For clarity, no private records submitted since 1 January 2016 have been linked to any NHS records and all NHS Numbers collected before 26th May 2018 will be destroyed on or before 31 December 2018. All hospitals should continue to collect NHS Numbers in line with their obligations under the Health and Social Care Act, and for future submission to PHIN.

PHIN will continue to make available privacy notices for patients, consultants and providers[6] on its website to discharge its fair processing obligations.

References:

[1] https://assets.publishing.service.gov.uk/media/542c1543e5274a1314000c56/Non-Divestment_Order_amended.pdf
[2] https://www.legislation.gov.uk/ukpga/2002/40/contents
[3] https://assets.publishing.service.gov.uk/media/58b5614fe5274a2a5f000089/private-healthcare-order-part-4-as-amended-2017-draft.pdf
[4] https://www.gov.uk/government/publications/patient-safety-letter-to-independent-healthcare-providers/patient-safety-and-acute-care-in-the-independent-sector
[5] https://www.phin.org.uk/footer/privacy-notice
[6] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/
[7] https://assets.publishing.service.gov.uk/media/533af065e5274a5660000023/Private_healthcare_main_report.pdf