Implementing Health Identifiers

A STRATEGIC INFORMATION GOVERNANCE PERSPECTIVE

DARAGH O BRIEN, KATHERINE O'KEEFE

Version 3.0 – November 2015

Updated to reflect impacts of recent rulings of the European Court of Justice and the European Data Protection Supervisor's Opinion on Ethics in Data Management

Castlebridge Associates | Invent Centre DCU Glasnevin Dublin 9 | www.castlebridge.ie

CONTENTS

ABOUT CASTLEBRIDGE ASSOCIATES

Castlebridge Associates is a boutique Information Management training and consulting company providing coaching, consulting, mentoring, and project management services to organisations. We specialise in helping organisations tackle Information Quality challenges, defeating Data Governance difficulties, ensuring Data Protection Compliance safety, or solving complex Information Strategy conundrums/

Drawing from our experiences on the business side of information-driven change management we focus on helping organisations develop internal capabilities to embrace rapidly evolving challenges and secure completive advantages through better use of trusted and trustworthy information and data.

We engage with clients either directly or through our strategic international partners. Our clients have included:

Client	Description of Project(s)
An international airline	• Data Governance Maturity Assessment and Roadmap
EU Institution (Luxembourg)	• Data Governance Maturity Assessment and Roadmap
Irish Public Sector organisation	• Data Protection training • Data Governance and Data Quality advisory on high profile data integration project
Private Hospitals	• Data Protection policy advisory • Data Protection impact assessment on invoice discount financing • Data Protection Audit
An Irish telecommunications company	• Data Protection compliance review • Data Governance Maturity Assessment and Roadmap • Data Governance programme execution • Data Protection incident response support
Irish public service organisation	• Data Protection advisory during tendering process for set up of new Public Sector body • Data Protection training for staff • On-going Data Protection compliance supports
Irish Financial Services organisation	• Information Quality certification training • Information Quality strategy advisory
US based software services organisation	• Data Governance strategy advisory • EU Data Privacy compliance advisory
International not-for-profit	• EU Data Protection advisory • Data Governance for Data Privacy advisory
Education services provider	• Data Protection compliance audit • Staff training across entire organisation • On-going Data Protection supports • Data Retention policy and process definition
Medical secure messaging startup	• Data Protection compliance support • Data Governance policy and process advisory

Contact us via our website: www.castlebridge.ie

EXECUTIVE SUMMARY

This is the third edition of this report. Earlier editions have focused on the draft HIQA standards and their Information Governance implications, and the implications of legislation relating to Gender Identity. The month of October 2015 saw a number of rulings from the European Court of Justice that have had a significant impact on the scope and effect of Data Protection law in Ireland, all with significant implications for the roll out of integrated data sets and data sharing, particularly in a Public Sector context. In addition, the European Data Protection Supervisor's Opinion on Ethics in Data Management, issued in September 2015, is also considered in this edition.

The development of Health Identifiers is placed in the context of a range of legislation that enable and support the objectives of improved patient care through better information management, including the Heath Identifiers Act of 2014, the Health Act of 2007, and the Data Protection Acts of 1988 and 2003. This paper discusses the practical implications of these acts on the implementation of Health Identifiers.

The impacts of impending legislation must also be considered, and the information governance structures for the implementation of Health Identifiers must be flexible and capable of taking into account impending and future legislative changes, such as the European Data Protection Regulation (currently in draft), the Legal Recognition of Gender Bill, and any upcoming Data Governance and Sharing legislation.

The HIQA standards for the implementation of Health Identifiers align closely with standards for Safer Better Healthcare. Thus, the overall strategy for the implementation of governance and standards of Health Identifiers may be closely aligned with existing strategy for Better Safer Healthcare standards. HIQA's standard themes focus on quality of information, communication, effective governance training and skills, a strong focus on privacy, and accountability with clear auditability of controls and a strong evidence-based emphasis.

However, we express concern that an entire theme from the Better Safer Patient Care standards has been removed from the standards for Health Identifiers. This creates a risk of a lack of focus on the outcomes of the full range of stakeholders for Health Identifiers. Furthermore, it removes the explicit requirement to ensure an ethics and evidence-based decision making model for the implementation of Health Identifiers.

We welcome the explicit focus on the development of workforce skills that address the Data Privacy and Information Governance implications of Health Identifiers, but submit that training required must go beyond the fundamentals of the 8 Data Protection principles and address critical skills in Information Governance and Information Quality also.

We provide models for an outcomes-focused, person-centred information strategy for implementing Health Identifiers.

- Our 11 box model illustrates a holistic perspective on the development and execution of effective Business, Technology, and Information strategies that are

aligned with supporting clearly defined Process and Information Outcomes for the providers of healthcare services and the recipients of those services.
- The 11-box model is also presented in the context of an ethics framework that addresses the interplay between the ethical priorities of society and the ethical bias of the organisation in the development and execution of Information Governance structures.
- Castlebridge Associates' 3DC information stewardship model defines the relationships various information stewards have to data and information across strategic, tactical, and operational levels.

Coupled with this, the far reaching implications of the rulings of the European Court of Justice in *Bara* and *Schrems* need to be considered in terms of both their impact on the compatibility of current legislation with EU Law and the practical challenges for Information Governance and stakeholder engagement they present.

We further examine as a case study a recent Irish Public Sector data integration and integration project, which demonstrates several ways in which proper information strategy and governance is key to ensuring successful implementation of a project of this scale.

Key lessons learned from this case study include:

1) Identify and engage with the correct stakeholders in the planning stage;
2) Ensure that the project puts the person at the centre;
3) Ensure a clear basis for processing of currently proposed and future data;
4) Engage with concerns raised rather than dismissing them;
5) Privacy Impact Assessments must be conducted throughout the planning and implementation.

The vital importance Privacy Impact Assessments to successful implementation of a Health Identifier project are a key lesson learned not only from this case study but also from HIQA's international review of similar implementations of unique healthcare identifiers. We also address the importance of sequencing of Privacy Impact Assessments in the context of the life cycle of Information Assets and highlight a fundamental error in the current approach to the roll out of Health Identifiers in that context.

Finally, a structured and methodology based approach to the Governance of Health Identifier information, its use and its development, must be adopted that ensures the desired and desirable Information and Process Outcomes of health care service users are addressed as well as those of health care operators. We present such a framework and outline how it can be scaled to address the ethical issues raised by the European Data Protection Supervisor.

INTRODUCTION

The Health Information and Quality Authority is currently approaching the final stages of drafting standards for the implementation of unique Healthcare Identifiers for individuals and organisations, in accordance with the Health Identifiers Act of 2014.

The introduction of unique Healthcare identifiers will present significant challenges in planning and implementation. It presents many opportunities for great benefit, but it also exposes many risks. The implementation of Health Identifiers is a high stakes project with very strong implications for public trust of Irish healthcare systems, organisations, and healthcare practitioners. As the Irish public has recently witnessed flawed implementations of large scale public sector data integration projects such as Irish Water and the Primary Online Database, public awareness of the risks to privacy in processing of personal data is very high. It is reasonable to expect a very low public tolerance for similar errors in a rollout of identifiers in a field as personal and sensitive as healthcare.

It is paramount that the strategy for design and implementation of data integration in the introduction of Health Identifiers is planned with transparency, accountability, and full engagement with concerns for the respecting of the fundamental rights of individuals (both potential recipients and providers of healthcare).

This paper examines the legal and regulatory context for the introduction of Health Identifiers, aligns the standards in their current form with relevant relevant standards for Better Safer Healthcare, and proposes an information strategy to ensure an outcomes-focussed, person-centred Information Governance Framework that supports best practice in patient care and ensures compliance with legal frameworks and standards. Planning a solid information strategy to implement proper governance structures, good communication, and clear lines of accountability with clear respect for individual rights and privacy should help to ensure the development of a person-centred, outcomes focused rollout of Healthcare Identifiers that supports standards for Better Safer Healthcare.

In addition, the recent ruling of the European Court of Justice in *Bara,* as well as the comments of the Court in *Schrems,* are considered as they have significant implications for the development of integrated data registers through the sharing of public sector data. We have updated our section by section analysis of the Health Identifiers Act 2014 with reference to these cases and include a detailed analysis of their impacts in a new section of this report.

The European Data Protection Supervisor's (EDPS) Opinion on Ethics in Data Management, which the EDPS has highlighted in a number of public forums as being a model for future assessment by Regulators of the privacy risk management approaches

of Data Controllers, is also examined, drawing on models presented in our *Primer on Ethical Principles in an Information Governance Framework*[1].

As before, we continue to keep this report updated to reflect developments in relevant legislation or information governance practices and will publish updated editions as required. Purchasers of this edition of this report will receive one free update. Castlebridge Associates ClouDPO or CloudCDO customers will receive all updates for free as part of their monthly or annual subscription.

Finally, it must be note that nothing in this report should be construed as legal advice and is presented for information purposes only. Readers are advised to seek independent advice before taking actions on foot of this analysis.

[1] O'Keefe, K., O Brien, D, *A Primer on Ethical Principles in an Information Governance Framework,* Castlebridge, 2015 https://castlebridge.ie/products/whitepapers/2015/10/primer-ethical-principles-information-governance-framework

DRIVERS FOR A HEALTH IDENTIFIER

When considering drivers for health identifiers, it is important to bear in mind that the Health Identifiers Act 2014 defines two types of identifier: one for individuals in receipt of care and another for organisations and individuals involved in the delivery of that care.

The main benefit of having an individual health identifier is an improvement to patient safety. Being able to uniquely identify each user will improve patient safety by reducing the number of adverse events that may happen, such as giving the patient incorrect medication or vaccinations or admitting the wrong person for surgery.

Other expected benefits of an Individual Health Identifiers include improved accuracy and efficiency in record keeping across healthcare organizations, including seamless sharing of information such as records and referral letters between public and private providers. This should result in a more complete record of care.

It is anticipated that the introduction of Individual Health Identifiers will enable electronic transfer of health information, improving speed and efficiency in care, and supporting safe transfer of information between correctly identified organisations and providers. The Health Information Quality Authority anticipates the use of Individual Health Identifiers for electronic referrals, discharges, and prescriptions.

HIQA has also identified several significant drivers for the introduction of a Health Services Provider Identifier, including providing clearer accountability by clearly identifying the person and organization responsible at each stage of care, and reducing administrative costs. Another driver is the possibility of improved capabilities for tracking and audit, including the enabling tracking of healthcare practitioners across regulatory authorities.

The Register is intended to be seen as a single authoritative source of information, thus reducing administrative effort and supporting measurement and analysis of resources for better planning of services. Another driver could include an improved ability to track health care costs.

However, these benefits assume identifiers implemented to a high level of quality. The expected benefits driving the implementation of Health Identifiers are dependent on high information quality and have very little tolerance for error. The information must be fit for purpose to support any of these benefits. Ultimately, Individual Health Identifiers and Health Service Provider Identifiers are simply data. Their benefit depends on their fitness for purpose and how they are used. Care must be taken to avoid a technology being presented as a panacea to all ills in the Healthcare system.

It is important to avoid conflation of Health Identifiers with Electronic Health Records. While one is an enabler of the other, as we discuss later the legislation requires a very clear segregation of function and management of scope creep in the development of Health Identifer Registers.

THE LEGAL BACKGROUND

The development of a Health Identifier must be seen in the context of a range of legislation that enable and support the objectives of improved patient care through better information management. The underlying goals, the creation of a single unique identifier that would provide a means to tie together currently patient care information across multiple providers and the creation of a master record of health service providers, require the aggregation and integration of data from a variety of sources.

The goal of the legislation is to provide a legal basis for a "single view of patient" and "single view of provider". Challenging as it was to define the legislation, the lessons from other industry sectors are that the implementation of systems and processes for the creation and maintenance of these "single views" present both a significant opportunity and a serious challenge.

THE HEALTH IDENTIFIERS ACT 2014

The Health Identifiers Act 2014 provides the legal basis for the creation of two categories of Health Identifier, the Individual Health Identifier and a Health Services Provider Identifier. The Act also provides for the creation of two registers. The first is a National Register of Individual Health Identifiers, which will contain data about people. The second is a National Register of Health Services Provider Identifiers, which will contain unique identifiers for organisations, locations, and individuals.

The Act sets out a range of provisions for the establishment of both, including defining the "other identifying particulars" of individuals and the "relevant information (health services provider)" for health services providers.

In addition, it sets out a range of decision points, time scales for response to data-impacting events, rules regarding the transfer of Health Identifier data outside the jurisdiction, and enumerates a range of permitted uses of the identifiers.

A series of offences are set out in the legislation, including offences arising from "recklessness" in the provision of data, unauthorized access to or processing of Health Identifier data, or accessing "purporting to be other specified person". Penalties on summary conviction will be up to €4000 (Class B fine) or up to €100,000 on indictment.

Interestingly, the legislation only creates an offence for the provision of misleading information relating to a Health Services Provider Identifier. Notwithstanding that the legislation clearly envisages the Health Services Identifier data as including personal data of clinical and other staff, it would appear that unauthorized access to or processing of the data of individuals who are providing health care are protected primarily by the Data Protection Acts, with a lower maximum penalty (for now).

As with the Data Protection Acts, there is a provision for personal liability of officers of bodies corporate such as managers where an offence is committed under the legislation.

Finally, the legislation sets out the specific interplay between the Data Protection Acts.

SUMMARY OF KEY PROVISIONS

Section	Summary of Meaning & Implication
Section 2(1)	A number of key definitions are contained in this section. • *Health research* is defined in the context of an ethics board; Therefore, Information Governance will need to reflect rules about when/how to refer secondary purposes to an ethics board. *Other identifying particulars* is defined as including "Sex". How this is to be defined and modelled is a key question (see below). Other data enumerated includes "signature", subject to a somewhat Kafkaesque exclusion test.
Section 3(7)(b) and (c) and Section 3(9)	Introduces a public interest test in the definition of master data and meta data that is central to the application of the Registers in practice. Public interest determination will be balanced towards the protection of privacy and the securing of one or more relevant purposes. In the context of Article 8 ECHR and *Digital Rights Ireland* this would suggest that there will need to be a clear necessity for the processing and that the processing will be proportionate to the purpose. ***Bara* would also suggest that this Public Interest test would need to be communicated and communicable as part of the stated purposes for processing. *Bara* reaffirms the need for data to be obtained and processed fairly and for the purposes of processing to be communicated – explaining why the trade-off in privacy is necessary/proportionate in a Public Interest context is likely a key element of that as it would fall under the "other information necessary to guarantee fair processing" provisions of Article 10 and Article 11 of the Data Protection Directive 95/46/EC, and Recital 38 of the Directive.**
Section 3(10)	Allows for regulations made under the Act to be annulled within 21 sitting parliament days but it will not affect the legality of previous processing. This is an important time frame. **Where a Regulation made under the Act is incompatible with EU law, processing on foot of it cannot be held to be legal. This has been made clear by the CJEU and obligations under EU Treaty trump Statutory Instruments. *Bara* makes clear yet again the primacy of the Directive, Charter, and TFEU obligations.** **This highlights the need for *prior execution* of PIAs.**

Section	Summary of Meaning & Implication
Section 5	Individual Health Identifiers apply to both the living and the deceased regardless of whether the individual is resident in the State. The key factor for creating one is that a health service is *or may be* provided. Processing from a Data Protection perspective starts at the first presentation at a care provider. The section also states that the Individual Health Identifier itself is Personal Data, but won't contain any other personal data. In practical terms this means that the Personal Health Identifier is personal data, even if it is not linked to other personally identifying data. Finally, the section deals with telling people, or their carers or next of kin, what their Identifier is ***Schrems* may have an impact here in the context of the powers conferred on the Minister under Section 5(4). The Minister's perception of 'appropriateness' must be secondary to the findings of the DPC and the obligations of the State under Article 16(2) of the TFEU and Article 8 of the Charter of Fundamental Rights. The CJEU in *Schrems* was at pains to stress the independence of Data Protection Authorities and that constraints on their independence in legislation or Commission decisions were incompatible with Treaty obligations.** **In practice therefore, the Minister's powers under Section5(4) will need to be exercised with the guidance of, and subordinate to, any decision or recommendation from the Office of the Data Protection Commissioner. From an Information Governance perspective this will require effective Privacy Impact Assessments and the execution of a clearly defined, privacy supportive, ethical framework around the operation of Health Identifiers.**
Section 6	Addresses the establishing of the Individual Health Identifier Register. The scope of data to be included in the Register is restricted to ONLY that data that is defined in section 2 of the Act. Changes to the Register to include other data will require either amendment of the Act or a Statutory Instrument. • Permits the retention of data of deceased persons and requires the Individual Health Identifier register to be updated with death details.

Section	Summary of Meaning & Implication
	It is important to note that this section effectively and explicitly precludes the conflation of Health Identifiers with Electronic Health Records. While IHIs may be a key enabler for EHRs, in terms of the scope of any Privacy Impact Assessments and the design of the underlying Information Architecture and Data Model for the IHI Registers must reflect this clear segregation of purposes. **For any data model design that conflates EHR purposes with the IHI not to be unlawful under the Data Protection Acts, the Health Identifiers Act 2014 would require an amendment, and the sharing of data for that purpose would in turn need to meet the tests set out in the *Bara* case.**
Section 7	This section sets out some ground rules for the use of data in the Individual National Health Identifier. It empowers the Minister to use any "identifying particulars" of a person already in the Ministers' possession to create the Register, **regardless of when it was obtained**. The practical application of the above It requires individuals to comply with a request for information "as soon as reasonably practicable. It requires Health Services Providers to provide "other identifying particulars" provided to them to the Minister (i.e. to update the Register) within **30 days** of being provided with such data. It introduces a 2 stage test for health services providers to communicate updates and correct errors in the Individual Health Identifier Register. • Where the Health Services Provider becomes aware that there is an error, they must notify the Minister with details of the error within 30 days, but they do not need to have or to provide the correct data. This means that as soon as an error is known, it must be reported in 30 days. • However, once the correct data comes into their possession they have to provide it to the Minister within 30 days.

Section	Summary of Meaning & Implication
Section 8	For the purposes of developing and validating the accuracy of the Register of Individual Health Identifiers, any Government Minister may be asked to provide data such name, address, ppsn, date of birth etc. so that the Register can be created and validated. *This is an exceptionally broad section and would encompass any pre-existing register of personal data held by any Government Department or Government Agency acting on behalf of a Minister. Examples of Data sets that could be requested:* • LPT register from Revenue Commissioners • Data from POD and other databases held by the Dept of Education • Registers for statutory schemes administered by the Department of Agriculture • Data from schemes administered by the Department of Enterprise Trade and Employment • Databases held by the Department of Social Protection **BARA IMPACT** **Bara makes this section difficult to execute without effective and proactive Governance and communication around information. A detailed analysis will be included later in this document. However, it is no longer sufficient (and indeed never was sufficient under the Directive and Charter of Fundamental Rights) for Public Sector bodies to rely solely on a statutory basis for data sharing.**
Section 9	This section requires that data of births and deaths and the identifying particulars of the born or deceased, would be provided to the Minister to update and maintain the Register. **Again, this would require changes to notification to parents of children that data would be shared in this way in order to comply with *Bara*.**

Section	Summary of Meaning & Implication
Section 10	Section 10 addresses access rights and controls. It does so by referencing the concept of a "specified person", a "relevant purpose", and "relevant information". A "relevant purpose" is defined as either being the provision of healthcare or a range of secondary purposes set out in Section 2 of the Act[2]. This includes sharing the Health Identifiers and associated data with Health Insurers and the performance of "any function conferred on a person under this act or another enactment for which the processing of identifiers is necessary".
Section 11	This section addresses the use of the health identifier and the Register. This section allows for a search of the register based on "other identifying particulars" to identify individual's health identifiers, as well as empowering health service providers to request at point of treatment. The Individual Health Identifier will be associated with the record that the provider makes of the provision of Health Services and will be "indicated" in any relevant communication, which includes any communication sent to the Minister, any other "specified person" or "authorized disclose", or the individual for any "relevant purpose". *In the context of the* HSE Standards and Recommended Practices for Healthcare Records Management *it is important to note that "communications relating to the service user and his/her care" are considered part of the Healthcare Record. This means it would constitute breach of the Act not to include the Health Identifier in a WhatsApp or SMS communication relating to the care of a patient*. Section 11(5) requires that an "Exceptions Log" be kept for instances where patients don't have a Health Identifier or refuse to provide it or other identifying particulars, or the access to the

[2] These are essentially the lawful processing conditions for Sensitive Personal Data in the Data Protection Acts restated. Specific secondary purposes that are envisaged include promotion of patient safety including clinical audit, the identification or prevention of public health threats, the management of health services (which includes logistics, evaluation, compliant handling, and management of IT systems), the conduct of research *that is subject to an Ethics approval process.* Some "catchall" terms are used to further extend the scope of Secondary Purposes.

Section	Summary of Meaning & Implication
	National Individual Identifiers database is unavailable (see Section 11(4)). The section also allows for transfer to specified persons or authorized discloses for primary of secondary purposes. ***Bara* may also impact the execution of this section in practice, particularly with regard to the transfer of data to specified persons or other forms of disclosure for secondary purposes. This would extend to the sharing of the "Exceptions log" data with other bodies – such sharing purposes would need to be disclosed at the time of creating the log entry.**
Section 12	This section deals with the transfer of Individual Health Identifiers outside the State relating to people who are receiving an equivalent Health Service in another Member State (we must assume this is "Member State" of the EU as this term is not defined). Such transfers will be permitted only where: • The service being availed of is an "equivalent service" • It is being offered in an EU Member State • There must be an agreement between the Minister and a person they consider to be the equivalent of a Health Services provider to allow access to the Individual Health Identifier Register • The DPC has been consulted about the agreement (note: not the same as DPC having approved an agreement) These agreements will require an amount of detail to be recorded about the counterparty, including personal contact details of their "nominated representative", the specific activities for which they will be processing the relevant information and/or access the National Register of Individual Health Identifiers. Furthermore, these agreements must contain specific provisions regarding security and ensuring that data is not accessed without authorization and sanctions that are to be provided for in the event of any breach. Finally, this section gives the DPC a watered down version of powers that the Office would have already under Section 10(1)(a) of the Data Protection Acts in that they can, at any time, review the operation of an agreement. The difference here is that the DPC would report to the Minister who would take any action they deemed appropriate.

Section	Summary of Meaning & Implication
	Bara has implications for the 'in practice' operation of data sharing under this section. While a Statutory basis exists for the sharing, and while there is a requirement for the DPC to be consulted, Bara requires prior notification to affected Data Subjects of the sharing of data, which would include any proposed transfers outside the State. **It is possible that the only way in which the transparency and disclosure requirement of _Bara_ can be met in this context is through the publication of such Data Transfer Agreements, specifically the information set out in Section 12(2) of the Health Identifiers Act in a publicly accessible format** **_Schrems_ also has implications for this section should the DPC determine that a transfer is to a 3rd country that does not provide the required level of protections for personal data privacy. The apparent discretion of the Minister in this context to pick and choose from the recommendations or findings of the DPC in this context would raise a significant question as to the effective independence of the DPC**
Section 13	This section mirrors Section 5 but with regard to Health Services Providers. Each Health Service Provider will have a unique identifier, even if they provide Health Services in a number of different contexts (as an organization, as a facility within an organization etc.) It will apply to both individuals and organisations. Where it applies to an individual the Identifier will be personal data in its own right. Section 13(4) seems to suggest that the identifier could be "intelligent" with an internal classification scheme for categories of health practitioners being a component of the identifier (e.g. an alphanumeric code or other structure).[3]
Section 14	This section reveals that the Health Services Provider Identifier Register will actually be four registers. • Healthcare Practitioners • Healthcare services bodies • "Relevant Employees" of healthcare providers • "Relevant Agents" of healthcare providers who are individuals • "Relevant Agents of healthcare providers who are organizations An array of data including first names, surnames, and job roles and place(s) of work are to be recorded.

[3] If this is the case it is not consistent with best practice in both data quality and data modelling as it may have overloaded a variable to hold two distinct facts.

Section	Summary of Meaning & Implication
	The Minister is empowered to seek additional identifying data, however this power can only be exercised after consultation with the DPC. *The drafting of this and Section 13 gives cause for concern regarding the data modelling and design of processes to keep this register updated.* ***Bara* would suggest that the statutory basis itself would not be sufficient and prior communication to Data Subjects would be required.**
Section 15	This section empowers the Minister to request data from relevant professional regulatory bodies. • Organizations will have 3 months to provide the initial data load. • Updates will need to be processed within 30 days. • Inaccuracies will need to be reported within 30 days, but corrected data need only be provided within 30 days of it being received. ***Bara* applies in this context also. The statutory basis for sharing of data is insufficient and the source organizations will need to have communicated the sharing purpose with their members, and the agency administering the Register would need also to set out to the affected data subject the purposes of their processing and other relevant information.**
Section 16	As above, only for "relevant bodies", which are defined as being either the HSE or any other body corporate or unincorporated body of persons who the Health Services Practitioner delivers Health Services. In short: Hospitals, clinics, GP practices, counselling providers etc. all constitute "Relevant bodies". ***Bara* again applies in the context of this section.**
Section 17	This section is broadly the same in effect as the previous two sections. It relates to the provision of data about employees and agents of health practitioners or "relevant bodies". One key difference is that where a health care provider or relevant body has no employees or agents, they must still disclose the zero headcount. ***Bara*, yet again, raises additional requirements in terms of the practical implementation of data sharing in the context of employee data.**
Section 18	This equates to Section 7 and grants the Minister the power to use any data that is in the possession of the Minister or the HSE to establish and maintain a register of health service provider identifiers, regardless of when the data was originally obtained.

Section	Summary of Meaning & Implication
	***Bara* ruling will impact the application of this section as it is no longer sufficient for there to be simply a statutory basis for the data sharing for it to be lawful.**
Section 19	This states that the Register of Health Services Providers will be, in effect, a publicly accessible register. The Minister will need to put in place measures to allow this register to be accessed. Issues such as those raised in the provision of data to genealogy websites may arise here from a Data Protection perspective. However, many health service providers are already listed in public registers. **This section is a processing purpose for Health Identifiers for Health Service Providers that will require prior notification to employees, especially where those employees are not members of bodies publishing public registers of members. *Bara* (again) raises its head here.**
Section 20	This section governs the actual use of the health services identifier and the National Register of Health Service Identifiers. It creates an imperative requirement for Health Service Providers to associate their Health Service Provider Identifier with "the record" that they make *or cause to be made* (i.e. instructs that it be recorded). It also creates an imperative that their identifier is contained in any "relevant communication". A "relevant communication" is defined in the same way as in Section 11(7) with the same implications in the context of HSE Guidelines on Patient Care Record Records management.
Section 21 – 25	These sections set out the specific prosecutable offences under the Acts. For Individual health Identifiers, the following offences will exist: • Making false or misleading statements either knowingly or recklessly[4] to obtain a Health Identifier for an individual. • Concealing a material fact in the application for an individual Health identifier • Giving of false or misleading information of a material nature in purported compliance with a provision of the Act • Access to the Register, unless in accordance with the Health Identifiers Act or some other enactment • Processing someone else's individual health identifier for a purpose other than a relevant purpose • Accessing the National Register of Individual Health Identifiers using someone else's login ("by use of a means

[4] Recklessness in law goes beyond carelessness or negligence and requires a degree of conscious disregard to consequences in the conduct of an action.

Section	Summary of Meaning & Implication
	which purports to identify the specified person as a different specified person") Fines will range from between €4000 to €100,000. For the Health Service provider identifiers, a similar set of offences is created: • Making false or misleading statements either knowingly or recklessly to obtain a Health Identifier for an individual. • Concealing a material fact in the application for a Health Services Provider identifier • Giving of false or misleading information of a material nature in purported compliance with a provision of the Act It should be noted that there is no offence committed if the Register of Health Service Providers is accessed without a purpose under the Health Identifiers Act or other enactment, nor is it an offence to process a Health Service Provider's Identifier for a purpose other than a relevant purpose. Fundamental Data Protection Act principles will apply in this case. Finally, Section 25 creates a clear personal liability for officers, director, and managers of Bodies Corporate, including bodies that are managed by their members. If any of the above offences are committed with the consent, connivance, or is attributable to negligence on the part of such persons, or people purporting to be such persons, that person, as well as the body corporate, is guilty of an offence and may be prosecuted. This reflects the personal liability of officers of bodies corporate that exists under Section 29 of the Data Protection Acts 1988 and 2003, but extends it to a wider scope of issues in the context of effective patient records management.
Section 26	Allows for the Minister for Health and Children to delegate functions to other entities. **The *Bara* ruling would indicate a need for effective Information Governance to clearly manage the roles, responsibilities, and accountabilities of such bodies but also to ensure that those roles, and the nature of processing or sharing of data between such bodies, is clearly communicated.** **This section clearly requires a well-defined governance model to be in place in which the roles, responsibilities, and accountabilities for information and information related outcomes which may be delegated are clearly understood and transparently documented.**

Section	Summary of Meaning & Implication
Section 27	This section sets out the relationship with the Data Protection Acts 1988 and 2003. • It reaffirms that living individual's individual health identifier is personal data (as stated in Section 5). • It reaffirms that the individual health identifier will ALWAYS be personal data regardless of who is actually holding the identifier. No mention is made of the individual identifiers assigned to Health Services Practitioners which would also constitute personal data as stated in Section 13 of the Act. The section also states that the provisions of the Data Protection Acts relating to appropriate organizational and technical controls to ensure the security of data against unauthorized access, alteration, and disclosure will apply equally to data held in a Health Register relating to a deceased person.
Section 28 – 29	Section 28 empowers the Minister to conduct investigations into the operation of the Act to ensure the proper assignment and use of identifiers. Section 29 grants the Minister powers to enter into agreements with third parties to conduct one or more functions under the Act. These two together would suggest that the Minister is empowered to engage independent third parties to review the operation and use of identifiers. **The reasoning of the CJEU in *Bara* would suggest that the powers conferred on the Minister under Section 29 would need to be executed with appropriate care and transparency to identify, at the time that data used to create the identifier was obtained, at the very least the categories of entity that data might be shared with and what functions might be performed by such entities with data.**
Section 30	This is an extensively powerful section that allows the Minister to do, or cause to be done, anything that is considered necessary to verify information from any non-governmental source and to establish the efficient and effective operation of the Registers. There is a positive requirement to co-operate with such requests. This presumes "official" data sets are 100% accurate at all times. **Again, *Bara* would suggest that prior communication of the kinds of activities or methods that would be used to verify data and ensure effectiveness and efficiency of the operation of the Registers would be required.** **The HSE/Dept of Health/Minister would, we suggest, be well advised to consider how the overall scheme of processing and strategy for execution and administration of the Register will be communicated on an *on-going* basis.**

Section	Summary of Meaning & Implication
Section 31	This section empowers the Minister to enter into data exchange agreements that will specify the procedures to be followed by each party with respect to the sharing of personal data between them for the purposes that the agreement relates. It is important to highlight that an agreement will need to be clear as to the purposes and a key governance control would be to control against scope creep in the operation of the data sharing agreement. The section requires the Minister to consult with the Data Protection Commissioner in relation to the creation of or alteration of any such agreement. This strongly implies that Privacy Impact Assessments will be required as part of this process. **This section has a potentially increased significance under the *Bara* ruling. Reading the two together, it would appear that for any data exchange agreement authorized under this section to be lawful it would appear that the DPC would need to be satisfied as to the level of information about the data exchange that was being communicated to the Data Subjects.** **This makes the adoption of rigorous Information Governance controls and effective Privacy Impact Assessments during the *planning* of any data exchange (not *post fact*) an essential element of compliant operation of any Register.** **In essence, *Bara* creates a situation under this section where the Minister *must* consult with the DPC (whose role as an *independent* Regulator was stressed by the CJEU in *Schrems*) and satisfy them that they are communicating appropriately with Data Subjects as key stakeholders in any Data exchange.** **The CJEU in *Schrems* made clear that a Data Protection Authority has a duty to investigate breaches of the Data Protection Acts, the Directive, and fundamental rights to Data Privacy under the Charter, so any failure to do so would raise questions about the independence of the DPC.**
Section 32	This section requires that all processing is necessary for the performance of a function under the Acts. This is a "belt-and-braces" restatement of the Purpose Limitation principle in the Data Protection Acts and the clear proportionality principle set out by the CJEU in *Digital Rights Ireland v Ireland*. Again, it would strongly suggest that Privacy Impact Assessments will be necessary to ensure that processing is compatible with the Health Identifiers Act and the Data Protection Acts. This is especially the case given the penalties for access or processing of Health Identifiers without cause.

Section	Summary of Meaning & Implication
	Taken in conjunction with *Bara* this section would suggest that any communication of processing must be transparently linked, in a readily explicable manner, to a function under the Acts and that this must be presented to Data Subjects.

As can be seen, the Health Identifiers Act 2014 creates an incredibly powerful framework for the gathering of data about individuals from the cradle to the grave (and beyond). Whether by accident or design the Act also contains differing levels of protection for the personal data of the users of healthcare services as compared to the individuals providing those services.

Some of the provisions appear to have the effect of creating "baked in" data quality and data governance issues, not least the provisions in Section 13(4), and the potential day to day operational challenges of ensuring that the various Registers envisaged are kept accurate and up to date cannot be understated.

Furthermore, the day to day operational realities in health service delivery may pose challenges in ensuring compliance with requirements such as those not to share logins etc. The clear requirement to associate both individual health identifiers and health service provider or practitioner identifiers with "relevant communications" has significant implications for the use of "civilian" instant messaging tools such WhatsApp or Apple iMessage. More structured and controlled solutions will inevitably be required.

Finally, the recent rulings in *Bara* and *Schrems* impact on a wide range of functions and powers conferred in under the legislation. Effective compliance with the principles set out in these rulings will require effective and robust Information Governance frameworks to be put in place. A key element of such frameworks will need to be a strong focus on the individual (service user, medic, employee) as a stakeholder to be communicated with and engaged with.

In implementing and establishing these Registers, we would recommend that the key lessons of "consumer focus" and transparency from other recent Public Sector and quasi-public sector initiatives taken to heart. The strong "patient-centric" focus, as espoused by HIQA in their National Standards for Safer Better Patient Care is essential, and echoes the emphasis on individual rights highlighted by the CJEU in *Bara*.

DATA PROTECTION LAW

Data Protection law in this context encompasses both the Data Protection Acts 1988 and 2003 and the provisions of Article 7 and Article 8 of the Charter of Fundamental Rights as enshrined in the Treaty for the Formation of the European Union. By necessity it must also encompass the interpretation by the European Court of Justice (CJEU) of the Directive, Charter, and Treaty and the compatibility of national laws with the aforesaid foundational laws.

It is important to note that personal data privacy rights in the EU are grounded in fundamental rights and are enshrined as a right under EU treaties. National legislation must be drafted and interpreted in a manner that is consistent and compatible with those Treaty rights. The CJEU in *Bara* makes it clear that selective derogations in national law from fundamental principles in the EU Charter of Fundamental Rights are not sustainable, can be challenged, and will be struck down with retrospective effect.

Where the Health Identifiers Act 2014, or actions taken in the course of pursuing the objectives of that Act is at odds with either the Data Protection Acts or Article 8 of the Charter of Fundamental Rights, then the key test will be whether any infringement of personal data privacy rights which may arise is both necessary and proportionate in the context of the purpose (*Digital Rights Ireland*) and whether there was appropriate communication of the processing to the Data Subject, notwithstanding the existence of a statutory basis (*Bara*).

Given that the Health Identifiers Act recognizes in Section 11(4) that treatment can be, and indeed must be, provided irrespective of whether the individual receiving treatment has a Health Identifier or provides "relevant identifying information" or not, and the practical challenges in a clinical environment of giving information about processing and potential sharing of data, this may be a difficult threshold to meet and will likely need to be assessed on a case by case basis. The Governance structures around the implementation and operation of the Identifiers will need to cater for circumstances where communication of 'fair processing notices' is not possible and information will need to be developed in readily digestible packages for patients, medical staff, and non-medical employees.

The Health Identifiers Act 2014 defines both individual health identifiers and health service practitioner identifiers as being personal data in and of themselves, regardless of context. Therefore, the full gamut of the existing Data Protection Acts applies to them with regard to fair obtaining, purpose specification and limitation, security, retention, adequacy, etc. Therefore, the necessity and proportionality test will apply to any proposed secondary uses of these identifiers. Likewise, the need to meet the 'fair obtaining' test in *Bara*, notwithstanding any existing statutory basis for processing, applies to the identifiers themselves, not just any additional data that might be processed ancillary to the identifier data (e.g. the inclusion of the identifier in an EHR record).

Furthermore, as these identifiers have been defined in law as being, in and of themselves, personal data it will **not** be possible to use these identifiers as pseudonymous identifiers for individuals in research or other purposes. Appropriate governance will need to be implemented to ensure that this does not happen.

In the context of the proposed matching and consolidation of data from a variety of different sources to create the various registers, it is important to note that the act of matching and consolidating data constitutes processing under the Data Protection Acts. Notwithstanding the powers granted to the Minister under the Health Identifiers Act 2014, the processing of data for the creation of the Registers must also be compatible with the purpose for which the data was originally obtained by the source[5].

Bara adds a further requirement that there be communication of the potential for sharing by the source and that the purposes for processing by the recipient agency must also be communicated to the Data Subject. We will examine this in more detail in a later section.

Furthermore, the accuracy of any resulting matches will need to be appropriately quality assured to avoid falling foul of the Accuracy and "up-to-date" requirements of the Data Protection Acts. Appropriate mechanisms will be required to remedy any incorrect matches in a timely manner (a 30 day wait might might be perfectly OK for a direct marketing company, but a patient-care impacting error in identifier data could have significant impacts on quality of care. Likewise, a 30 day wait for Healthcare Practitioner data to be updated could lead to issues in reliability of data for audit and/or investigation purposes.)

Individuals may be unaware of the proposal or potential for data about them to be matched and consolidated for the purposes of creating a Health Identifier, either for an Individual or for a Health Care Practitioner. *Bara* makes clear that this is an unsupportable position that is incompatible with Article 8 of the Charter and with the obligation on legislatures under Article 16(2) of the TFEU to enact legislation that is compatible with the fundamental right to personal data privacy.

Given the incredible breadth of potential data sources that the Health Identifiers initiative will potentially consolidate data from, it is essential that appropriate briefings and education are provided both to individuals about whom identifiers are to be created and to the staff, consultants, and contractors who will be engaged to implement the various Registers. Such briefings and communications will need to be kept up to date and will need to reflect changes in sharing, sharing partners, purposes, and transfers. This will require an effective and transparent Information Governance framework to be put in place.

Such an approach would be entirely consistent with HIQA standards for Safer and Better Patient Care which put the individual at the centre of attention. Failure to

[5] For reference, see this guidance note from the Data Protection Commissioner : https://www.dataprotection.ie/docs/Data-Protection-Rule-3/25.htm

engage such an "individual centric" approach to planning, governing, and executing the development and operation of the Register will inevitably result in otherwise avoidable public disquiet, over-reaching and disproportionate processing, and inadvertent breaches of fundamental data privacy rights.

The emphasis on the "individual centric" approach in the HIQA standards for Safer and Better Patient care can be applied equally to non-patients who fall under the scope of the Health Identifiers Act 2014. In this context, it is worth considering the principles set out in the EDPS in his Opinion on Ethics in Big Data, not least the introduction into the discussion of Data Protection compliance the issue of respecting human dignity, which is set out in Article 1 of the Charter of Fundamental Rights and is the only right enumerated in the Charter which is non-negotiable and cannot be balanced against other rights.

OTHER RELEVANT LEGISLATIVE CHANGES PENDING

Of course legislation does not stand still. In this section we discuss a number of pending legislative developments that will have a direct influence on the design and execution of a Health Identifier system. For the purposes of this paper we have focused on two legislative changes that are pending within the next two years, but others exist and organisations should ensure that their Information Governance and data management structures are established in such a way as to ensure an appropriate treatment of these impending changes.

In the context of these two pieces of legislative change, we examine just one area of change, recognition of gender identity, and outline some potential implications within the context of the implementation of Health Identifiers

EU DATA PROTECTION REGULATION

In the Draft EU Data Protection text approved by the European Parliament, "Gender Identity" has been introduced as a new category of Sensitive Personal Data alongside "Sexual Orientation". The Human Rights basis for this inclusion is consistent with the reasoning behind all the other categories of Sensitive Personal Data[6].

"Gender Identity" isn't defined as a term in the EU Data Protection Regulation texts. But it does pose a complication when we consider the question of "Sex" as an identifying particular within the Health Identifiers Register. Simply put, "Sex" is not the same as "Gender" and is not a fixed concept and a clear and consistently applied standard for recording this data will be required. Also, the design of the Health Identifiers Registers will need to accommodate the concept of the "identified-as" gender of a person changing over time.

[6] For more on this topic, see: O'Keefe, Katherine *An interesting definitional bind: EUDataP and Modelling Gender,* Castlebridge Associates blog, April 2009 https://castlebridge.ie/blog/2015/04/29/interesting-definitional-bind-eudatap-and-modelling-gender

The Gender Recognition Act 2015

The Gender Recognition Act recently passed by the Oireachtas does provide a definition of "Gender Identity" as referring:

> *"…to each person's deeply felt internal and individual experience of gender, which may or may not correspond with the sex assigned at birth, including the personal sense of the body (which may involve, if freely chosen, modification of bodily appearance or function by medical, surgical or other means) and other expressions of gender, including dress, speech and mannerisms;"*

This definition encompasses the concept of gender reassignment over time or the representation of gender identity through other means. This raises an interesting data modelling challenge in the context of the Health Identifiers database.

The Act allows anyone over the age of 18 to request the An t-Ard Chláraitheoir to record and recognize their gender identity in a Gender Recognition Register and to note the existence of that registry entry on the Register of Births. Applications by persons under the age of 18 can be made by their parent or guardian.

The Act allows for the registration of a preferred forename or forenames where the applicant so wishes.

In addition, the Act states that the layout of Birth Certificates for persons who are registered on the Gender Recognition Register be indistinguishable from a certificate issued to people who aren't on that particular Register. It also requires that any request for a Birth Certificate will be interpreted as being a request for a copy of a certificate that contains the particulars entered in the Gender Recognition Register unless the alternative is specified and authorized.

Data Sharing & Governance Bill

This Bill, originally proposed by the Department of Public Expenditure and Reform last year, proposed the creation of a framework for data sharing in the public sector that would allow for sharing between different master data registers.

The scope of the Bill was criticized by a number of stakeholders during the Public Consultation phase. One key area of challenge was the definition of what was meant by "sharing". Another area of challenge was the variability of standards and standard practices across public sector organisations.

Castlebridge Associates, on behalf of Digital Rights Ireland, submitted an extensive analysis of the proposed Bill and made a series of recommendations to address deficiencies identified. A copy is available on our website.

Revised Heads of Bill for the Data Sharing & Governance Bill have recently been published by DPER and will be the subject of a separate analysis and report by Castlebridge Associates shortly.

IMPLICATIONS

The implications of the Gender Identity Bill and the EU Data Protection Regulation for the governance of data in a Health Identifiers Register would include:

1. The structure of the data model for Health Identifier Registers or identifying particulars may need to change to cater for scenarios where a patient, healthcare practitioner, relevant employee, or relevant agent formally reassign their gender identity. A key decision will need to be taken as to whether a Health Identifier is a permanently unique identifier or if, on foot of a change of gender identity, a new entry is required. If the latter, the question then arises about lineage of data and ensuring that, for patients and practitioners, a full and complete history can be identified.
2. User access controls will be required to limit the access of individuals to historic data indicating a change of gender identity, in line with the restrictions that are proposed in the Gender Identity Bill and the proposed classification of Gender Identity as "Sensitive Personal Data" in the General Data Protection Regulation.
3. The Identifying particular of "Sex" as a binary concept in the Health Identifiers Act 2014 will need to be interpreted more broadly than simply physical sex and it may also need to reflect gender identity. This will include a need to reflect changes over time to physical sex in response to recognition of gender identity.
4. Processes will need to be developed to obtain access to data from the Gender Recognition Register. These processes will need to have a clear statutory basis and will need to reflect the strong confidentiality principle that is enshrined in the current draft Legal Recognition of Gender Bill and the potential recognition of Gender Identity as a distinct category of Sensitive Personal Data under the Data Protection Regulation.

This is not an exhaustive list. It does highlight the need for a clear and consistent approach to the definition of and governance of key data within the Health Identifiers registers. This issue brings into clear relief the need for any Registers created under this Act to be subject to a sectoral approach to Information Governance that will address:

- Definition of data models
- Definition of metadata and master data standards
- Change control policies
- On-going Privacy Impact Assessments to ensure changes to legislation or work processes continue to provide high levels of protection
- Quality-assured data lineage and data integration standards
- Clear definition of controls and frameworks for appropriate user access to ensure that the privacy of personal data held in any of the Health Identifier Registers proposed is balanced effectively against a range of competing rights and duties.
- Development of methods and models for communicating accurate and up-to-date information about how data will be used, shared, or disclosed, that support the dignity of the individual and ensure the key tests in *Bara* can be met.

All of this must be done in a manner that reflects the importance on focusing on information and process outcomes for patients, health care practitioners, and relevant employees and agents in a manner that is supportive of the preservation of human dignity and balances fundamental rights.

NATIONAL STANDARDS FROM HIQA

The Health Information and Quality Authority (HIQA) has set out a range of standards for Safer Better Patient Care. The interpretation of HIQA's perspective or expectations on any activities in the Healthcare sector must be based on these standards and any associated guidance and guidelines.

In this section we provide a brief summary of HIQA's standards and then examine the application of those standards to the question of Health Identifiers.

OVERVIEW OF HIQA'S STANDARDS

In June 2012 HIQA issued a set of formal national standards for *Safer Better Patient Care*. These standards were divided up into 8 key themes that support a culture of quality and safety that places the users of Healthcare Services at the centre of focus and attention.

FIGURE 1HIQA SAFER BETTER PATIENT CARE THEMES

These themes are further divided into a set of defined standards that describe the features and outcomes of a health service that is meeting the required standards under that particular theme.

Health Identifiers for service users, Health Care Practitioners and Health Care Providers have been identified by HIQA as having potentially significant benefits in the context of the audit and management of these standards and ensuring the correct identification of all participants in a patient's care pathway.

The table on the following page provides a summary of the key themes and standards contained in the *National Standards for Safer Better Patient Care*. Themes and standards that have relevance to the development of and use of Health Identifiers are highlighted in **bold** text.

The themes and standards we have identified as having relevance to the roll out and use of health identifiers include a number of elements relating to the "supporting competencies" needed to ensure a quality and trusted implementation of these new capabilities.

Almost every thematic area and standards requirement set out by HIQA in the *National Standards for Safer Better Patient Care* is impacted in some way by the introduction of Health Identifiers. For example, issues such as the training of staff in appropriate skills for data matching, data governance, and data protection in the context of a holistic Health Identifier for individuals would need to be considered under Theme 6, and the timelines for updates will need to be reflected in processes and controls under Theme 8.

HIQA Theme	Defined Standards
1. Person-Centred Care and Support	1. The planning, design and delivery of services are informed by service users' identified needs and preferences. 2. Service users have equitable access to healthcare services based on their assessed needs. **3. Service users experience healthcare which respects their diversity and protects their rights.** 4. Service users are enabled to participate in making informed decisions about their care. 5. Service users' informed consent to care and treatment is obtained in accordance with legislation and best available evidence **6. Service users' dignity, privacy and autonomy are respected and promoted.** 7. Service providers promote a culture of kindness, consideration and respect. 8. Service users' complaints and concerns are responded to promptly, openly and effectively with clear communication and support provided throughout this process. 9. Service users are supported in maintaining and improving their own health and wellbeing.
2. Effective Care and Support	1. Healthcare reflects national and international evidence of what is known to achieve best outcomes for service users. **2. Care is planned and delivered to meet the individual service user's initial and ongoing assessed healthcare needs, while taking account of the needs of other service users.** **3. Service users receive integrated care which is coordinated effectively within and between services.** **4. An identified healthcare professional has overall responsibility and accountability for a service user's care during an episode of care.** **5. All information necessary to support the provision of effective care, including information provided by the service user, is available at the point of clinical decision making.** 6. Care is provided through a model of service designed to deliver high quality, safe and reliable healthcare. 7. Healthcare is provided in a physical environment which supports the delivery of high quality, safe, reliable care and protects the health and welfare of service users. **8. The effectiveness of healthcare is systematically monitored, evaluated and continuously improved.**

HIQA Theme	Defined Standards
3. Safe Care and Support	1. Service providers protect service users from the risk of harm associated with the design and delivery of healthcare services. 2. Service providers monitor and learn from information relevant to the provision of safe services and actively promote learning both internally and externally. **3. Service providers effectively identify, manage, respond to and report on patient-safety incidents.** 4. Service providers ensure all reasonable measures are taken to protect service users from abuse. 5. Service providers fully and openly inform and support service users as soon as possible after an adverse event affecting them has occurred, or becomes known, and continue to provide information and support as needed. 6. Service providers actively support and promote the safety of service users as part of a wider culture of quality and safety. 7. Service providers implement, evaluate and publicly report on a structured patient-safety improvement programme.
4. Better Health and Wellbeing	1. The health and wellbeing of service users are promoted, protected and improved.
5. Leadership, Governance and Management	**1. Service providers have clear accountability arrangements to achieve the delivery of high quality, safe and reliable healthcare.** **2. Service providers have formalized governance arrangements for assuring the delivery of high quality, safe and reliable healthcare.** **3. Service providers maintain a publicly available statement of purpose that accurately describes the services provided, including how and where they are provided.** 4. Service providers set clear objectives and develop a clear plan for delivering high quality, safe and reliable healthcare services. **5. Service providers have effective management arrangements to support and promote the delivery of high quality, safe and reliable healthcare services.** 6. Leaders at all levels promote and strengthen a culture of quality and safety throughout the service. 7. Members of the workforce at all levels are enabled to exercise their personal and professional responsibility for the quality and safety of services provided. 8. Service providers have systematic monitoring arrangements for identifying and acting on opportunities to continually improve the quality, safety and reliability of healthcare services. 9. The quality and safety of services provided on behalf of healthcare service providers are monitored through formalised agreements.

HIQA Theme	Defined Standards
	10. The conduct and provision of healthcare services are compliant with relevant Irish and European legislation. 11. Service providers act on standards and alerts, and take into account recommendations and guidance, as formally issued by relevant regulatory bodies as they apply to their service. Service providers act on standards and alerts, and take into account recommendations and guidance, as formally issued by relevant regulatory bodies as they apply to their service.
6. Workforce	1. Service providers plan, organise and manage their workforce to achieve the service objectives for high quality, safe and reliable healthcare. **2. Service providers recruit people with the required competencies to provide high quality, safe and reliable healthcare.** **3. Service providers ensure their workforce have the competencies required to deliver high quality, safe and reliable healthcare.** **4. Service providers support their workforce in delivering high quality, safe and reliable healthcare.**
7. Use of Resources	1. Service providers plan and manage the use of resources to deliver high quality, safe and reliable healthcare efficiently and sustainably. **2. Service providers have arrangements in place to achieve best possible quality and safety outcomes for service users for the money and resources used.**
8. Use of Information	1. Service providers use information as a resource in planning, delivering, managing and improving the quality, safety and reliability of healthcare. **2. Service providers have effective arrangements in place for information governance** **3. Service providers have effective arrangements for the management of healthcare records.**

HIQA'S PUBLISHED STANDARDS FOR INFORMATION GOVERNANCE & MANAGEMENT STANDARDS FOR HEALTH IDENTIFIERS

In the context of the wider standards for *Safer Better Patient Care* HIQA has engaged in an extensive consultation on specific standards for Information Governance and Management for Health Identifiers.

HIQA published their final standards 5 August 2015. These standards provide some useful guidance as to the priorities they see in terms of implementing standards in this area. Overall, HIQA sets out a clear statement that the Health Identifiers Operator will need to demonstrate evidence of the effectiveness of operation of controls and of compliance with the standards. They will also have to enter into formalized data sharing agreements with "trusted source owners" and health service providers that will govern the use, sharing, and governance of the Registers and their data in line with standards and relevant legislation. In reviewing these standards Castlebridge Associates note a few missed opportunities and areas of concern. We will discuss some of these these areas in comparison to the Draft Standards published as part of the consultation process.

HIQA have selected four key thematic areas to focus on in the development of their Standards. These confirm the high level mapping undertaken earlier in this paper.

- Person Centred Support
- Leadership, Governance, and Management
- Use of Information,
- Workforce

In short: HIQA expect a documented system of internal governance over health identifier data and associated identifying particulars that encompasses all data providers and data consumers, including the Data Protection Commissioner. However, the standards may not adequately support as rigorous a framework of governance and accountability as it might have.

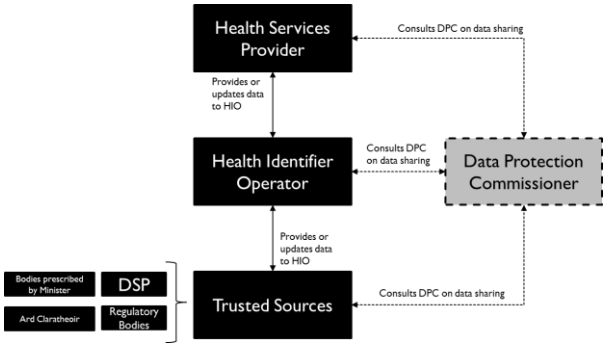


FIGURE 2: MAP OF KEY ACTORS IN HEALTH IDENTIFIERS (BASED ON HIQA STANDARDS)

This diagram illustrates the general structure for Data Protection governance envisaged by HIQA's draft standards. It shows a clear consultative role for the Data Protection Commissioner, but equally a critical accountability on the part of Health Service Providers, the Health Identifier Operator, as well as the "trusted sources" who would contribute data to the development of the Registers.

As Data Sharing will be a key component, we direct readers to our submission on the Data Sharing and Governance bill for further discussion of that topic.

KEY THEMES AND STANDARDS IN CONTEXT OF HEALTH IDENTIFIERS

HIQA's standards contain a number of specific recommendations broken out by the various themes of *Better Safer Patient Care.* Under each Theme they have created a specific set of standards that apply in the context of Health Identifiers.

PERSON CENTERED SUPPORT

HIQA stress the importance of the development of a relationship based on trust when communicating with stakeholders such as patients, health service practitioners etc. It is interesting that *communication* is stressed to such an extent as a requirement in the operation of Health Identifiers given the range of high profile failures to do so in other high profile public sector projects.

Protection of privacy and autonomy are also stressed as key themes.

In terms of specific standards:

1. **Privacy Impact Assessments are required at critical points during the establishment and operation of the various Registers**.

   This is in keeping with best practice that PIAs are not "once off" activities. It is significant that PIAs are identified as a key standard practice under "person centered support" rather than a more technical or IT focused theme.

   The key requirements here are for "arrangements to be in place" to conduct Privacy Impact Assessments prior to the establishment of the Registers and "*when significant system changes are planned to identify any new or potential privacy risks that may arise as a consequence of the proposed system change.*"

   This is a critical Information/Data Governance function as the assessments will need to feed "lessons learned" into the next phases of implementation.

   The emphasis on Privacy Impact Assessments in the standards is welcome. However, Castlebridge Associates notes a missed opportunity to ensure Privacy Impact Assessments are conducted in line with international standards. HIQA's finalized Standards revised a specification that for Privacy Impact Assessments to be conducted "*when significant system changes are planned to identify any new or potential privacy risks that may arise as a consequence of the proposed system change.*" In contrast, the Draft Standards called for PIAs "at appropriate intervals to identify any new or potential privacy risks that may arise during the operation of the national registers.

   The wording in the earlier draft was closer to being in line with the standards of BS10012:2009, which mandates ongoing monitoring and control of processes, instituting regular checks over compliance at appropriate intervals to ensure ongoing maintenance of standards, plus special checks when changes are proposed.

An effective approach to privacy requires a mindset and way of operations that builds privacy into the design of processes and operations and ensures a mindset of constant vigilance in maintaining compliance, rather than a tick-box approach.

The *Bara* ruling highlights a practical benefit to conducting Privacy Impact Assessments 'early and often' in that any requirement to communicate with data subjects or to update existing communication can be identified, and appropriate measures can be put in place to ensure that any data sharing or other processing is in compliance with fundamental rights, including the data privacy and preservation of dignity. It also provides a timely opportunity to risk-assess the reliance on statutory provisions versus other lawful processing conditions with a view to ensuring trusted and trustworthy data processing

2. **The Health Identifiers Operator develops, implements, and reviews a communications plan that effectively informs service users in relation to the use of national registers.**

This is a laudable standard, and is indicative of some key learnings from other initiatives being applied to the development of these Registers. This standard includes in it a requirement for continuous improvement and regular reviews of statements of information practice (fair processing notices) as well as reviewing the actual effectiveness of communication (is the message being understood, is it being communicated appropriately).

The outcomes of the feedback process in determining these standards for communication, however, reveal what may be a breakdown in the understanding of what communication is. In response to feedback on the Draft Standards during the consultation phase of developing the Standards[7], HIQA added a feature of the standard with specific reference to two-way communication:

> 1.2.3 Mechanisms are in place that allow for two-way communication between the health identifiers operator and health service providers and service users. This allows health service providers and service users submit complaints, queries and comments to the health identifiers operator.

This is, in itself, a strong feature, but it must be emphasized that two-way communication should be part of all features of this standard, as otherwise it fails to be effective communication.

HIQA has emphasized that clear communication was one of the key learnings from international review of health identifier implementations. Communication with key stakeholders including the public will be essential to a smooth rollout of health identifiers in Ireland.

[7] Statement of outcomes – Report on the outcome of the public consultation on Draft Information Governance and Management Standards for the Health Identifiers Operator in Ireland.

Bara highlights the importance of communication of purposes for processing. It is essential that this HIQA standard is fully embraced in the implementation of the Health identifiers system. Communication with stakeholders will require effective Information Governance structures to be in place to ensure that the correct information is communicated to external stakeholders and that the input received from stakeholders is relayed back for appropriate action.

LEADERSHIP, GOVERNMENT & MANAGEMENT
HIQA's standards state that:

> *"... the health identifiers operator is obliged to protect service users' personal data. This is an aim that is achievable when effective governance arrangements are in place, reviewed regularly and updated if necessary"*

The standard identifies the Health Identifiers Operator as being the Data Controller for Health Identifiers and associated identifying particulars.

In terms of specific standard requirements, HIQA defines the following:

1. **The health identifiers operator has effective leadership, governance and management arrangements in place with clear lines of accountability.**

HIQA recommends that having an identified individual with overall accountability for the service delivery by the Health Identifiers Operator is a good practice, and that clear reporting lines are in place with cascaded accountability and responsibility and an appropriate focus on ensuring the monitoring and performance development of their own staff.

This role would also be responsible for establishing effective information governance arrangements to protect the health records of services users and service providers.

Systems for ensuring the quality assurance of the health identifiers would also fall under this organizational role, as well as Risk Management.

HIQA suggests the establishment of an oversight committee "to advise the health identifiers operator on the operation and management of the national registers" as one of the features of this standard. This suggestion highlights the underlying need for a mechanism to align oversight (strategic) with line management and operations.

2. **The health identifiers operator maintains a publicly available statement of purpose**

This requires that the Health Identifiers Operator establish, publish, and keep under review what amounts to a Fair Processing Notice in Data Protection terms. While welcome as a specific standard, it must be pointed out that this is already an enforceable legal obligation underpinned by rights under EU Treaties.

Furthermore, the recent media comment on Health Identifiers has addressed only one category of purposes for one category of individual who will be identified by a Health Identifier. This would need to be clearly and transparently addressed.

The *Bara* case extends this obligation further as, in the context of data sharing, it requires that there be a statement from the source entity that sharing will take place, the categories of entity that data will be shared with, and why. It also requires that the receiving entity provide to the Data Subject a clear statement of what their purpose is for the data.

3. The health identifiers operator complies with relevant Irish and European legislation and standards when establishing and managing the national registers

In short, it is a standard requirement to comply with relevant legislation and standards. This will require regular reviews of legislation and maintaining a Risk Register of any identified gaps in compliance, with an appropriate Risk Treatment being implemented

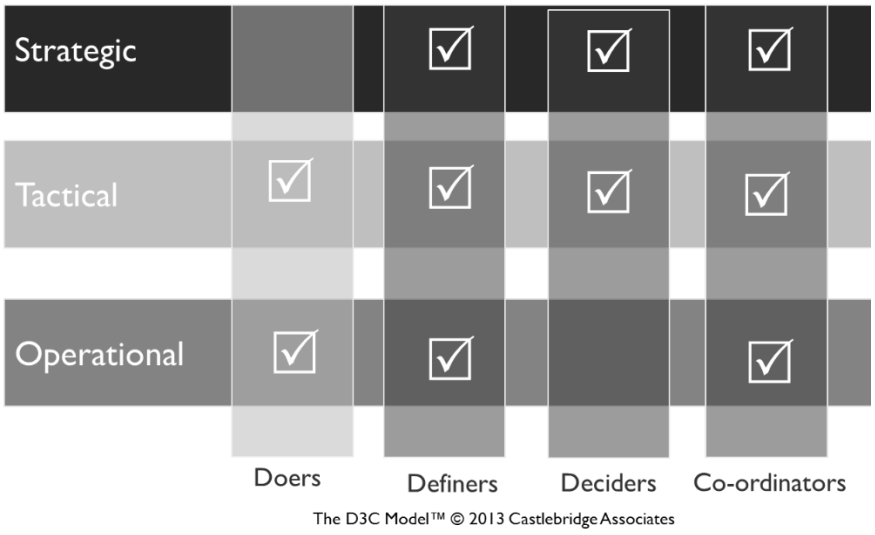
Documented evidence of compliance and effective governance is required, along with an effective governance arrangement to allow audit findings to be reported, acted upon, and monitored.

There is, however, a lack of clarity about Information Governance roles with a risk of role conflation in this standard. Standard 2.3.1 specifies the appointment of "an identified individual" whose role includes:

- Conducting regular reviews of Irish and European legislation and published standards to determine what is relevant to the establishment and operation of the national registers
- Documenting risk assessment of any identified gap in compliance with legislation and taking appropriate, timely action to achieve compliance to ensure the quality and safety of the functions of the health identifiers operator.

The position of the appointed individual in relation to the role of a Data Protection Officer (specified in standard 3.1.1) is left in question here. Would this individual be filling the role of Data Protection Officer as well or would there be segregation of duties?

Clear definitions and understanding of roles and responsibilities and their relationships are required to build a functioning governance framework with clear lines of accountability. Castlebridge Associates' 3DC Information Stewardship model is one method by which we determine where identified roles fit in an information governance strategy.



In this context, we would ask about this appointed role: Is this Appointed Individual a Doer, Decider, Definer, or Coordinator? Is this a strategic or tactical role?

What relationship does this identified individual have to data and to other roles such as that of the Data Protection Officer?

FIGURE 3: THE 3DC MODEL

Would this "Appointed Individual" be a steward of the Data Privacy requirements, with the Data Protection Officer performing a wider Data Governance role in ensuring that those requirements were implemented consistently in practice? Is it envisaged that the Appointed Individual and the Data Protection Officer will be the same person?

4. **The health identifiers operator has formalised arrangements with health service providers for the effective use of the national registers in line with relevant legislation and standards**

This extends the role of the Health Services Operator to encompass the implementation of appropriate governance controls and frameworks with Health Service providers.

HIQA suggests this framework would be based on a "self-certification" of compliance with relevant standards, however a stronger "evidence based" approach would be more in keeping with lessons learned in other sectors (telco, financial services etc.)

This is particularly true given that HIQA presumes a monitoring and evaluation role for the Health Identifiers Operator. This will require some level of objective data on compliance. Castlebridge Associates would strongly advise that standards certification and compliance must be evidence-based to be effective and recommendations against a self-certification model.

HIQA also identify the use of service level agreements between various parties to formalize governance structures. Training and education for health service providers and their staff as to how Identifiers are to be accessed and used is suggested. However, the "information leaflet" suggested in the Standards document is, in our experience, insufficient investment in training to embed a strong culture and work practice change. This reflects the questions about communication raised in the first theme, and raises questions about standards for effectiveness of training in later standards.

We will further discuss evaluation of training and education in context of the "Workforce" theme. In general, however, this highlights the need to understand the vital importance of effective communication (which *must* be two-way) and training, which *must* go beyond superficial broadcast and ensure not just transferal of knowledge at some level but behavioral change.

These are essential to information governance. Again, we highlight the fact that Health Identifiers are simply data, and that the proper governance and use of such data relies on effectively trained people who understand their roles in relation to the data, know what can be done to which data and under what circumstances, and who can be held accountable for their actions. We would raise concerns regarding the compatibility of a programme of self-certification and the need for accountability to standards when it comes to sensitive personal data such as health information.

5. **The health identifiers operator has data exchange agreements with trusted sources that protect personal information and define which data can be shared for the purpose of establishing and maintaining the national registers.**

This recommended Standard reflects the actual requirements of the Health Identifiers Act. However, it is of importance to note the emphasis on privacy, data quality, and appropriate governance arrangements in the supporting narrative.

This is indicative of the kind of information that is likely to be required to be shared and communicated to Data Subjects to ensure compliance with the ruling in *Bara*.

6. **The health identifier operator monitors, reviews, evaluates and improves the service it provides on an ongoing basis.**

This proposed standard sets out a requirement for an Information Quality Management function within the Health Identifiers Operator to ensure that there is a continuous monitoring and improvement of the quality of the Register that is takes evidence-based decisions. It also requires that there be feedback mechanisms to get input from stakeholders.

This implicitly requires a level of data quality scorecarding, appropriate mechanisms for the reporting of and tracking of data quality issues, and a generally strong culture of information quality around the Registers.

It would appear that tracking and monitoring for privacy impacts or privacy breaches would also form part of the quality focus of this role.

USE OF INFORMATION

Under the theme of *Use of Information* HIQA considers a number of topics such as Information Quality, Information Governance, and Data Protection.

1. **The health identifiers operator maintains and reviews the privacy of health identifier records contained in the national registers.**

This standard requires that there be standardized procedures developed for the collection, storage, sharing, use, and protection of Health Identifiers in both paper and electronic forms.

It is also required that there be processes in place to allow a Health Service user and Health Service provider to request modification to their Health Identifier Record. Finally, it is necessary to ensure that Health Identifiers are not reused.

We note that HIQA confines that last element to just individual Health Identifiers of Service Users, but we would suggest that not mapping that to Healthcare Practitioners and staff/employee/agents would diminish the benefits of a unique identifier in those contexts.

This standard also suggests that the nomination of a Data Protection Officer would be a feature likely to meet the standard:

> "3.1.1 A nominated Data Protection Officer is appointed whose role includes maintaining, improving, and auditing systems and processes used to protect all data processed by the health identifiers operator."

This is not currently a mandatory requirement, although a Data Protection Officer is likely to be required by the upcoming EU Data Protection Regulation. However, as it stands currently the role of the Data Protection Officer here would not have legal basis or authority.

Castlebridge Associates applaud the forward thinking in considering the need for a Data Protection Officer here. However, as currently proposed, this is an optional toothless role with no statutory basis in either the Health Identifiers Act or the Data Protection Acts. The Government could show strong leadership in Data Protection by supporting the forward looking drive of HIQA's standards with an amendment to the current Data Protection Acts to put into place the Data Protection Officer role that has been envisaged under the Draft General Data Protection Regulation. This would serve to clarify the Governance mandate and authority of the Data Protection Officer function with respect to Health Identifiers.

In this context, we would direct readers to our submission, in conjunction with Digital Rights Ireland, to the Department of Public Expenditure and Reform[8] on the proposed

[8] https://castlebridge.ie/products/whitepapers/2014/09/data-governance-and-sharing-bill-consultation-submission, March 2014.

Data Governance and Sharing Bill and our recommendations therein for a professionalization of the "Data Protection Officer" role within the Public Service.

2. The health identifiers operator maintains and reviews the quality of data contained in the national registers.

This standard will require the Health Identifiers Operator to implement a Quality Management framework for the Registers, including ensuring that there are mechanisms in place to support verification of data and to validate change requests to data and that there are appropriate formal arrangements for data quality audits and improvement.

There is a strong emphasis on the consistent application of policies and procedures for access to or alteration of Health Identifier information, with an explicit requirement for compliance audits.

Business Continuity is included under this heading as well.

However, as information quality is determined ultimately by the "fitness for purpose" for a defined objective, it is essential that the Information Governance frameworks to support the Health Identifiers system are capable of adapting to:

- New purposes
- New types of data within the Health Identifier
- New technologies

This would suggest that the adoption of a standard such as the BS10012:2009 for Personal Information Management as the basis for Governance of Health Identifiers would be a positive first step.

WORKFORCE

HIQA's Workforce standards put a strong emphasis on the necessity of effective, evidence-based training and its vital role in maintaining compliance with the Data Protection Acts and upholding individuals' fundamental rights in the implementation and operation of health identifiers. The standards state that:

> "Having an appropriately skilled and trained workforce in place to establish and manage the national registers is essential for the health identifiers operator to achieve its objectives"

1. **The health identifiers operator delivers regular evidence-based training programmes to its own workforce in relation to establishing, maintaining and using the national registers.**

This standard calls for, amongst other things:

- Mandatory training covering data privacy and confidentiality
- Evidence based training that focuses on the legislation, principles of privacy and confidentiality, processes and procedures, and information sharing agreements.

The standard also calls for a formal training schedule, tailored to learner needs, to develop critical core competencies and skills.

Interestingly, the standard also calls for the effectiveness of training materials, training programmes, and translation of learning to actual work practices to be evidenced and evaluated. Effective training involves the imparting of knowledge. Knowledge is similar to Data and Information in that it is an intangible asset. It can appear difficult to measure the value of a set of concepts or the formal development of a proficiency in skills. However, there are models by which we can evaluate the effectiveness of training. Donald Kirkpatrick's four level model of evaluating learning measures effectiveness at the following levels:

1. **Reaction**: Level 1 of this model is the basic "customer satisfaction survey" type of evaluation that should be conducted for all training programmes. The logic is that effective learning will not have taken place if the learners were not satisfied with the trainer/training or environment.
2. **Learning**: Level 2 of the model is the standard "proficiency test" that should be part of any training programme. It measures the effectiveness of how well the desired knowledge has been transferred.
3. **Behaviour**: Level 3 looks at the behavioural changes that have come about as a result of the training. This level of evaluation looks at how the learners are putting the principles in to practice and are applying the information that was imparted in the training. For Data Protection training to be of any use, it must be reflected in behavioural changes.
4. **Results**: Level 4 measures whether the training is achieving results. Here we look at the KPIs that should be affected by changes in behaviour

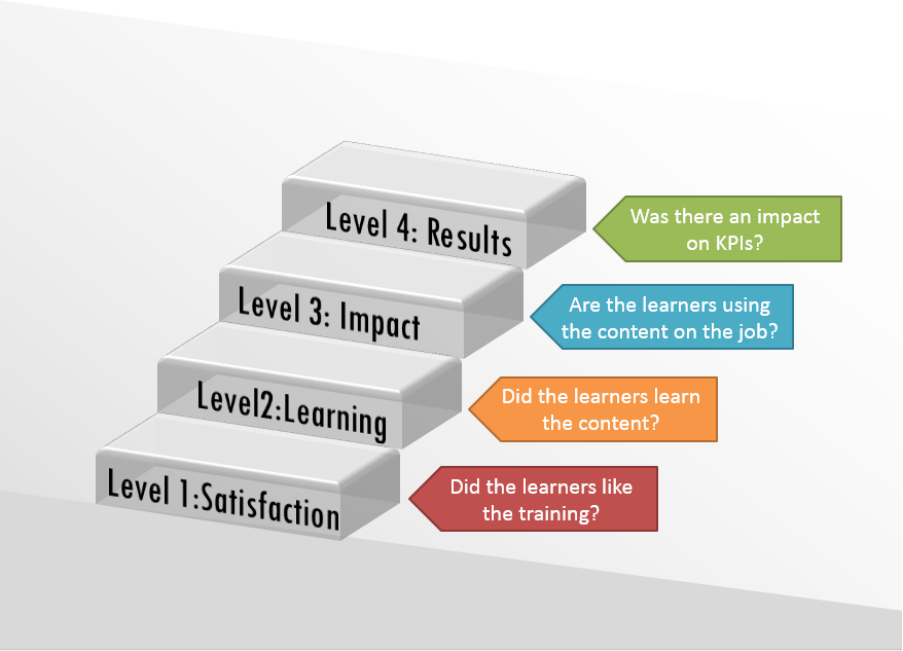


FIGURE 3 KIRKPATRICK MODEL OF TRAINING EVALUATION

Each successive level builds upon the previous level. "Tick the Box" training will not suffice if Data Protection training is to be reflected in work practices. To have a clear concept of what is to be considered effective training and the ability to evaluate effectiveness it is important to have a baseline of KPI performance before engaging in training. What is it that people should be able to do, and what do they need to know to be able to do that?

We believe that the HIQA's strong emphasis on the need for effective training reveals a greater need for clear standards for effective Data Protection training, going beyond teaching the 8 Rules of Data Protection to ensuring a practical, principles-based outcomes-focused approach that results in tangible changes in the way people think about privacy implications and treat data in their organization.

In the context of the HIQA standards, the Health Identifiers operator and all stakeholders in the Health service need to consider if traditional training or training providers will continue to be fit for purpose.

The training offered by Castlebridge Associates[9], which uniquely addresses Data Protection obligations through the perspective of Information Governance and Information Quality practices, represents an example of the type of training that will required. Other courses that also go beyond the basics include the Law Society of Ireland's *Certificate in Data Protection Practice* (which Daragh O Brien, our Managing Director helped develop).

[9] See Castlebridge Associates Training Catalogue: https://castlebridge.ie/resources/training-course-catalogue

A MISSING THEME:

HIQA's Draft Standards included a fifth theme, "Use of Resources". This theme has been removed from their finalized Standards document.

This section of HIQA's Draft Standards addressed the need to ensure that the Registers are sustained and maintained as a relevant asset. Resources is defined as including people, money, and natural resources. Resource allocations are linked to data quality explicitly. The theme and standard in HIQA's Draft Standard stated the following:

> ***Theme 4 Use of resources:***
>
> *The health identifiers operator is required to plan and effectively manage its resources in line with the objectives of the creation and ongoing existence of the national registers. It must make sure that its resources are adequate to ensure the sustainability, continuous relevance and maximum impact of the national registers. Resources include human, physical, financial and natural resources. Since resources are finite, and budgets limited, the health identifiers operator is required to carefully manage its resources to ensure that they are used in the most efficient, useful and effective manner. The allocation of resources is a fundamental factor in the delivery of quality data as the deployment of resources significantly impacts on the quality of information provided and the future sustainability of the national registers.*
>
> *Standard 4.1*
>
> *The health identifiers operator plans and manages the allocation and uses of resources assigned to it to meet the objectives of the national registers.*
>
> *Features meeting this standard are likely to include the following:*
>
> *4.1.1 Clear plans that take account of the funding and resources required for the viability of the health identifiers operator.*
>
> *4.1.2 Consultation with key stakeholders including service users, policy makers and their own workforce regarding the allocation of resources to achieve the best quality and safety outcomes for service users.*
>
> *4.1.3 Transparent and effective decision-making arrangements when planning, procuring and managing the use of resources for the effective establishment and operation of the National Registers.*
>
> *4.1.4 Resource decisions are informed by:*
>
> - *explicit consideration of the quality, safety and ethical implications of such decisions*
> - *risk assessment of the decisions*

- *best available evidence*
- *service users and health service providers' views.*

4.1.5 Transparent reporting on financial performance in line with relevant legislation and national policy.

This deleted standard called for consultation on resource allocations and planning. It also required that decision making be transparent and effective. In essence, it set out some of the core rules about "how to decide to decide" in the context of Health Identifiers, with quality, safety, ethics, and risk assessment being key considerations. Some of these features have been woven into the Theme 2: Leadership, Management, and Governance[10]. However, while Leadership, Management and Governance have a key relation to proper Use of Resources, the clarifications made in Use of Resources as a separate theme for standards were valuable.

It is notable that references to consulting key stakeholders have been removed from HIQA's final Standards document. While "Communication" is still recognized as an important inter-related theme, it is unfortunate that this key lesson learned is now implicit in the Communications standard rather than explicitly laid out and linked to accountability.
Considering that failures recent large-scale data integration projects such as the Department of Education's Primary Online Database can be attributed to, among other things, failure to adequately engage with key stakeholders, this is somewhat alarming. The removal of focus on explicit consideration of best available evidence, risk assessment, quality, safety, sustainability, and ethical implications of decisions are also concerning.

Decision making must be evidence based and take the views of stakeholders such as service users and health service providers into account. This removal may send an unintended message about the priorities and expectations of the Authority regarding sustainability, accountability, and lessons learned from best evidence and previous initiatives.

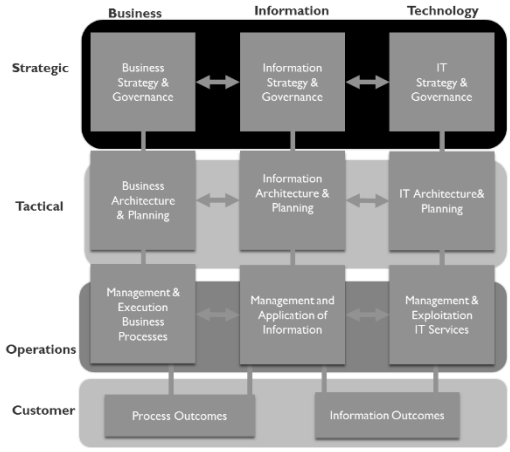


FIGURE 4: REFLECTING OUTCOMES

The removal of this theme weakens the emphasis within the HIQA standards on the need to ensure alignment of and investment in the three pillars of Business capabilities, Information Strategy, and Technology infrastructure necessary to consistently deliver the Information and Process outcomes sought by stakeholders in the Health care system.

[10] Standard 2.1.9: Resources allocated to the health identifiers operator are planned and managed so that the objectives of the national registers are met.

SUMMARY OF HIQA'S STANDARDS

Notwithstanding that they must be read in the broader context of *Better Safer Patient Care* standards and that they are written primarily for the benefit of a Health Identifiers Operator, the HIQA standards reflect a generally strong set of Information Governance and Information Quality principles.

The summary messages to be taken from the standards set out thus far are:

1. Quality of Information drives quality of service user or healthcare practitioner outcome. Therefore, a strong focus on information quality planning, control, and improvement is evident.
2. The service user and health care provider/practitioner must be kept front and centre in the planning and execution of the Registers. Communication is key, and the explicit recognition of the importance of *effective* communication to ensure trust is noteworthy.
3. Effective governance structures will need to be implemented internally, but also across organizational boundaries, to ensure that the day to day processes of using and maintaining Health Identifiers operate correctly and deliver the expected outcomes.
4. Training and skills development is a key component of developing that Governance structure. Training is not a once-off induction exercise, and specific training will be required related to the skills and experience of staff. All training must be evaluated for effectiveness.
5. Privacy of data is a key quality characteristic. Privacy Impact Assessments will need to be ongoing activities not just once off tasks. Governance structures must operate to support the Privacy requirement.
6. Everything should be evidence based, with clear auditability of controls

OTHER RELEVANT STANDARDS AND GUIDELINES

While the HIQA standards relate to the operation of the Health Identifiers Registers, it is important to remember that existing standards and regulations will equally apply to the use of Health Identifiers in the course of delivering treatment.

This is implicit in HIQA's declaration that the use of Health Identifiers will reduce cost and provide clear accountability at each stage of a service-user's care pathway.

As alluded to earlier in our discussion of the legal background and issues, the requirement under Section 11 and Section 20 of the Health Identifiers Act 2014 that health identifiers for service users and healthcare practitioners and providers be associated with an "relevant communication" echoes the statement in the HSE's Guidelines on Information Management Patient Records which requires any communication relating to patient care to form part of the Patient Care Record.

Therefore, there is a need for Healthcare Providers to ensure that they are recording Health Identifiers in communications and ensuring that those communications are linked to the Patient Care Record.

This has significant implications given the widespread, but uncontrolled, use of messaging applications for medical staff to communicate instructions or updates about patient care in a clinical environment or in the case of a consultation. Quite apart from the Data Protection implications of such communication, and the implications should a treatment error occur, it would appear that using such technologies now may constitute a breach of the Health Identifiers Act 2014 if there is a "relevant communication".

ASSESSING IMPACT OF BARA AND SCHREMS CASES

October 2015 saw two significant European Court of Justice rulings which have direct impacts on the implementation of Health Identifiers and other public sector data sharing projects. We have indicated some of the impacts in earlier sections. In this section we provide a more in-depth analysis of each case.

SCHREMS CASE

The *Schrems*[11] case relates to the appeal by Maximillian Schrems against the decision of the Irish Data Protection Commissioner not to suspend data transfers by Facebook to the United States under the Safe Harbor scheme.

While the headline of the case is that it resulted in the suspension of the Safe Harbor mechanism for cross border data transfers, the ruling of the European Court of Justice clarified a number of other key points of EU Data Protection law:

INDEPENDENCE OF THE REGULATORY AUTHORITY

In *Schrems*, the CJEU ruled that national Data Protection Authorities must be able to conduct investigations with "complete independence" relating to any claim filed by an individual "concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him", and that such investigations must be undertaken unless it is clear that the arguments put forward by the complaint are unfounded. In such cases the complainant has a right to appeal via the national courts and upwards to the CJEU as required.

While the questions presented in the case related to the ability of a national Data Protection Authority to overrule the decisions of the EU Commission, the principle of Regulatory independence is very clearly stated in this case. Even where the issue complained of relates to an EU Commission decision, the court says, the national DPA *must* investigate and *must* act to vindicate the rights of the individual. While decisions of the EU Commission require the CJEU to adjudicate in the final analysis, there is still a duty on the DPC to act.

In the context of domestic legislation and the relationship between the DPC and government departments or other public or private sector bodies, *Schrems* makes it clear that a national Data Protection Authority must investigate and reach a determination. As such, the various provisions in the Health Identifiers Act where the DPC is required to submit a report on privacy impacting issues to the Minister who may then choose the appropriate actions to take would appear to be incompatible with EU law and, if applied as set out in the legislation, could raise significant questions as to the practical independence of the Irish Data Protection Commissioner.

In light of *Schrems*, and the growing canon of case law from the CJEU in relation to the independence of the Office of the Commissioner under EU Law, Castlebridge

[11] *Maximillian Schrems v Data Protection Commissioner,* Case C-362/14, http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=

Associates would suggest that a robust Information Governance framework that adopts a Privacy by Design approach, engages in early and effective Privacy Impact Assessments that engages with the DPC as a stakeholder to prevent infringements on fundamental rights rather than an investigating regulator, as well as engaging the perspective of data subjects in key decisions, should be a target operating model.

BARA CASE

In the *Bara*[12] case, the action concerned the transfer of personal data between the Romanian taxation authorities and their National Health Insurance Fund on foot of a statutory provision. Self-employed persons whose data was transferred under this mechanism objected on the grounds that the processing took place without prior explicit consent and without their having been informed of the processing.

The Court of Justice ruled that "the requirement of fair processing of personal data requires a public administrative body to inform the data subjects of the fact that their data will be transferred to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data. The directive expressly requires that any restrictions on the requirement to provide information are imposed by legislative measures"[13]. The scope of those restrictions are set out in Article 13 of the Directive 95/46/EC.

The Court also ruled that: "*In accordance with the provisions of Chapter II of Directive 95/46, entitled 'General rules on the lawfulness of the processing of personal data', subject to the exceptions permitted under Article 13 of that directive, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive*"[14], and that Public Bodies, as Data Controllers, are required to provide information in accordance with Article 10 and Article 11 of the Directive in relation to the nature, purpose, and scope of processing.

The Court examined the specific provision of Romanian law which provided for a general and broad provision of information deemed necessary by the receiving agency for its purposes without providing any detailed specification of what that data would be. On that basis, the Court held that the legislative provision did not meet the requirement of Article 10 of the Directive. The CJEU specifically commented that:

> *"it must be observed that Article 315 of Law No 95/2006 merely envisages the principle of the transfer of personal data relating to income held by authorities, public institutions and other institutions. It is also apparent from the order for reference that*

[12] *Smaranda Bara and Others* Case C-201/14 http://curia.europa.eu/juris/document/document.jsf?text=&docid=168943&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=19870

[13] Summary Press release of Bara ruling: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf

[14] *Bara* case at paragraph 30

the definition of transferable information and the detailed arrangements for transferring that information were laid down not in a legislative measure but in the 2007 Protocol agreed between the ANAF (tax authority) and the CNAS (Health Insurance Fund Agency), which was not the subject of an official publication"

The Court applied similar reasoning when considering the application of Article 11 of the Directive, with an identical result.

The Court considered the potential application of Article 11(2) of the Directive which allows for a limited derogation from fair processing notices where data is not obtained from the data subject directly. This provision relates to the processing of data for statistical purposes or for historic or scientific research. The Court ruled that this was not applicable in this case.

From *Bara* it is clear that the sharing of data between Public Sector bodies will require the formal governance of and publication and communication of the purposes for sharing data, the scope of processing when data is shared, and the identity of entities data is shared with and acquired from. This will require strong attention to data lineage, change control, privacy impact assessments, and a clear formal publication methodology. It is clear from *Bara* that the 'traditional' approach of using defined data exchange protocols is insufficient.

The provisions of Section 31 of the Act become more significant now in light of *Bara*, particularly as it is clear that this formal specification of data sharing will be required *before* any sharing takes place and will need to be communicated clearly and in an intelligible form to Data Subjects. An 'official publication' mechanism will be required also. This echoes some of the concepts from the Data Sharing and Governance Bill which will be explored in our review of the Heads of that Bill.

A STRATEGIC DATA GOVERNANCE APPROACH

A piecemeal siloed approach to the implementation of Health Identifiers and associated technologies will result in sub-optimal outcomes for all stakeholders, and may lead to key dependencies being missed or key requirements under *Safer Better Patient Care* being sub-optimally delivered.

A key lesson from other industries that have implemented "Single View of…" initiatives is that the technology investment is often confused with the execution of a strategy. Getting it wrong in the consumer packaged goods industry might cost the organization money. Getting it wrong in healthcare could potentially cost lives.

It is important that the execution strategy learns the lessons of other sectors!

PATIENT OUTCOME FOCUSSED

It is essential that organizations in the Health Care sector develop a clear focus on patient outcomes in their technology implementation strategies. This extends beyond the implementation of Health Identifiers or Electronic Healthcare Records, and should include the adoption of any new technologies for safer better patient care.

Castlebridge Associates propose a simple 11-box model through which organizations can develop a holistic perspective on the development and execution of effective Business, Technology, and Information strategies that are aligned with supporting clearly defined Process and Information Outcomes for the providers of healthcare services and the recipients of those services.

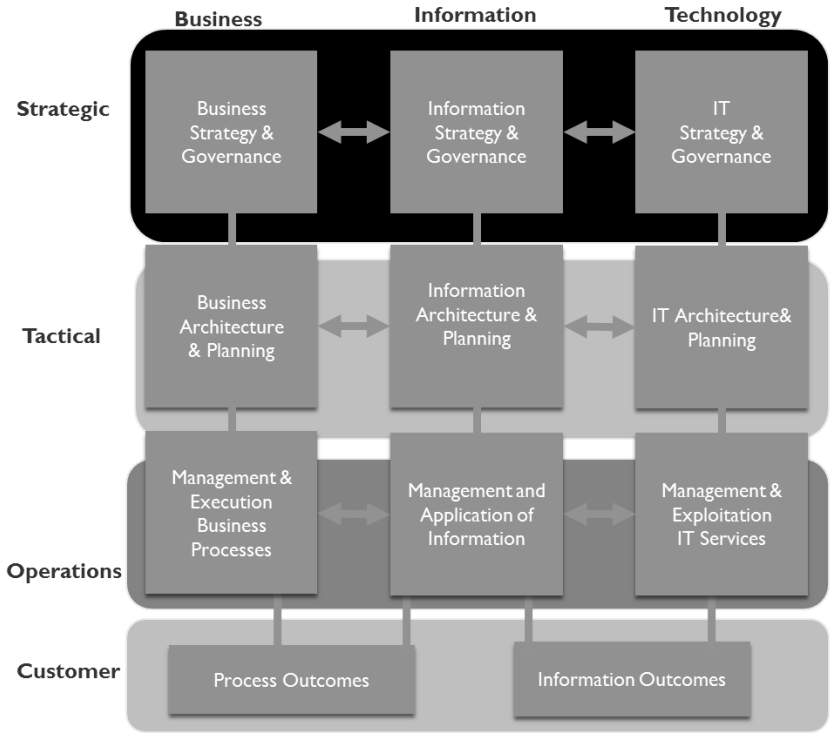


FIGURE 5 THE 11-BOX MODEL (BASED ON 9-BOX AMSTERDAM MODEL BY MAES ET AL)

In this context, Health Identifiers for both Individuals and Health Service Providers form only part of the strategic map. The effective use of these master data registers will require a clear and well-articulated Information Strategy with associated Governance structures that ensure alignment of Business functions and Technology deployment.

While the Health Identifiers Act 2014 sets out specific operational and tactical governance requirements, and the national standards for Safer Better Patient Care provides an important strategic perspective, the challenge of translating that into a coherent change vision in the Health sector that puts the patient at the centre will require practical and pragmatic investment in Information Governance competencies and Information Quality Management skills. This goes far beyond investment in Technology and must encompass the Business and Information verticals in the 11 box model to ensure that desired process and information outcomes can be consistently achieved for all stakeholders.

THE ROLE OF INFORMATION STEWARDSHIP & COMMUNICATION

A key success factor that has been identified in Master Data Management initiatives in other sectors is the importance of Information Stewardship and the need to focus on communication of the value drivers for executing the strategy. This can only be achieved through coherent and systemic Information Governance strategy that ensures that there is:

- Clarity of definitions and meaning of data (*e.g. what is "sex" in the context of the Health record? How should gender identity questions be dealt with consistently?*)
- Clarity of decision rights and responsibilities for information related processes (*e.g. who should be responsible or accountable for updating errors in Individual Health Identity details such as incorrect matches or missing values?*)
- Agreed upon models for decision making (*e.g. how can decisions on standards or deviation from standards, or the introduction of secondary purposes for data be consistently applied across all stakeholder communities?)*

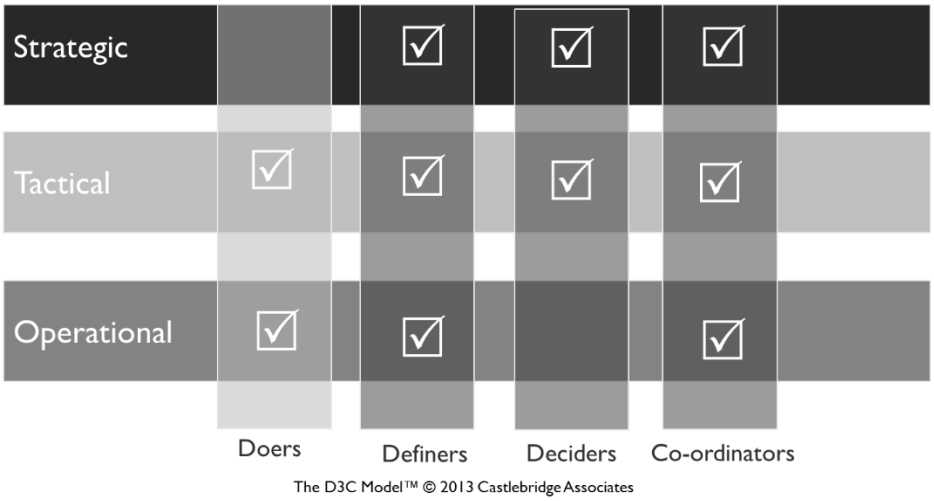


FIGURE 6 THE D3C INFORMATION STEWARDSHIP MODEL

Effective introduction of Health Identifiers in a way that supports and aligns with the standards of Safer Better Patient Care will require a clear focus on Governance of information that includes active participation from the front-line staff (Doers, Definers) and middle and upper management (Definers and Deciders) with a clear emphasis on developing staff across all levels to effectively communicate, clarify, and align Business, Information, and Technology disciplines at all levels (Co-ordinators).

This Information Governance framework will need to address both "macro-level" data governance issues relating to the purpose and use of Health Identifiers, and the development and application of relevant standards for data formats and reference data sets (such as gender codes) across a range of organisations to ensure consistency and compatibility of data.

This "macro-level" governance will also need ensure that appropriate standards are in place to govern sharing of data with third parties, including health services in other EU Member States, and the uses that that data can be put to once transferred (i.e. ensuring purpose limitation to the primary purpose and having controls over use for secondary purposes such as research).

The "macro-level" governance will also need to address the need to ensure the overall statutory basis for data gathering and processing is kept under review and that a clear statutory basis in in place at all times for any data that is being captured by any Health Service Provider to provide to a Register. In the recent findings against the Department of Education with regard to the operation of the Primary On-Line Database, the Office of the Data Protection Commissioner was clear that the processing of data that had been obtained for one purpose in a school for a new secondary purpose required a clear statutory basis to be in place ***before*** that processing commenced[15].

The POD case study is particularly relevant for the development of Health Identifiers Registers given that a centralized body (the Department of Education) was asking organisations that were data controllers in their own right (schools) to request and process new data for a new purpose and to process data already held by the Data Controller for new purposes previously not in existence.

A consistent Data Governance function will also be required at the "micro-level" of the individual Health Service Providers to ensure the correct application of standards, development and delivery of appropriate training, and clear and consistent definition and implementation of common policies and procedures. This will particularly important in the context of issues such as:

- Ensuring consistency of data input standards for "relevant identifying particulars"
- Error handling and corrections policies and procedures within organisations and between organisations.

[15] See: http://www.tuppenceworth.ie/blog/2015/06/18/data-protection-commissioner-finds-pod-was-and-still-is-unlawful/ and http://www.irishexaminer.com/ireland/concern-over-database-of-pupils-info-337870.html for more information

- Ensuring security of access to Health Identifiers and the Health Identifiers register. Issues such as sharing of user credentials for systems that allow access to the Register will become of increased significance given the personal penalties involved.

It is essential that the Governance structures that are defined and developed for the Health Identifiers Registers address not just technology concerns but also address the Business needs, Human Factors, and Information and Communication challenges and opportunities presented by these Registers.

While technology and tools will play a key role in the implementation of the Health Identifiers and the Health Identifiers Registers, ultimately it will be how they are governed and used by people and for people that will determine the perceived success or failure of this initiative.

INFORMATION QUALITY AND OUTCOME RISKS

The creation of new Health Identifiers Registers brings with it a range of potential information quality challenges in an environment that has a low tolerance level for errors given the life altering consequences of medical treatment errors.

One example of where this will be an issue is the use of the PPSN to be a common linking identifier as part of the data matching and integration processes. This process is dependent on the quality of the PPSN data provided at the point of data capture.

Historically, this data would have been used for largely administrative purposes unrelated to the delivery of patient care such as billing, processing of medical cards, or ensuring the correct application of Social Welfare entitlement. Under the Health Identifiers Act 2014 the purpose of PPSN changes and it becomes a critical piece of data to link currently silo'd data sets together for the purposes of creating the relevant Health Identifier.

Issues which could affect the effectiveness of this process will include:

- Mis-keying or transposition errors in the input of PPSN data in Health Service Providers or other organisations leading to incorrect matches
- Incorrect linking of PPSNs to other identifying data in a source record, leading to incorrect matches in the Health Identifiers Register.
- Inconsistencies between PPSNs and other identifying particulars passed from source data providers. For example: PPSN 1234567X being linked to Daragh O Brien in one system and Dara O'Briain in another. Are these the same person?

In the UK, the Information Commissioners Office prosecuted a financial services provider for incorrectly linking the pension funds of two people resulting in one person's premiums being paid into the other person's pension fund. The pension provider was fined £50,000 for failing to correct the incorrect matching of data.

The potential impacts of incorrect matching of data in a health care context are slightly more than having one's pension fund underfunded.

It is also important to bear in mind the potential for fraudulent uses of PPSNs. In 2011 it was estimated by the Department of Social Protection that there were 7.2 million PPSNs in circulation for a population of 4.6 million people. This raises a significant risk of identity theft.

However, there are often valid reasons why individuals might have been issued with more than one PPSN. For example, witness relocation and similar purposes in the law enforcement context often require an entirely new Public Services Identity to be created for witnesses and their families. The approach to matching and consolidation of data needs to take into account valid reasons for exceptions to the obvious business rules that might exist in the lineage of data.

EXTENDING TO AN ETHICAL FRAMEWORK

When we consider the 'voice of the individual' in the context of the Information Governance structures that should be applied to the development and operation of the Health Identifiers platforms, we have an opportunity to consider the Ethical dimension of what is to be achieved. This echoes the provision in Section 2 of the Health Identifiers Act 2014 which requires research use of the identifiers to be subject to an Ethics Review Board.

The European Data Protection Supervisor has published an Opinion on Ethics in Big Data which, while focussed on the "big data" agenda, is directly applicable to traditional data management. The EDPS proposes an ethical approach to Information Management that is focussed on promoting Human Dignity through effective governance and controls, based on four key pillars of:

- Informed and empowered Data Subjects
- Accountable Data controllers
- Innovative Privacy Engineering
- Future-oriented rules and enforcement.

We examine how this ethical framework can be defined and implemented an information management environment in our Whitepaper report *A Primer on Ethical Principles in an Information Governance Framework*. For the purposes of this report, we set out the summary framework, which includes the "voice of the customer", their expectations, and the societal and organisational ethic frameworks and priorities which will influence how information is managed and governed in the organisation.

By adopting an ethical framework that places the emphasis on how the human dignity of the individual is enhanced, the governance of information around Health Identifiers can be implemented in a way that moves the emphasis away from a pure technology and administrative focus and aligns with the delivery of value to the individual (service user, medical staff, other employee) and the core values of the HIQA standard in Better and Safer Patient Care. Furthermore, as this requires proactive identification of and mitigation of risks to personal data privacy and other fundamental rights, it would drive a focus on appropriate use of Privacy Impact Assessments and the importance of the "voice of the customer".

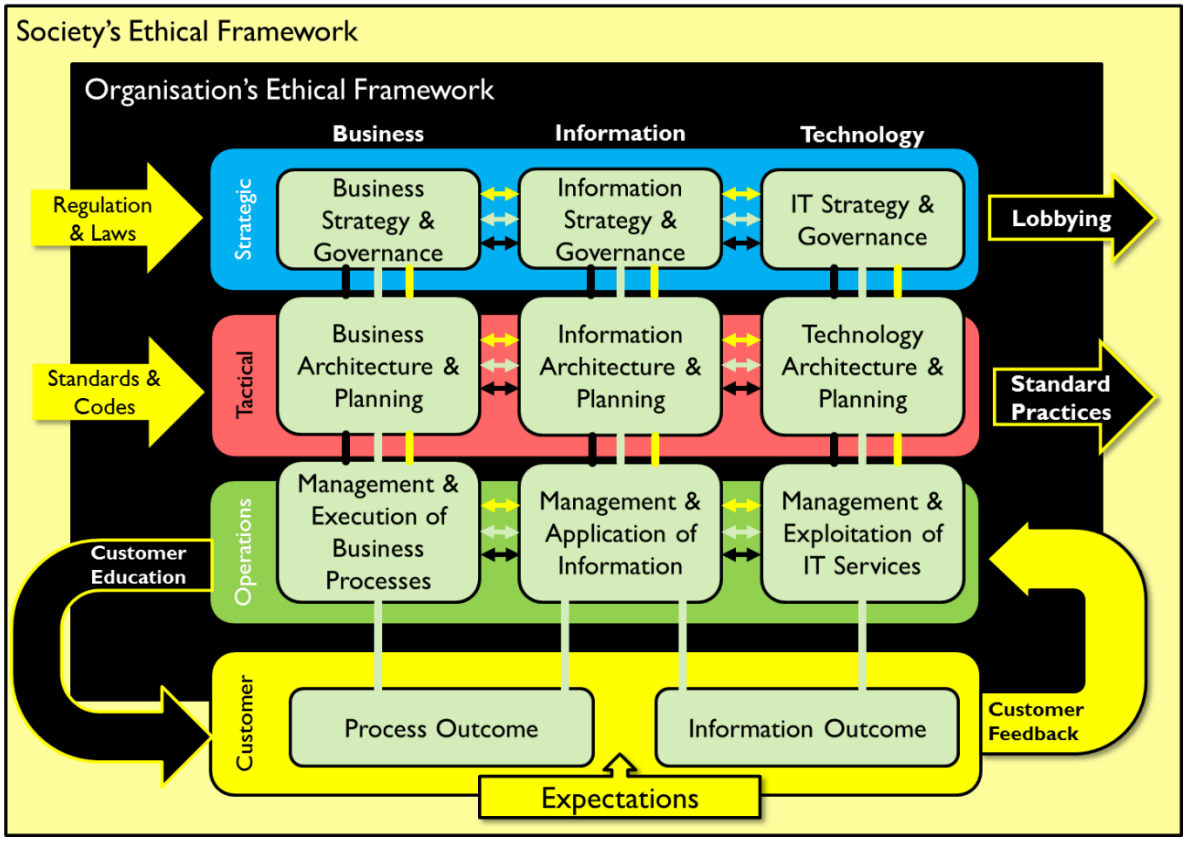


FIGURE 7 AN ETHICAL FRAMEWORK FOR INFORMATION MANAGEMENT

The Castlebridge Ethical Framework for Information Management extends our 11-box model. The operation of this framework is detailed in our Ethics Primer report.

PRIVACY IMPACT ASSESSEMENTS AND THE INFORMATION LIFE CYCLE

Given the importance of Privacy Impact Assessments in the context of a data sharing environment that requires prior notification, effective management of risks to privacy, and which increasingly calls for an ethical approach to managing information, it is essential that the development and operation of the Health Identifiers Registers and associated systems is approached in the context of an Information Asset Life Cycle model.

A recent criticism of the Health Identifiers project has been that it appears the Registers have been built *before* any Privacy Impact Assessments have been conducted. PIAs are a key *planning* activity and, in the context of a Life Cycle approach to Information Asset Management, should come **before** the Obtaining of data, its storage and sharing, and the other phases of the life cycle.

In light of the rulings in *Schrems* and *Bara* and the need for clarity of communication of purpose, controls, and scope of Health Identifiers, it is essential that the Information Governance and Stewardship structures that are implemented from a Strategical and Tactical perspective ensure that appropriate investment is made in the Planning phase of revisions to the system that ensures Privacy Impact Assessments and other planning activities are undertaken to ensure that the Registers operate with the appropriate levels of information quality, respect for privacy, and controls against unauthorized use so that all stakeholders can consider them a trusted and trustworthy source of key master data identifiers in the Healthcare system.

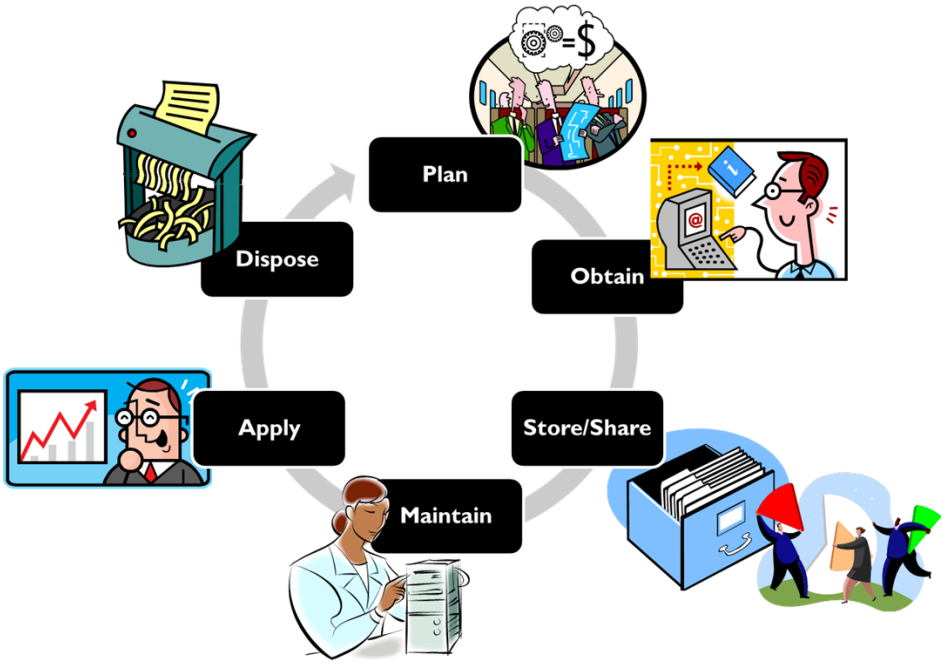


FIGURE 8 THE INFORMATION ASSET LIFE CYCLE

IMPLEMENTATION LESSONS THAT CAN BE LEARNED

While it is tempting to use the UK NHS's "Health.Data" privacy debacle of recent years as a case study example, recent Irish Public Sector data integration projects have provided a wealth of examples of, for want of a better expression, not to do it.

The most recent, and most relevant to the Health Registers scenario, is the Primary Online Database project in the Department of Education.

PRIMARY ONLINE DATABASE

The Primary Online Database debacle provides a number of key lessons that can be learned from in the implementation of the Health Identifiers Registers.

IDENTIFY AND ENGAGE WITH THE CORRECT STAKEHOLDERS

The Department of Education engaged only with schools, until the parents started complaining to the Data Protection Commissioner.

School principals were being asked to provide personal and sensitive personal data about students and to derive other information. Appropriate timely engagement with parents of children (not just parents representative groups) to explain the nature and purpose of processing could have improved the level of trust in the process.

PUT THE PERSON AT THE CENTRE

The Department of Education's response to criticism of POD was to defend their position, to the point that the Minister for Education stated to the Dáil that the DPC had approved the processing when the DPC has no power to issue such approvals.

The proposed retention periods within the original POD scheme did not appear to link to any obvious purpose and gave rise to a suspicion among parents that data, including sensitive personal data, was being retained by the Department for unstated purposes such as to support defences against claims taken by pupils who had been subject to sexual abuse.

This retention period was ultimately dropped from being *at least* 30 years to being capped at 19 years.

Lesson to learn: It is essential to have a focus on the end-customer perspective. This is consistent with HIQA standards and best practices in information quality management.

ENSURE CLEAR BASIS FOR THE PROCESSING OF CURRENTLY PROPOSED AND FUTURE DATA

The Data Protection Commissioner has held that a range of data that was being sought by the Department of Education from schools had no legal basis. These fields included:

Mother's Maiden Name; Enrolment Date; Enrolment Source; Leaving Date; Leaving Destination; Integrated Indicator; Indicator for Receipt of Learning Support; Pupil Type and Special Class Type.

An amending Statutory Instrument should have been implemented before this data was sought. It was not. In this case, the DPC is allowing for a Statutory Instrument to be introduced to retrospectively authorize the gathering of this data. However, there is no guarantee that in future the DPC would be amenable to such a legislative "reboot" given the clear precedent that has been set in this case.

Furthermore, any amended Statutory Instrument would need to properly address the scope and purpose of any new data gathering or data processing. Privacy Impact Assessments conducted *before* implementation begins are a useful tool to achieve this.

Lesson to learn: "Scope Creep" needs to be controlled through effective governance to ensure clarity on the statutory basis and proportionality of any processing. Privacy Impact Assessments are a key tool to achieving this.

ENGAGE WITH CONCERNS, DON'T DISMISS THEM: PRIVACY IMPACT ASSESSMENTS!

The POD case study is interesting in that one of the parents who raised concerns, and whose complaint to the DPC resulted in the recent finding against the Department, was a solicitor who specializes in Data Protection law and has successfully challenged EU Directives on the basis of their incompatibility with fundamental Data Protection rights.

Parents with Data Protection experience serving on or supporting school Boards of Management also raised concerns early on.

The Department dismissed concerns raised by knowledgeable and aware parents who recognized benefits of POD but wanted to ensure they were achieved in a manner that was compliant.

Effective and timely engagement with parents, subject matter experts, or civic society groups could have delivered an improved approach in a more timely manner, rather than tying up resources in a Data Protection Commissioner investigation which delivered a series of about faces from a Minister who was adamant at the start that the non-compliant scheme was compliant.

Furthermore, the data sharing which took place as part of the development of the POD system is unlikely to meet the test in *Bara*, not least because the Department engaged with the schools as the lead stakeholder, not with the parents and guardians of the children in question to educate and inform as to the purposes of processing etc.

Lesson Learned: It's important to engage with stakeholders. Privacy Impact Assessments provide a structured way to ensure that this engagement can take place in a manner that supports effective governance. Ignoring concerns, especially when raised by concerned stakeholders with relevant professional expertise, can lead to public reversals of policy or negative findings from the DPC.

FIND OUT MORE ABOUT

PRIVACY IMPACT ASSESSMENTS

To find out more about Privacy Impact Assessments, to get help or support in conducting an independent and objective Privacy Impact Assessment, or to get training in a structured method for conducting Privacy Impact Assessments that is based on proven Data Governance and Information Quality Management principles, please contact Castlebridge Associates.

Our expert consultants have developed a unique structured method based on a proven Data Management Body of Knowledge that supports a range of levels of Privacy Impact Assessment, from high level reviews to detailed "deep dive" analysis.

Our Privacy Impact Assessment methodology also provides a "Data Governance for Privacy Health Check" that highlights key areas in the Business, Information, and Technology management in your organization that have potential to impact on your customers' Information and Process outcomes including the impact on their Privacy.

Castlebridge Associates has also developed an indepth training course on Privacy Impact Assessments, the theory elements of which are used in the Law Society's Professional Certificate in Data Protection Practice, a course which our founder Daragh O Brien helped develop and lectures on.

TRAINING & COACHING

Castlebridge Associates provides specialist training, coaching, and skills development services in Information Governance, Data Protection, and Information Quality.

Many of our courses map to the learning objectives of industry standard certifications.

ADVISORY AND CONSULTING

We provide a range of advisory and consulting services in the areas of Information Governance, Information Systems Project Management, Data Protection, Information Quality, and Information Systems Requirements analysis and definition.

We also conduct holistic Information Governance maturity assessments, Data Protection compliance assessments, and Information Quality audits.

CONTACT US

To find out more about the services we offer and how we might be able to help with PIAS or consulting, training, or coaching for Data Protection, Data Governance, or Information Quality:

Email: enquiries@castlebridge.ie

Web: www.castlebridge.ie/contact

Phone: +353 76 6031850

> The team from Castlebridge provided invaluable insight and input to help us develop a roadmap and vision for our Data Governance program. Bringing together a pragmatic perspective and a strong methodical approach, they delivered a valuable route map for our Data Governance journey.
> *- John Greene, Head of Data Governance, Aer Lingus*