Comments on the EC Working Document (WP 131 – 00323/07/EN) on the processing of personal data relating to health in electronic health records (EHR) produced by the Article 29 Data Protection Working Party

The Department of Health and Children (Dublin) welcomes the development by the Article 29 Working Party of the Working Document. It provides a good analysis of the data protection issues that need to be examined in relation to developing and maintaining an electronic health record (EHR).

By way of background information on the position in Ireland with regard to an EHR, the policy document underpinning health information development, the National Health Information Strategy, endorsed the phased introduction of such record, subject to there being in place a statutory information governance framework in relation to the sharing, etc. of health information and to the availability of a unique health identifier. Work has just commenced in relation to the drafting of proposals for legislation that will facilitate full and proper use of information while, at the same time, respecting and protecting the privacy of the individual. The Working Document will assist in informing the development of these proposals. Additionally, work in relation to developing a public sector wide approach to unique identification for the purpose of accessing public services, including health services, has also commenced. Both are at early stages of development.

Having consulted with various interests, the following represent issues raised that require further consideration/clarification:

1 Specific Comments on the content of the Working Document

1.1 Page 4, Section I: Introduction

The definition of an EHR used in the document does not match the ISO definition of EHR. The ISO/TR 20514 is the definition which is used by Eurorec in its methodology for quality labelling and certification of EHR systems in Europe.

The Working Document definition is as follows:
"A comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical treatment and other closely related purposes."

and the ISO definition states:
"The Integrated Care EHR is defined as a repository of information regarding the health of a subject of care in computer processable form, stored and transmitted securely, and accessible by multiple authorised users. It has a commonly agreed logical information model which is independent of EHR systems. Its primary purpose is the support of continuing, efficient and quality integrated health care and it contains information which is retrospective, concurrent and prospective."

The ISO definition is much more complete but the Working Document does supply additional text underneath its definition and it becomes clear that the Working Document makes three of the same assumptions as ISO:

- patient-centred (an EHR relates to a patient, not to an episode of care at an institution)
- longitudinal (long-term record of care, possibly from birth to death)
- comprehensive (it includes a record of care events from all types of carers and provider institutions tending to a patient)

The point on which they differ is that the Working Document does not elude to prospective data where ISO says:

- prospective (not only are previous events recorded but also decisional and prospective information such as plans, goals, orders and evaluations)

It is not clear as to why no reference is made to the prospective use of an EHR.

1.2 Page 5, Section I: Introduction

The Working Document says:

"EHR is claimed to be an appropriate means to:
bring about better quality of treatment because of better information about the patient;
improve the cost efficiency of medical treatments and thus prevent further rapid growth of health care budget deficits;
furnish the necessary data for quality control, statistics and planning in the public health care sector which should also have a positive effect on public health care budgets."

In light of the purpose of the document, this list could be added to by saying that an EHRis a fundamental component in the delivery of the optimum healthcare, as it:
supports education and research,
supports consumer access and eHealth.

1.3 Page 6 - General Principles - data quality principle

The document states in the second bullet point
"......Thus any irrelevant data must not be collected and if it has been collected it must be discarded."

Further elaboration on this point may be needed as it does not seem clear who has responsibility for deciding what data is deemed relevant. It is assumed that it may depend on the organisational structure that the EHR will follow as discussed in Section III, part 5 – Organisational Structure of an EHR system.

1.4 Pages 8 and 9 – Article 8 (2) (a) - Explicit Consent

- If a person enrolling with a primary care team, for example, refuses to give consent to information sharing, could that individual be refused enrolment in the team?

- In relation to the statement, "Consent must be specific", is it the case that this implies that consent (probably verbal) would be required for each specific disclosure, in particular to third party practitioners such as for specialist consultations/second opinions? This point is further discussed in relation to – Article 8 (3) on page 10: "processing of (medical) data by health professionals", however, further clarification of this point is needed.

- Should it be permissible for a patient to restrict the use of their data post-anonymisation. For example, if a patient has ethical objections to a particular field of research, is it permissible to prohibit the use of their data for that purpose? Is it permissible in the first place to prohibit anonymisation of certain of their data?

1.5 Page 9 - Article 8 (2)(c) "vital interests of the data subject"

Emergency Care
It is not clear from the document how emergency care situations will be handled – does the guidance need to further consider how access to the EHR will be allowed in these circumstances without permitting more access than is necessary for this care?

1.6 Pages 13 and 14 – Section III, Part 1 – Respecting Self Determination

- The comments of the Working Group on self-determination[1] are helpful but it would be very useful if the Working Group could be more definitive in stating whether it was consistent with the Directive (particularly given the references to Article 8 of the European Convention on Human Rights) to oblige an individual to join an EHR and/or to prohibit an individual from opting-out[2] and would the view on this point be affected if the individual was paying for his or her own healthcare.

- Understandably, there is much discussion in the document on opt-ing in/out from the patient's perspective but what is the position in relation to clinicians,

1.7 Page 17 - Section III, Part 5 - Organisational structure of an EHR system

The analysis of the organisational structure of an EHR system may suggest that hybrid structures are required to take account of the strengths and weaknesses of each model. As indicated, system modularity and the recognition of categories of data or sensitivity will permit the adaptation of flexible solutions.

1.9 Page 19 - Section III, Part 8 – Data Security

User-friendly PETS

[1] Pages 13 and 14

[2] It is noted in this regard that the WP predicated its Articles 8(4) comments "on the assumption that nobody would be forced by law to join an EHR, there must also be provision for withdrawing from the system."

The development of PETs is critical to improved data protection. The document focuses on the user friendliness of these technologies is welcome. The success of PET features is greatly dependent on the burden it places on the user, particularly at the individual and team level. PETs which enhance the user experience are more likely to gain the acceptance needed. It may be possible to develop embedded PETs as core system structures to support the efficient delivery of functions as in the past the master patient index enabled efficiency and consistency in equal measure.

2 General Comments

2.1 Records of the Deceased.

Personal information under the data protection directives covers living persons only. The duty of confidentiality enshrined in the Hippocratic oath does not dissolve on the death of the patient. It is important that EHR systems be extremely sensitive and accurate in relation to the deaths of subjects.

- There is a need for debate on the implications of the death of the person for the use of their data within the health system and for access to it by others including their family.
- The disclosure of data relating to a deceased person will have privacy implications for their relatives and others. At the same time, the need for access to this data may come from these same relatives or others.
- As suggested by the Working Document in Section III, Part 6, structures to manage security and access issues may generate categories of sensitivity. These could be relevant to permissible use of data of the deceased.

One possibility is that EHR technologies give more prominence to an ongoing understanding of the patient's wishes with regard to actions permissible in the event of incapacity and in the event of death.

2.2 Time locks and combinations

Relevance and timeliness are key concepts in the development of EHR systems. These will have application in the development of appropriate security features. A key hazard arises from the extent of instant access to sensitive data which is possible. This is not unlike the problem of free water on a car ferry deck which is designed without bulkheads. Useful approaches to this problem could include –

- Time locks on access to specific data with notification of key parties of access intended, with escalation procedures to request a relaxation of the time barrier.
- Multi-lock mechanisms where a number of parties must clear the specific access and providing for patient participation in this.

2.3 EHR systems in Member States

More information on the development of EHR systems in individual Member States and how they are addressing the issues in Article 8 (2) to (4) would be informative as, for example, the reference to France in footnote 23 of the document.

2.4 EHR systems outside EU

It would be helpful if the paper commented on the position in Canada, Australia, New Zealand and USA, especially given the importance of trying to ensure as much consistency as possible between the EU and these countries. This is especially important given the broad international nature of some clinical/medical research which results in global flows of data.

2.5 Persons going abroad for treatment

What happens in situations where the individual goes abroad for treatment - would the healthcare provider in another (Member) State be obliged to forward any information on treatment, etc. back to the EHR manager in the individual's home State?

2.6 Annual Spring Conference of EU and Council of Europe Data Protection Authorities (Larnaca, 2007)

It would be useful if the (updated) paper included some reference to views expressed at the where EHRs were discussed.