ARTICLE EIGHT ADVOCACY

Submission to the Health Information and Quality Authority's Draft Recommendations on the Implementation of a National Electronic Patient Summary in Ireland

About Article Eight Advocacy

Article Eight Advocacy is an independent not for profit organisation which advocates for data subject rights in Ireland. We support data subjects by using all the tools available to us to ensure their fundamental right to protection of their personal data is respected.

We do this by providing easy to understand information on what data protection means for individuals on our datasubject.ie website, submitting complaints to the Data Protection Commission on behalf of individuals and managing the progress of these, initiating litigation where necessary, and carrying out research to uncover misuses of personal data.

Web: article8.ie | **Email:** info@article8.ie | 8/10 Coke Lane, Smithfield, Dublin 7, D07 EN2Y Ireland | **CRO:** #663077

INTRODUCTION

Article Eight Advocacy (A8A) is grateful to the Health Information and Quality Authority (HIQA) for this opportunity to provide submissions to this public consultation on the development of Draft Recommendations on the Implementation of a National Electronic Patient Summary in Ireland (hereafter the *Draft NEPS Recommendations Document*).[1]

In an editorial piece in the most recent issue of *International Data Privacy Law*, Dr Nóra Ni Loideain writes *"in contrast to the well-established legal systems governing data protection in Europe, many countries in Africa are in the preliminary stages of developing comprehensive data protection frameworks in the area of health research."*[2] Therefore it was a matter of some concern to Article Eight Advocacy that the General Data Protection Regulation (GDPR), and *particularly* the obligation on all data controllers to implement data protection by design and by default (Article 25 GDPR), appear to have been given scant consideration in the development of the draft recommendations.

According to the European Data Protection Board (EDPB) this requirement is for controllers to have data protection designed into and as a default setting in the processing of personal data. Controllers *"should think of data protection by design and default from the initial stages of planning a processing operation, even before the time of determination of the means of processing."*[3]

The Article 25 GDPR obligation applies throughout the lifecycle of any project from the conceptual and planning phases when the purposes and means of processing of personal data are being determined through to implementation, ongoing operation and decommissioning. Anticipating risks before they occur and taking steps to prevent harm to individuals is central to this obligation.

Consideration of data protection matters at the earliest stages of projects can:

- Reduce implementation and ongoing operation costs and timeframes since potential data protection problems can be mitigated against at the design phase.
- Improve transparency and the resulting trust on which data processing operations such as those involved in the delivery of an electronic patient summary rely.

However, in the case of the draft recommendations, it appears that a significant amount of work has been carried out without consideration of data protection issues upfront. All processing of personal data must comply with the data protection principles in the GDPR and

1 **HIQA**,'Draft Recommendations on the implementation of a National Electronic Patient Summary in Ireland', August 2020.
2 **Nóra Ni Loidean**, 'Regulating health research and respecting data protection: a global dialogue', International Data Privacy Law, Volume 10, Issue 2, May 2020, Pages 115–116
3 **EDPB**, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version for public consultation' , November 2019, page 26

data subjects have extensive rights which give them control over their personal data. Not baking in data protection principles from the initial phases increases the risk that data protection issues will arise in the future. Furthermore, according to the EDPB:

> **Early consideration of DpbDD is crucial for a successful implementation of the principles. From a cost-benefit perspective, it would be in controllers' interest to take this into account sooner rather than later, as it could be challenging and costly to make changes to plans that have already been made and processing operations that have already been designed.**[4]

Article Eight Advocacy is aware of recent media reports[5] in which HIQA states that data protection obligations, such as the preparation of a Data Protection Impact Assessment (DPIA), will be the responsibility of the Health Service Executive (HSE). The position of data controller in data protection law is not one which can be assigned to a particular body. Any entity which is responsible for determining the means and purposes of a processing operation may be a data controller. The *Draft NEPS Recommendations Document* contains suggestions for Key Performance Indicators (KPIs) and design decisions for the system and clearly sets out the purposes of the system.

The National Electronic Patient Summary represents a major shift in the nature of relationships within the healthcare system. Patients in Ireland currently regard their GP as the trusted custodian of their health information and the primary entry point for them to interact with the broader healthcare system. Introducing a new entity to which patients'personal data will be transferred is a significant change. A8A is not opposed to the development of a national electronic patient summary **if the benefits of this can be shown to be necessary, proportionate and provided the system incorporates the required extensive safeguards.**

It is finally worth noting that any legislation introduced to support the creation of the electronic patient summary must also meet the necessity and proportionality tests.

What follows is a brief assessment of some of the items outlined in the *Draft NEPS Recommendations Document* viewed through a data protection lens.

4 **EDPB**, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version for public consultation' , November 2019, page 10

5 **Irish Examiner**, 'Data protection cannot be an 'afterthought' in plans for electronic patient records, says watchdog' 5th September 2020

DATA PROTECTION PRINCIPLES

All personal data, whether special categories or otherwise, must be processed in accordance with the principles set out in Article 5 of the GDPR.

"lawfulness, fairness and transparency"

Article 5.1(a) sets out this principle.

Lawful basis

The default position in European data protection law is that personal data cannot be processed without a lawful basis. The envisaged lawful bases for the processing operations which will make up the implementation and ongoing operation of the electronic patient summary system are not mentioned in the *Draft NEPS Recommendations Document*.

Article 9 of the GDPR states that "processing of … data concerning health … shall be prohibited" unless one of ten conditions specified in 9.2 applies.

Article 9.2(c) is "processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent". This lawful basis is usually only applicable in short-term emergency situations and would not be suitable when the purpose of the data processing is to create a centralised and permanent store of health information.

Recital 46 further clarifies the limited application of vital interests as a lawful basis: "Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis."

Unless specific legislation is introduced to allow sharing of data from the sources discussed in Chapter 5 for the purpose of populating the electronic patient summary store, the only one of the conditions in Article 9.2 which would seem to apply to many of the processing operations envisaged in the *Draft NEPS Recommendations Document* is 9.2(a) "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes".

That consent is perhaps being envisaged as a lawful basis is further suggested by the discussion in Chapter 3 of the development of a "consent model".

> **HIQA is developing recommendations on a consent model for the collection, use and sharing of personal health information in Ireland. The recommendations development process will include a national public engagement survey that will be undertaken to provide knowledge and understanding in relation to public opinion on the use of health information, electronic health records and other eHealth initiatives. It is intended that this national survey will be completed during 2020 and published in early 2021. The**

> survey findings will also inform recommendations to the Minister for Health that will be published in 2021.
> *Draft NEPS Recommendations Document, page 26*

The European Data Protection Board has recently adopted updated guidelines on consent[6] which highlight a key element of the use of consent as a lawful basis – data subjects have the right to withdraw their consent at any time, and it must be as easy for them to withdraw consent as it was to give it. In many situations, consent is not the most appropriate lawful basis for a controller to use.

> *122.* It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. 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.
>
> *123.* In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.[7]

Mechanisms must be in place to allow this withdrawal of consent.

Since the intention is to populate the electronic patient summary from existing data stores within the health system it should be borne in mind that if consent is the lawful basis for this then multiple consents may be required for the creation of the electronic patient summary. The data controllers of these existing stores may also have to complete their own Data Protection Impact Assessments before any sharing of personal data can take place.

> A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.[8]

6 **EDPB**, 'Guidelines 05/2020 on consent under Regulation 2016/679', May 2020
7 **EDPB**, 'Guidelines 05/2020 on consent under Regulation 2016/679', May 2020, page 24
8 **EDPB**, 'Guidelines 05/2020 on consent under Regulation 2016/679', May 2020, page 12

In Chapter 5 of the *Draft NEPS Recommendations Document* the discussion of possible potential sources of information mentions:

> **The Terms of Agreement between the Department of Health, the HSE and the IMO regarding GP Contractual Reform and Service Development (2019) outline the planned introduction of the national electronic patient summary (called a 'summary care record') with a clinical dataset compliant with the National Standard. Under the Agreement, it is expected that a national shared care record will to expand the patient summary dataset, providing a longitudinal record of the treatment across healthcare settings—for example, for chronic conditions. The Agreement outlines the expectation that the patient summary will be populated from GP practice management systems.**
> ***Draft NEPS Recommendations Document, page 32***

An agreement entered into by data controllers is not necessarily a lawful basis for the processing of personal data. If any data sharing has already taken place under the terms of this agreement it may have been unlawful and could attract regulatory sanction and even legal action from any impacted data subjects.

The 2019 *Terms of Agreement*[9] document covers elements of consent in more detail than the Draft NEPS Recommendations Document so it is unclear which document takes precedence.

The preferred "Hybrid model" outlined on page 42 of the Terms of Agreement document describes different types of consents which could be provided by a patient but is silent on the lawful basis to be relied on for the processing operations required to create the summary care record.

Fairness

> **Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processes).**[10]

There is no discussion of fairness in the *Draft NEPS Recommendations Document*, nor of the rights and freedoms of data subjects which fair processing must guarantee. One of the key elements of a Data Protection Impact Assessment is an analysis of the risks to the rights and freedoms of data subjects[11]. This relates to all rights and freedoms set out in the Charter of

9 'Terms of Agreement between the Department of Health, the HSE and the IMO regarding GP Contractual Reform and Service Development'

10 **EDPB**, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version for public consultation' , November 2019, page 16

11 Recital 75, GDPR

Fundamental Rights of the European Union, not merely the data protection rights set out in the GDPR and national data protection legislation.

Transparency

Chapter 3 of the *Draft NEPS Recommendations Document* considers the successes of stakeholder engagement in other jurisdictions with no mention of the extensive transparency and information provision obligations placed upon data controllers by the GDPR, or indeed the purpose limitation principle which is dealt with in the following section.

> **Both programmes also worked to allay concerns that the Patient Summary was the surreptitious introduction of an electronic health record system—for example, in Northern Ireland, the commitment was also given that this data would be used only for direct healthcare, which built public trust.**
> ***Draft NEPS Recommendations Document, page 25***

This quote above seems at odds with other sections in the *Draft NEPS Recommendations Document* which identify the electronic patient summary as "an initial step in the longer term road map" (page 11, page 45). This longer term road map presumably includes implementation of a full electronic health record, the primary reason for the creation of the IHI.

The 'Terms of Agreement between the Department of Health, the HSE and the IMO regarding GP Contractual Reform and Service Development (2019)' document states that development "of the Summary Care and Shared Care Record will start in parallel as the lead time required to develop the more complex shared care record is longer than that required to develop the Summary Care Record." (page 41)

Therefore it is not clear whether the electronic summary record is being worked on as a standalone project or the first phase of a larger project.

"purpose limitation"

Article 5.1(b)

Personal data which has been collected for a particular purpose cannot be further processed for a different purpose. Thus it would seem that none of the existing information stores which are identified in Chapter 5 as potential sources from which to populate the electronic patient summary record contain data which has been collected for this entirely new purpose, and therefore a separate and new lawful basis for any sharing of personal data from one store to the electronic patient summary record store would be required.

Further processing and sharing of health data with commercial entities without the knowledge of data subjects has been a matter of serious and growing concern over recent years. Any

centralised store of healthcare data such as this will naturally attract the interest of third parties.

> US drugs giants, including Merck (referred to outside the US and Canada as MSD, Merck Sharp and Dohme), Bristol-Myers Squibb and Eli Lilly, have paid the Department of Health and Social Care, which holds data derived from GPs' surgeries, for licences costing up to £330,000 each in return for anonymised data to be used for research.[12]

Safeguards should be in place to prevent situations such as this arising. No potential safeguards in this area are discussed in the *Draft NEPS Recommendations Document*.

Potential international transfers of personal data are not mentioned in the *Draft NEPS Recommendations Document*. In July of this year, the Court of Justice of the European Union struck down the Privacy Shield EU-US data transfer arrangement. As things stand the UK looks set to shortly become a third-country for data protection purposes.

The effect of these developments should be considered at an early stage in the design of any system which may make use of joint controllers or processors which are not located in the European Economic Area.

"data minimisation"

Article 5.1(c) says that personal data processed must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". The tension between this principle and the apparent planned expansion of the electronic patient summary record into a shared care record and subsequently into a full electronic health record should be considered.

"accuracy"

Article 5.1(d). The *Draft NEPS Recommendations Document* identifies significant potential problems with accuracy in the data stores intended to be used to populate the electronic patient summary system. These must naturally be resolved in order to ensure the accuracy principle is met by the electronic patient summary system, and should indeed be resolved in all systems in which they currently occur as a matter of course.

"accountability"

Article 5.2 requires that controllers be able to demonstrate compliance with all the data protection principles set out in 5.1.

12 **The Guardian**, 'Patient data from GP surgeries sold to US companies', 7th December 2019

> Controllers must be able to demonstrate compliance with data protection provisions to data subjects, the general public and supervisory authorities at any time. [13]

Data Protection Impact Assessments as set out in Article 35 are important elements of this obligation.

A DPIA is a living iterative document as outlined in the European Data Protection Board's guidelines, which are worth quoting at length here:

> The DPIA should be carried out "prior to the processing" (Articles 35(1)and 35(10), recitals 90 and 93). This is consistent with data protection by design and by default principles (Article25 and recital 78). The DPIA should be seen as a tool for helping decision-making concerning the processing.
>
> The DPIA should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown. Updating the DPIA throughout the lifecycle project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.
>
> The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise.[14]

A DPIA should be carried out before this project continues any further.

13 **European Union Agency for Fundamental Rights**, 'Handbook on European data protection law', 2018 Edition, page 134

14 **EDPB**, 'Guidelines on Data Protection Impact Assessment (DPIA)', (WP248rev.01, October 2017), page 14

DATA SUBJECT RIGHTS

The *Draft NEPS Recommendations Document* makes no mention of how data subjects will be able to exercise their rights. At the most basic level, there is no clarity about who the data controller(s) for this system will be, and what entity data subjects will have to engage with in order to exercise their rights.

These rights are not new in the GDPR and any project involving such a volume of special categories of personal data should be cognisant of them from the very earliest stages and plan for mechanisms whereby individuals will be able to exercise these rights.

> **Data protection's supervisory model is quite unlike that for medical devices or financial services. Nobody expects a patient to check the reliability of a pacemaker before it is inserted into their heart or stress test a bank before they open a current account. And so the law does not provide patients and bank customers with tools that they would need to undertake such checks. Data protection is different: it expects that data subjects will do their own research and make their own decisions. The GDPR provides subjects with the tools to undertake those tasks. Subjects have the right to access their data, object to its processing, seek rectifications and corrections. These rights are not new. Similar rights were to be found in the GDPR's predecessors, the Strasbourg Convention and Directive 95/46. The difference is that the GDPR provides real supervisory and enforcement mechanisms to ensure that these rights can be successfully invoked.**[15]

The rights of data subjects are set out primarily in Articles 12-22 of the GDPR

Right of Access

The right of access is a pivotal data protection right and how individuals might go about exercising this right is not addressed in the *Draft NEPS Recommendations Document*.

If the right of access cannot be exercised "**easily"** (Recital 63, GDPR) then data subjects are frustrated before they can make any further inquiries about whether their data is being processed in manner compliant with data protection law.

15 **Denis Kelleher and Karen Murray**, EU Data Protection Law (London: Bloomsbury Professional, 2018), para. 9.01

> The GDPR does not set out any particular method for making a valid access or portability request, therefore a request may be made by an individual in writing or verbally.[16]

Consideration should be given to storage formats as data subjects are entitled to access a copy of all of their personal data and a failure to store this data in a format which is easily accessible can lead to significant overheads for the data controller when fulfilling these requests.

> Storage of health-related data in proprietary formats that have an effect of denying access by the data subject to the health-related data may constitute a restriction on the exercise of rights of data subjects.[17]

Other rights: Rectification, Erasure and Restriction etc.

How data subjects will be able to exercise these rights is not addressed at all. Since there is no concrete information about the lawful bases which will be used it is not possible to assess which of these rights will apply and in which contexts.

Right to Withdraw Consent

As mentioned above, if processing of personal data is based on the consent of the data subject then the data subject has a right to withdraw that consent at any time. Withdrawal of consent must be as easy to effect as it was to give consent. "The processing shall facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, any given consent is not valid"[18]

16 **Data Protection Commission**, 'Access and Portability'
17 **United Nations Special Rapporteur on the Right to Privacy, Task Force on Privacy and the Protection of Health Data**, 'Draft Recommendation on the Protection and Use of Health-related Data', Third Draft for Consultation, 2019, page 13
18 **EDPB**, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version for public consultation' , November 2019, page 15

CONCLUSION

These are just some of the issues we have identified in the *Draft NEPS Recommendations Document*. The document does not provide enough detail to allow for further analysis and feedback.

A failure to consider data protection principles, obligations and particularly data subject rights from an early stage may present problems and delays in implementation for any project of this scale, especially one which involves special categories of personal data and a significant shift in the nature of the relationship between patients, GPs and the data controller(s) of the NEPS system.

The risks and potential harms to data subjects are many and potentially severe and can best be mitigated against through careful planning to ensure all the data protection principles and mechanisms for data subjects to exercise their rights are baked in to the system from the outset.

References

Data Protection Commission, 'Access and Portability'

Data Protection Commission, 'Data protection by Design and by Default'

Data Protection Commission, 'List of Types of Data Processing Operations which require a Data Protection Impact Assessment'

Denis Kelleher and Karen Murray, EU Data Protection Law (London: Bloomsbury Professional, 2018)

European Data Protection Board, 'Guidelines on Transparency under Regulation 2016/679' (WP260 rev.01, 11 April 2018)

European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679', May 2020

European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – version for public consultation' , November 2019

European Data Protection Board, 'Guidelines on Data Protection Impact Assessment (DPIA)', (WP248rev.01, October 2017)

European Union Agency for Fundamental Rights, 'Handbook on European data protection law', 2018 Edition

HIQA,'Draft Recommendations on the implementation of a National Electronic Patient Summary in Ireland', August 2020.

Nóra Ni Loidean, 'Regulating health research and respecting data protection: a global dialogue', International Data Privacy Law, Volume 10, Issue 2, May 2020

United Nations Special Rapporteur on the Right to Privacy, Task Force on Privacy and the Protection of Health Data, 'Draft Recommendation on the Protection and Use of Health-related Data', Third Draft for Consultation, 2019