IMO Position Paper on the

General Scheme of the Health Information Bill

October 2023
Irish Medical Organisation
10 Fitzwilliam Place
Dublin 2
Tel (01) 676 72 73
E-Mail: imo@imo.ie
Website: www.imo.ie

Introduction

The IMO is the representative body for all doctors in Ireland and has for a number of years been calling for investment in electronic health records and IT infrastructure to support the delivery of safe, quality, integrated care. The IMO also recognises the value of health data for research and innovation, management of disease and health service planning. The IMO has also been calling for a legislative framework that provides clarity for the sharing of sensitive health information and ensures the core principles of doctor/patient confidentiality are respected.

The General Scheme of the Health Information Bill, published earlier this year, provides the legal framework for the sharing of electronic patient information both for care and treatment of patients and for other relevant purposes as well as the creation of a number of bodies to facilitate and govern the sharing of health information.

The framework is ambitious and if delivered correctly has the potential to bring considerable benefits to the delivery and planning of health care in Ireland, however the IMO is concerned that the costs will be substantial and there may be a number of unforeseen consequences that may not have been fully considered.

IMO concerns are as follows:

- Medical practitioners require accurate patient records to support the safe and effective delivery of care.
- The information to be contained in the Summary Care Record goes far beyond the requirements agreed in the 2019 GP Agreement between the Department of Health, the HSE and the IMO.
- General Practice is insufficiently resourced to gather and validate the information at the level that will be required under the Bill.
- As additional sources feed into the patient records, patient safety is paramount.
- Medical Officers of Health must not be impeded in their statutory function to protect public health.
- Substantial resources will be needed across General Practice, HSE and the National Health Information Authority to implement the framework and ensure confidential patient information is sufficiently protected.
- Concerted efforts and investment will be required to ensure confidence in the system and raise public awareness
- The Bill also ties in with the EU proposal on a European Health Data Space which has raised similar concerns with the Irish and European medical profession alike.

The IMO would like to make the following comments with regards to specific aspects of the draft Heads of Bill.

1 Information to be contained in the Summary Care Record.

Head 6 lays out the information to be contained in the Summary care record which includes:

a) Personal and demographic details**, -** PPSN will be used as the primary patient identifier and Eircodes for the address.
b) Health information including:
    - current health status, -health conditions, applicable diagnoses and relevant lifestyle information,
    - current prescribed medications,
    - recent procedures including hospital admission and discharge information
    - Allergies and intolerances and adverse reactions
    - Immunisations and vaccinations
    - Cause of death if deceased
    - Details of GP
c) Patient provided information - individuals may request that non-clinical information relating to his or her care is included in the Summary Care Record.

General Practitioners recognise the value of Electronic Patient Records and the vast majority have invested in GP practice management systems. Under the terms of the 2019 GP Agreement between the Department of Health, the HSE and the IMO (Hereafter 2019 GP Agreement),[1] GPs agreed to co-operate with a number of eHealth initiatives including the roll out of the Individual Health Identifier (IHI) and the development and deployment of Summary Care Records and Shared Care Records. However, the IMO is concerned that the information required under Head 6 varies significantly from the requirements laid out in Appendix D, 2019 GP Agreement. In addition the information required varies further from the information required in the Patient Summary Data outlined in Annex I,[2] of the legislative proposal on the European Health Data Space (EHDS). The configuration of GP practice systems to meet multiple requirements will create confusion and additional expense and thus a more consistent approach is required.

(a) Personal and demographic details - Use of the PPSN as the primary individual health identifier

As per the 2019 GP Agreement, the integration of the IHI with GP practice management systems is well underway and accredited General Practice systems are configured to store and display the IHI. Head 35 provides for the use of the PPSN (Personal Public Service Number) as the primary individual health identifier and appears to run contrary to the 2019 GP agreement and clarity on this matter is required.

In addition there may be individuals seeking care within the State (such as tourists or temporary visitors) who will not have a PPSN.

[1] Terms of Agreement between the Department of Health, the HSE and the IMO regarding GP Contractual Reform and Service Development
https://www.hse.ie/eng/about/who/gmscontracts/2019agreement/agreement-2019.pdf
[2] https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_2&format=PDF

(b) health information
Appendix D of the 2019 GP Agreement lays out the information to be contained in the Summary Care Records which is designed to be auto -populated from GP practice systems at a point in time.

Requirements under the Bill to provide additional Health Information such as "applicable diagnoses, tests, scans and X-ray results and health relevant lifestyle information" (Head 6 (b) (i)) and Hospital admission and discharge information (Head 6 (b) (iii)) go far beyond the health information requirements agreed in the 2019 Agreement and will place a significant additional burden on GPs to ensure that the information in the SCR is complete and up-to-date. This will require both additional resources and will take away from clinical duties. As per the 2019 GP Agreement, practice management systems must be able to auto-populate and update the data as required.

(c) non-clinical information provided by the patient
Head 6 (c) allows individuals to request that non-clinical information relating to his or her treatment and care be included in the SCR. As per the explanatory notes, this approach "is consistent with empowering the patient which is the goal of Sláintecare", however, relevant non-clinical information is likely to be subjective and no examples are provided. In addition, the Bill does not indicate who is responsible for inputting this information into the SCR, but seems likely to fall to the GP.

Both the draft Bill (Head 17A) and the EU proposal for a European Health Data Space will go further allowing patients, not only to add information to their record, but also potentially to restrict access to part or all of the information in their Electronic Health Records. In addition, it should be noted that the proposal for a European Health Data Space will also allow patients to upload information from certified well-being apps into their Electronic Health Record.

Quality of data in the clinical record is paramount to the provision of safe, effective care, and doctors have a duty to maintain concise and accurate medical records. The IMO is concerned about the potential impact that these measures may have on the quality of data in Electronic Health Records with the potential of clogging the system, making it difficult to find relevant information and rendering the records unsuitable as a clinical tool.

- Currently under General Data Protection Regulations (GDPR), patients are entitled to ask for their records to be rectified if inaccurate, however this does not extend to a dispute over a medical opinion.
- Patient provided data and data from well-being apps is not clinical data and cannot be relied upon unless it has been validated by a health care professional with the appropriate competence.
- Restricting access to part or all of the Electronic Health Record may pose significant difficulties for medical professionals who will be required to diagnose and treat patients based on incomplete information.

This, along with the potential for data breaches will likely to pose significant medico-legal issues for doctors. Given the highly litigious environment within which doctors practice, it is essential that this provision is appropriately thought through. It is unclear if any potential liability issues will be covered by the Clinical Indemnity Scheme (CIS) or by GP indemnifiers at an additional cost to the GP.

Recommendations:

- **1.1. Information to be contained in the Summary Care Record (SCR) must be the minimum required to support the provision of quality, safe, effective care and a consistent approach is required across contractual agreements as well as national and European legislation;**
- **1.2. Clarity is needed on the use of the PPSN as the primary identifier as this appears to run contrary to the 2019 GP agreement;**
- **1.3. In order to relieve the administrative burden on GPs, practice management systems must be able to auto-populate and update the data as required (as per the 2019 GP Agreement);**
- **1.4. Given the highly litigious environment in which doctors practice, the Dept of Health should consult with indemnifiers, including the CIS, on liability issues in relation to non-clinical information provided by individuals as well as the implications of any partial or total restrictions on access to Electronic Health Records**

2 Requirement to provide health information for the purpose of the Summary Care Record

Head 13 places a requirement on health service providers to provide the health information to the HSE for the purpose of the SCR and to notify as soon as practical any changes to the information provided. It is envisaged that this will primarily fall to the GP and then extended to other providers to input into the records.

As per the 2019 agreement, information to be contained in the Summary Care Records are to be auto-populated from GP practice management systems and are a snap shot at a point in time. While GPs will endeavour to ensure that their records are up to date, GPs cannot be held responsible for data that is incomplete, inaccurate or not fully up to date.

As additional information sources are identified and used to provide information to Shared Care Records and eventually Electronic Health Records, security and patient safety must be paramount. GPs cannot be held responsible for data breaches or the quality of data populated or communicated from other sources.

- HSE will require mechanisms must be put in place to identify and mitigate against potential risk of error or discrepancy in the data that can arise from the use of multiple information sources.

- Doctors can only be responsible for the data they have inputted in the SCR. Follow-up on investigations (e.g. blood tests) is the sole responsibility of the requesting doctor and cannot be delegated to another without agreement.

Recommendations:

2.1 The information contained in the SCR is designed to be auto-populated from practice management systems at a point in time and GPs cannot be held responsible for data that is incomplete, inaccurate or not fully up to date.

2.2 As information is obtained from multiple sources, patient safety must be paramount. GPs cannot be held responsible for the quality of data populated or communicated from other sources.

- **Mechanisms must be put in place by the HSE to identify and mitigate against potential risk of error or discrepancy in the data that can arise from the use of multiple information sources.**
- **Doctors can only be responsible for the data they have inputted in the SCR. Follow-up on investigations (e.g. blood tests) is the sole responsibility of the requesting doctor and cannot be delegated to another without agreement.**

3 Requirement to provide health information to the National Health Information Authority for relevant purposes

Part 5 of the Bill also provides for the establishment of a National Health Information Authority (hereafter the Authority) and Part 3 empowers the Authority to mandate the provision of information from any *relevant person* for any *relevant purpose* where there is a substantial public interest. The definition of a relevant person will include General Practice and the relevant purposes are wide ranging and are likely to result in multiple requests for data from GPs are insufficiently resourced to comply with such demand.

It should be noted managing data requires significant resources. As seen with the HIPE system - gathering and validating the information requires not only input from clinicians, but input from clinical coders, HIPE managers, medical records staff, IT personnel, administrative and management staff not to mention the HIPE team within the Health Pricing Office who ensure software development and support, training, data quality and audit, data management, analysis and dissemination. None of these resources are currently available within the General Practice setting.

The Regulatory Impact Analysis recognises that the biggest impact of the new Framework in the Draft Bill will be on those required to make information available to the Authority and suggests that the provisions in the Regulation on a European Health Data Space will propose similar mandatory requirements. However, the proposal for a European Health Data Space

recognises the significant burden that such requests for information will entail on small practices and excludes micro enterprises (fewer than 10 employees and annual turnover below €2 million) [3] from the requirement to make electronic data available for secondary use. However, this may be insufficient to cover larger practices and CPME have recommended that the exclusion should be extended to small enterprises (fewer than 50 employees and annual turnover below €10 million). The IMO recommend that this same exclusion apply to Part 3 of the Health Information Bill.

As the vast majority of data required for relevant purposes can be anonymised or pseudo anonymised and extrapolated from the Summary Care Records and Shared Care Records in aggregate form (See 2019 GP agreement), any requests for data should be made to the HSE. The HSE must be adequately resourced to validate the data and ensure all the necessary safeguards are in place.

Recommendation:

3.1 GP Practices should be excluded from the requirement to provide health information to the National Health Information Authority. The is in line with the Proposal for a European Health Data Space.

4 Access to Health Information in the Public Interest

Few people are familiar with the Statutory Function of the Medical Officer of Health who has the responsibility and authority to investigate and control notifiable infectious diseases and outbreaks, under the Health Acts 1947 and 1953; Infectious Disease Regulations 1981 and subsequent amendments to these regulations.

While the there is no specific mention of the Medical Officer of Health in the legislation, Head 6 Paragraph (3) (b) provides that subject to suitable transparency arrangements, SCRs may be accessed by the HSE to improve, promote and protect health and welfare of the public.

Heads 78A also mandates the provision of health information to the HSE or to a body established or contacted by the HSE where it is in the public interest and necessary to improve, promote and protect the health and welfare of the public. - Requests must be in writing, specifying the reason and legal basis for the request, the information required, the type and format of the information required, the timeline(s) and implications for non-compliance. The request may be on a once-off or recurring basis and the HSE will publish on its website a notice in relation to each request.

During an infectious disease investigation the Medical Officer of Health and/or their team will sometimes need urgent access to information, or to share it with the responsible person in a setting in order to protect individuals and the public. It is vital that any new arrangements

[3] Article 2 of the Annex to Commission Recommendation 2003/361/EC

under the draft legislation does not create barriers or cause delay to Medical Officers of Health when performing their statutory duties.

It is equally important that the EU Proposal for a EHDS does not override national legislation in the interest of public health .

Recommendations:

- **4.1 New arrangements under the draft legislation must not create barriers or cause delay to Medical Officers of Health when performing their statutory duties.**
- **4.2 Similarly, EU regulations must not override national legislation that allows access to patient records in the public interest.**

5 Financial Cost and Confidence in the System

Confidentiality is central to the trust between doctors and their patients and is a core element of the doctor-patient relationship. While both doctors and patients recognise that sharing information, in appropriate circumstances both for patient care and for the safety of the patient and others, doctors also have a duty to protect your patients' privacy by keeping records and other information about patients securely.[4]

In order to reap the benefits of electronic patient records and data both patients and doctors will need reassurance that confidential patient information is protected to the highest standard. This will require substantial investment across General Practice and the HSE as well as sufficient resources to enable the establishment and functioning of the National Health Information Authority.

Financial Cost and administrative burden on General Practice

As highlighted above, The requirements under the draft legislation are likely to impose a substantial additional burden on General Practice, none of which has been adequately costed. As highlighted above the Health Information required for the Summary Care Record goes far beyond that agreed in the 2019 GP agreement. In addition there is both significant overlap and inconsistencies between the framework laid out in the Bill as well as the European legislative proposal for a European Health Data Space. All of which is likely to incur significant duplication of costs.

According to the Regulatory Impact Analysis, *Credible and realistic analysis and estimates of costs are currently being profiled as the developmental process on the proposed new*

[4] Medical Council, 2019 Guide to Professional Conduct and Ethics for Registered Medical Professionals – 8th Edition

framework takes on a complete picture. This must include a full assessment of the cost to General Practice of compliance with the multiple requirements under the Bill to include:

- Capital costs including hardware and software costs in General Practice as well as ongoing system maintenance fees from IT suppliers should be ascertained.
- Costs related to maintaining and validating the data as well as additional costs associated with updating non-clinical information at the request of patients.
- Administrative costs and implicit cost of lost clinical time. Experience from other jurisdictions shows that the introduction of Electronic Health Records increases time spent on note-taking and documentation, taking away from clinical time. [5]

The IMO would recommend Summary Care Records should be piloted to ensure the system is fit for purpose in a busy clinical environment.

As mentioned before, General Practice will be subject to multiple requests for data for *relevant purposes* from both the National Health Information Authority and the HSE. While many GPs have invested in practice management systems, General Practice is insufficiently resourced to gather, validate and protect the information at the level that will be required under the Bill. GPs should be excluded from this requirement.

HSE Investment in IT systems, infrastructure and security

While the vast majority of GPs have recognised the value of eHealth invested significantly in practice management systems, elsewhere across HSE acute and community services there are significant deficits in the IT systems and infrastructure:

- While Electronic Healthcare Records have been piloted in some hospitals, the majority of hospitals in Ireland are still using paper-based patient records and referral systems.
- Accessing any EHRs, laboratory or radiology systems in community services outside of the hospital system, such as psychiatry, is very poor.
- Some IT systems have developed on an ad-hoc basis and there are on-going issues of interoperability.
- In Public Health there are longstanding and critical IT infrastructure gaps, including the lack of a case and outbreak management system, an integrated surveillance system, an immunisation reporting system.

Significant investment is required in IT Systems, infrastructure across HSE acute and community services so that health care professionals can access electronic patient records.

HSE Resources to establish and maintain the National Register of Summary Care Records

Substantial resources will also be required by the HSE in order to establish and maintain the National Register of Summary Care Records (Head 8). As highlighted above the HSE will require additional resources to guard against errors and discrepancies in clinical records and

[5] "The impact of electronic health record systems on clinical documentation times: A systematic review": https://www.sciencedirect.com/science/article/pii/S0168851018301635

to ensure that data is valid and up-to date. GPs are not sufficiently resourced to do so. HSE Data controllers will also be responsible for the highest level security of patient data as it is populated from different sources with sufficient resources and mechanisms put in place to mitigate against data breaches that may arise from both the use of multiple sources of data as well as multiple users. Lessons must be learnt from the ransomware cyber-attack on the HSE by Russian hackers in May 2021 , when around 100,000 patients had their data stolen while the and the closure of IT systems for four months led to major disruption of patient services.[6] In total the financial cost to the HSE is reported at €87.9 million in the response and recovery, while upgrading of systems and cyber security improvements are estimated at almost €657 million over seven years. [7]

Resourcing the National Health Information Authority

Additional resources will also be required to support the establishment and wide-ranging functions of the National Health Information Authority. In addition to its primary functions, Chapter 7 also provides the Authority with powers to carry out additional activities in relation to their role including the power to investigate or cause investigations to be carried out in relation to the provisions of the Act while Part 10 allows for Summary proceedings for offences under the Act to be brought and prosecuted by the Authority. The offences include: Head 15 - offences relating to identity theft; Head 16 unauthorized access and Head 28 - unauthorized disclosure that could lead to the re-identification. Head 22A- Prohibits processing of information in that facilitates prejudicial or discriminatory decisions, marketing or advertising to individuals and health care professionals, provides access to health information of an individual or facilitates the development of harmful products or services and Head 82 – provides for the offence of buying or selling of personal health information.

The IMO welcomes the inclusion of the above offences in the Bill, however the National Health Information Authority will require sufficient resources in order to investigate and bring proceedings against individuals and entities for alleged offences under the legislation. Given the potential cross-border nature of such offences, co-operation both within and outside of the EU will also be required.

Raising Public Awareness

The results of the National Public Engagement on Health Information 2020-2021[8] show that

- 97% believe that it is important that a hospital doctor treating an individual should have access to accurate information about their medical history and medications and 99% of people think a hospital doctor should be able to access their health information electronically, without their permission, when they are unconscious.

[6] Brennan M, Cost of HSE cyberattack to hit 'an eye-watering' €144 million, Sunday Business Post - 15 May 2023
[7] Office of the Comptroller and Auditor General 2022, 12 Financial Impact of Cyber Security Attack, https://www.audit.gov.ie/en/find-report/publications/2022/12-financial-impact-of-cyber-security-attack.pdf
[8] https://www.hiqa.ie/sites/default/files/2021-09/Findings-from-the-National-Public-Engagement-on-Health-Information.pdf

- 90% trust their GP to keep their health information safe and secure while 74% trust the hospital and 77% trust community healthcare services to do so
- 91% trust that GPs will only share relevant information with the hospital.
- Equally the vast majority (94%) think that it is important for health information to be used for the purpose of improving the quality of care (94%) for plan healthcare services. (93%) And for research (94%)
- 61% of people trust that their health information will be kept safe and secure if research is undertaken by a public organisation, whereas only 45% trust that their health information will be kept safe and secure if the research is undertaken by a private organisation.

Real engagement will be needed with the public and individuals so that they are aware of what their data has been used for and how the sharing of data contributes to improving the treatment and care that they receive. A comprehensive public awareness campaign will be required to ensure that individuals are aware of the positive implications of sharing electronic patient records and health data to promote improvements to patient safety and care as well as providing reassurances that their personal health data is secure.

In addition it is estimated that up to 10% of the population may not be registered with a GP and the public awareness campaign should also encourage these individuals to register with a GP.

National Health Information Guardian

Part 7 -provides for the establishment of a National Health Information Guardian, whose role is to promote best practice and to champion rights of individuals in relation to the handling of health information as well as building confidence in the health information system. A rights based approach must be carefully balanced with the need for accurate patient records to support the delivery of safe, effective patient care and it is important that the National Health Information Guardian engages with the medical profession to ensure that health care records are fit for purpose.

Recommendations

5.1 The framework should be subject to a full economic impact assessment to include:

- **an assessment of the cost to General Practice of compliance with the multiple requirements in the draft Bill to include**
  - **Capital costs including hardware and software costs in General Practice as well as ongoing system maintenance fees from IT suppliers should be ascertained.**
  - **Costs related to maintaining and validating the data as well as additional costs associated with updating non-clinical information at the request of patients.**
  - **Administrative costs and implicit cost of lost clinical time.**
  - **Piloting of Summary Care Records to ensure the system is fit for purpose in a busy clinical environment.**
- **A full assessment of the IT Systems and infrastructure requirements across all HSE acute and community services.**
- **Appropriate resourcing of the HSE in order to establish and maintain the National Register of Summary Care Records including:**
  - **Sufficient resources to guard against errors and discrepancies in clinical records and to ensure that data is valid and up-to date;**
  - **resources and mechanisms to mitigate against data breaches that may arise from both multiple sources of data as well as multiple users.**
- **Additional resources to support the establishment and functions of the National Health Information Authority including:**
  - **resources in order to investigate and bring proceedings against individuals and entities for alleged offences under the legislation.**
  - **given the potential cross-border nature of such offences, co-operation both within and outside of the EU will also be required.**

5.2 A comprehensive public awareness campaign will be required to:

- **ensure that individuals are aware of the positive implications of sharing electronic patient records and health data to promote improvements to patient care as well as providing reassurances that their personal health data is secure;**
- **encourage all individuals to register with a GP.**

5.3 The National Health Information Guardian must ensure that a rights based-approach is carefully balanced with the need for accurate patient records to support the delivery of safe, effective patient care.

6 Engagement on the EU legislative proposal on a European Health Data Space

The Bill also ties in with EU legislative proposal for a European Health Data Space, which has raised concern among the European Medical Profession. The CPME (Standing Committee of European Doctors) Position paper on the European Health Data Space reflects many of the concerns raised by the IMO.

Recommendation

6.1 In relation to the EU Legislative Proposal for a European Health Data Space, the IMO wishes to draw attention to the issues raised and the recommendations in the CPME Position paper on the European Health Data Space.

Summary of Recommendations:

1. Information to be contained in the Summary Care Record (SCR).

1.1. Information to be contained in the Summary Care Record (SCR) must be the minimum required to support the provision of quality, safe, effective care and a consistent approach is required across contractual agreements as well as national and European legislation;

1.2. Clarity is needed on the use of the PPSN as the primary identifier as this appears to run contrary to the 2019 GP agreement;

1.3. In order to relieve the administrative burden on GPs, practice management systems must be able to auto-populate and update the data as required (as per the 2019 GP Agreement);

1.4. Given the highly litigious environment in which doctors practice, the Dept of Health should consult with indemnifiers, including the CIS, on liability issues in relation to non-clinical information provided by individuals as well as the implications of any partial or total restrictions on access to Electronic Health Records

2. Requirement to provide health information for the purpose of the SCR

2.1 The information contained in the SCR is designed to be auto-populated from practice management systems at a point in time and GPs cannot be held responsible for data that is incomplete, inaccurate or not fully up to date.

a. As information is obtained from multiple sources, patient safety must be paramount. GPs cannot be held responsible for the quality of data populated or communicated from other sources.

- **Mechanisms must be put in place by the HSE to identify and mitigate against potential risk of error or discrepancy in the data that can arise from the use of multiple information sources.**
- **Doctors can only be responsible for the data they have inputted in the SCR. Follow-up on investigations (e.g. blood tests) is the sole responsibility of the requesting doctor and cannot be delegated to another without agreement.**

3. Requirement to provide health information to the National Health Information Authority for relevant purposes

3.1 GP Practices should be excluded from the requirement to provide health information to the National Health Information Authority. The is in line with the Proposal for a European Health Data Space.

4. Access to Health Information in the Public Interest

4.1 New arrangements under the draft legislation must not create barriers or cause delay to Medical Officers of Health when performing their statutory duties.

4.2 Similarly, EU regulations must not override national legislation that allows access to patient records in the public interest.

5. Financial Cost and Confidence in the System

5.1 The framework should be subject to a full economic impact assessment to include:

- **an assessment of the cost to General Practice of compliance with the multiple requirements in the draft Bill to include**
  - **Capital costs including hardware and software costs in General Practice as well as ongoing system maintenance fees from IT suppliers should be ascertained.**
  - **Costs related to maintaining and validating the data as well as additional costs associated with updating non-clinical information at the request of patients.**
  - **Administrative costs and implicit cost of lost clinical time.**
  - **Piloting of Summary Care Records to ensure the system is fit for purpose in a busy clinical environment.**
- **A full assessment of the IT Systems and infrastructure requirements across all HSE acute and community services.**
- **Appropriate resourcing of the HSE in order to establish and maintain the National Register of Summary Care Records including:**
  - **Sufficient resources to guard against errors and discrepancies in clinical records and to ensure that data is valid and up-to date;**
  - **resources and mechanisms to mitigate against data breaches that may arise from both multiple sources of data as well as multiple users.**
- **Additional resources to support the establishment and functions of the National Health Information Authority including:**
  - **resources in order to investigate and bring proceedings against individuals and entities for alleged offences under the legislation.**
  - **given the potential cross-border nature of such offences, co-operation both within and outside of the EU will also be required.**

5.2 A comprehensive public awareness campaign will be required to:

- **ensure that individuals are aware of the positive implications of sharing electronic patient records and health data to promote improvements to patient care as well as providing reassurances that their personal health data is secure;**
- **encourage all individuals to register with a GP.**

5.3 The National Health Information Guardian must ensure that a rights based-approach is carefully balanced with the need for accurate patient records to support the delivery of safe, effective patient care.

6. Engagement on the EU legislative proposal on a European Health Data Space

In relation to the EU Legislative Proposal for a European Health Data Space, the IMO wishes to draw attention to the issues raised and the recommendations in the CPME Position paper on the European Health Data Space.