

Architecture Principles

 12th Dec 2019

|  |  |
| --- | --- |
| Date Issued | 12th Dec 2019 |
| Version No. | 2.1 |
| Status | [x]  Approved |
| Document Location | [click to enter Document link] |
| Prepared By | Lilly WalshBusiness Architecture Lead, Enterprise Architecture , OoCIO | Helen LambertCompliance, Assurance & Governance Lead, Enterprise Architecture,OoCIO |
| Security Classification | Public  |

# Document Control

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Issue Date** | **Changes** |
| 1.0+ | *Lilly Walsh* |  | *Working draft of document by author*  |
| 1.1 | Lilly Walsh  | 10/01/2018 | *Amendments following EA Team workshop*  |
| 1.2 | Martin Tully | 31/01/2018 | *Amendments from Martin Tully* |
| 1.3 | Lilly Walsh | 02/02/2018 | *Amendments following EA team conference call* |
| 1.4 | Lilly Walsh | 09/03/2018 | *Amendments following EA team feedback* |
| 1.5 | Helen Lambert | 13/07/2018 | *Amendments following EA team feedback* |
| 1.6 | Helen Lambert | 16/07/2018 | *Amendments following EA team feedback call* |
| 1.7 | Helen Lambert | 18/07/2018 | *Final adjustments from EA team* |
| 2.0 | Helen Lambert | 18/07/2018 | *Version for Approval* |
| 2.1 | Helen Lambert | 12/12/2019 | *Amendments from Helen Coughlan (CTO) to BP#6* |

Distribution List

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Business Unit** | **Title**  | **Responsibility** |
| Peter Connolly | Enterprise Architecture | Head of Enterprise Architecture | Owner |
| Martin Curley | OoCIO | CIO | Approver |

# Approvals

Sign Off – please see sign off matrix in the table below:

|  |  |  |
| --- | --- | --- |
| **Name** | **Latest Version Signed off** | **Sign off Date** |
| ***Peter Connolly***  | ***V2.0*** | ***18/07/2018*** |
| ***Martin Curley***  | ***V2.0*** | ***28/11/2018*** |

References

|  |  |
| --- | --- |
| **Document Name**  | **Document Link eHealth Ireland** |
| Standards Catalogue | [Design Authority Standards Catalogue](http://www.ehealthireland.ie/Library/Document-Library/Standards-Catalogue-v1_0.pdf). |

Contents

[Document Control 2](#_Toc519693687)

[Revision History 2](#_Toc519693688)

[Distribution List 2](#_Toc519693689)

[Approvals 3](#_Toc519693690)

[References 4](#_Toc519693691)

[Glossary 7](#_Toc519693692)

[1. Introduction 8](#_Toc519693693)

[1.1 Document Purpose 8](#_Toc519693694)

[1.2 Document Structure 8](#_Toc519693695)

[2. Overview Architecture Principles 9](#_Toc519693696)

[3. Overall - Architecture Principles 10](#_Toc519693697)

[OP #1 Primacy of Principles 10](#_Toc519693698)

[OP #2 Maximise the Benefit to the Enterprise 10](#_Toc519693699)

[OP #3 Integrated Care 11](#_Toc519693700)

[OP #4 ICT Responsibility 11](#_Toc519693701)

[OP #5 Protection of Intellectual Property 12](#_Toc519693702)

[OP #6 Compliance with Law 12](#_Toc519693703)

[4. Design - Architectural Principles 13](#_Toc519693704)

[DP #1 Single Consistent Identifier 13](#_Toc519693705)

[DP #2 Common and Consistently Enforced Access and Entitlements 13](#_Toc519693706)

[DP #3 Appropriate Configurations using Phased Implementations 14](#_Toc519693707)

[DP #4 National Core Components are Foundational 14](#_Toc519693708)

[DP #5 Patient Centric eHealth 15](#_Toc519693709)

[5. Business - Architecture Principles 16](#_Toc519693710)

[BP #1 Hierarchy of Standards 16](#_Toc519693711)

[BP #2 Information Management is Everybody’s Business 17](#_Toc519693712)

[BP #3 Common Use Applications 17](#_Toc519693713)

[BP #4 Reuse of Non- Core Functions 18](#_Toc519693714)

[BP #5 Insight from Analytics 18](#_Toc519693715)

[BP #6 Business Continuity 19](#_Toc519693716)

[BP #7 Open System Theory 20](#_Toc519693717)

[BP #8 Adaptive Organisation 20](#_Toc519693718)

[6. Application - Architectural Principles 21](#_Toc519693719)

[AP #1 End of Life or Obsolescence 21](#_Toc519693720)

[AP #2 Technology independence 22](#_Toc519693721)

[AP #3 Maximise Access to Applications 22](#_Toc519693722)

[AP #4 Design Together - Products and Service 23](#_Toc519693723)

[AP #5 Reduce Complexity 23](#_Toc519693724)

[7. Security - Architectural Principles 24](#_Toc519693725)

[SP #1 Data Security 24](#_Toc519693726)

[SP #2 Privacy and Security Safeguards 24](#_Toc519693727)

[SP #3 Security Design 25](#_Toc519693728)

[SP #4 Least Privilege 25](#_Toc519693729)

[8. Technology - Architecture Principles 26](#_Toc519693730)

[TP #1 Requirements based Change 26](#_Toc519693731)

[TP #2 Technology Based Change 27](#_Toc519693732)

[TP #3 Changes are Planned 27](#_Toc519693733)

[TP #4 Responsive Change Management 28](#_Toc519693734)

[TP #5 Control Technical Diversity 28](#_Toc519693735)

[TP #6 Decoupling the Distribution Channels 29](#_Toc519693736)

[TP #7 Enterprise-accessible On-demand Services 30](#_Toc519693737)

[TP #8 Resiliency and Availability 31](#_Toc519693738)

[TP #9 Scalability and Modularity 31](#_Toc519693739)

[TP #10 Industry Standard Technology 31](#_Toc519693740)

[TP #11 Technology Will Not Be Deployed Before Its Time 32](#_Toc519693741)

[9. Information - Architecture Principles 33](#_Toc519693742)

[IP #1 Data is an Asset 33](#_Toc519693743)

[IP #2 Data is Sharable Across & Between Institutions 34](#_Toc519693744)

[IP #3 Data is Accessible 34](#_Toc519693745)

[IP #4 Information is Everyone’s Business 35](#_Toc519693746)

[IP #5 Common Vocabulary and Data Definitions 35](#_Toc519693747)

[IP #6 Data Trustee 36](#_Toc519693748)

[10. Interoperability - Architectural Principles 37](#_Toc519693749)

[IOP #1 Technical and Syntactic Interoperability 37](#_Toc519693750)

[IOP #2 Semantic Interoperability 38](#_Toc519693751)

[Appendix 1 – EA Principles Management Process 39](#_Toc519693752)

Glossary

Please see the table below for a description of terms used within this document.

|  |  |  |
| --- | --- | --- |
| **Term**  | **Full Name** | **Description** |
|  |  |  |

# Introduction

## Document Purpose

The purpose of this document is to describe the Architecture Principles that reflect the eHealth’s strategic purpose, vision and values. The principles define the decision making framework upon which the future design and evolution of systems architecture is based. The principles should be followed by all Architects when making architecture and planning decisions, framing policies, procedures, and standards, and supporting resolution of contradictory situations.

Although the Architecture Principles are designed to be “timeless” because they define a value system, they should be reviewed upon changes in the organization’s business strategy and technology industry developments. Structures must be in place to approve the principles and any changes or exceptions to them, for example the Architecture Review Board and the Architecture Endorsement Board.

A good set of principles will be founded in the beliefs and values of the organization and expressed in language that the business understands and uses. Principles should be few in number, future-oriented, and endorsed and championed by senior management. They provide a firm foundation for making architecture and planning decisions, framing policies, procedures, and standards, and supporting resolution of contradictory situations. A poor set of principles will quickly become disused, and the resultant architectures, policies, and standards will appear arbitrary or self-serving, and thus lack credibility. Essentially, principles drive behaviour.

There are five criteria that distinguish a good set of principles:

* **Understandable:** the underlying tenets can be quickly grasped and understood by individuals throughout the organization. The intention of the principle is clear and unambiguous, so that violations, whether intentional or not, are minimized.
* **Robust:** enable good quality decisions about architectures and plans to be made, and enforceable policies and standards to be created. Each principle should be sufficiently definitive and precise to support consistent decision-making in complex, potentially controversial situations.
* **Complete:** every potentially important principle governing the management of information and technology for the organization is defined. The principles cover every situation perceived.
* **Consistent:** strict adherence to one principle may require a loose interpretation of another principle. The set of principles must be expressed in a way that allows a balance of interpretations. Principles should not be contradictory to the point where adhering to one principle would violate the spirit of another. Every word in a principle statement should be carefully chosen to allow consistent yet flexible interpretation.
* **Stable:** principles should be enduring, yet able to accommodate changes. An amendment process should be established for adding, removing, or altering principles after they are ratified initially.

## Document Structure

A table of all the principles by discipline is provided to give an over view. Each principle is then described by a name, short description, rationale, and implications.

The rationale highlights the purpose and business benefits of adhering to the principle, providing a basis for justifying architecture activities.

The implications address the requirements for carrying out the principle and how the principle affects business and technology. The requirements include key tasks, resources, and potential costs to the organization for adhering to the principle.

#

# Overview Architecture Principles

|  |  |  |
| --- | --- | --- |
| Overall | Design | Business |
| OP#1 | Primacy of Principles | DP#1 |  Single Consistent Identifier  | BP#1 | Hierarchy of Standards |
| OP#2 | Maximise the Benefit to the Enterprise | DP#2 | Common and Consistently Enforced Access and Entitlements  | BP#2 | Information Management is Everybody’s Business |
| OP#3 | Integrated Care | DP#3 | Appropriate Configurations using Phased Implementations | BP#3 | Common Use Applications |
| OP#4 | ICT Responsibility | DP#4 | National Core Components are Foundational | BP#4 | Reuse of Non-Core Functions  |
| OP#5 | Protection of Intellectual Property | DP#5 | Patient Centric eHealth | BP#5 | Insight from analytics  |
| OP#6 | Compliance with Law | **Technology** | BP#6 | Business Continuity |
| **Application** | TP#1 | Requirements Based Change | BP#7 | Open System Theory |
| AP#1 | End of life or obsolescence | TP#2 | Technology Based Change  | BP#8 | Adaptive Organisation |
| AP#2 | Technology Independence  | TP#3 | Changes are Planned | **Information** |
| AP#3 | Maximise Access to Applications | TP#4 | Responsive Change Management | IP#1 | Data is an Asset  |
| AP#4 | Design Together – Products and Services | TP#5 | Control Technical Diversity  | IP#2 | Data is Sharable Accross & Between Insitiutions |
| AP#5 | Reduce complexity | TP#6 | Decoupling the distribution channels | IP#3 | Data is Accessible |
| **Security** | TP#7 | Enterprise-accessible on-demand services  | IP#4 | Information is Everyone’s Business |
| SP#1 | Data Security | TP#8 | Resiliency and Availability | IP#5 | Common Vocabulary and Data Definitions |
| SP#2 | Privacy and Security Safeguards | TP#9 | Scalability and Modularity | IP#6 | Data Trustee |
| SP#3 | Security Design | TP#10 | Industry Standard Technology | **Interoperability** |
| SP#4 | Least Privilege | TP#11 | Technology will not be deployed before its time | IOP#1 | Technical & Syntactic Interoperability |
|  |  |  |  | IOP#2 | Semantic Interoperability |

# Overall - Architecture Principles

The following principles are high-level statements about how architecture should be used to support the business needs.

|  |
| --- |
| OP #1 Primacy of Principles  |
| These principles apply to all organisations within the HSE enterprise. |
| **Rationale:** The only way to provide a consistent and measurable level of quality information to decision-makers is if all organizations within the HSE abide by the principles. |
| **Implications :*** Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the management of information.
* Information management initiatives will not begin until they are examined for compliance with the principles.
 |

|  |
| --- |
| OP #2 Maximise the Benefit to the Enterprise |
| Information management decisions are made to provide maximum benefit to the enterprise as a whole. |
| **Rationale:** Decisions made from an enterprise wide perspective have greater long term value than decisions made from any particular organisational perspective. |
| **Implications:*** Achieving maximum enterprise wide benefit requires changes in the way information is planned and managed, technology alone will not bring about this change
* Some HSE division/function/department may have to concede their own preferences for the greater benefit of the entire enterprise.
* Applications components should be shared across the organisational boundaries.
* All initiatives should conform to the blueprints and priorities established by the enterprise.
* As needs arise, priorities must be adjusted. A forum with comprehensive enterprise representation should make these decisions.
* Maximum return on investment requires meta model standardisation.
 |

|  |
| --- |
| OP #3 Integrated Care  |
| Implement interoperability and data standards to support the delivery of integrated healthcare*.*  |
| **Rationale:** Maintains a single 360-degree view of the participant/patient profile, allowing providers and payers to serve participants/patients effectively and share data across the HSE. |
| **Implications:** * Adopt a standardised metadata registry framework that enables participant/patient records to be used/assembled for different purposes by different healthcare providers.
* Provide functionality to appropriately link disparate systems.
* Migrate from paper based records to electronic record systems.
* Implement appropriate metadata standards.
* Implement appropriate interoperability standards.
* Implement appropriate information management standards to ensure quality, complete and appropriate information is collected to support the delivery of integrated healthcare now and in the future.
* Facilitate the exchange of data among components to better enable their functionality.
* Define data standards and common data exchange schemas to permit data sharing across clinicians, labs, hospital, pharmacy and patient regardless of the application or the application vendor.
 |

|  |
| --- |
| OP #4 ICT Responsibility  |
| The ICT organisation is responsible for owning and implementing ICT processes and providing infrastructure that enables solutions to meet the business/service defined requirements for functionality, service levels, cost, and delivery timing.  |
| **Rationale:** * Bespoke solutions and inconsistency in ICT enabled delivery undermines the integration of and management of ICT enable business solutions and the delivery of business services.
* Efficient and effective solutions have reasonable costs and clear benefits.
* Maximum return on investment and national capability for all services requires ICT decisions to adhere to enterprise-wide drivers and priorities.
* No minority group should detract from the benefit of the whole.
 |
| **Implications**: * The IT function should define processes to manage business/service unit expectations.
* A process should be created to prioritise projects.
* Data, application, and technology models should be created to enable integrated quality solutions and to maximise results.
* The business needs to champion and continuously remind their services on the need to adhere to this principle and that National OoCIO approval should be sought prior to any consideration and especially procurement of any ICT dependant systems or services.
 |

|  |
| --- |
| OP #5 Protection of Intellectual Property |
| The enterprise’s Intellectual Property (IP) must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes. |
| **Rationale:**A major part of the enterprise’s IP is hosted in the IT domain. |
| **Implications:*** While protection of IP assets is everybody’s business, much of the actual protection is implemented in the IT domain. Even trust in non-IT processes (email, mandatory notes etc) can be managed by IT processes.
* A security policy, governing human and IT actors, will be required that can substantially improve the protection of IP. This must be capable of both avoiding compromises and reducing liabilities.
 |

|  |
| --- |
| OP #6 Compliance with Law |
| Enterprise information management processes comply with all relevant laws, policies, and regulations. |
| **Rationale:** HSE policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations that are not in conflict with legislation. |
| **Implications:** * The enterprise must be mindful to comply with laws, regulations, and external policies regarding the collection, retention and management of data.
* There should be adequate education and access to the legislation.
* Changes in the law and changes in regulations may drive changes in our processes or applications.
 |

# Design - Architectural Principles

The key principles of the future architecture direction consider the technology trends in health and are based on international best practice and experience in the health sector. Key themes underpinning these principles are the sharing of information, alignment with legislation and engagement with the Irish Data Protection Commissioner which will play a critical part in ensuring successful implementation.  The principles are set out below.

|  |
| --- |
| DP #1 Single Consistent Identifier |
| The Individual Health Identifier (IHI) Bill provides for patient and practitioner identifiers. Identifiers are also required for locations. |
| **Rationale:** Identifiers are required as a fundamental enabler of patient care records, to improve data protection through accurate data linking, and improve management through more accurate reporting.  |
| **Implications:** * The IHI must be applied to all systems that integrate with the HSE architecture, where a patient, practitioner or location is being described.
* All consumer systems must have an IHI field in the design.
 |

|  |
| --- |
| DP #2 Common and Consistently Enforced Access and Entitlements |
| User access should be based on a single identity and should be common, consistently enforced and reviewed across all systems. |
| **Rationale:**Consistency of access and entitlements is required to enable efficient entitlement management and audit of access and access rights across the enterprise. Access and entitlements should be reviewed regularly. |
| **Implications:*** Entitlements to access functionality and data should be based on consistent rules that are applied across all systems.
* Entitlements should be based on role and relationship to the patient.
* Access must be defined in the solution design – Security by design.
* Processes should be developed to review user access and remove where appropriate.
 |

|  |
| --- |
| DP #3 Appropriate Configurations using Phased Implementations  |
| Solutions should enable federated, hybrid or centralised solutions to be implemented in a phased manner, using standardised interfaces.  |
| **Rationale:** * The HSE has a mix of federated, centralised and hybrid (in-between) systems. This architecture design will support all of these options now and in the future.
* This architecture design supports future solutions, in particular solutions that integrate across systems.
 |
| **Implications:**Current and future system designs should support the implementation of standardised interfaces and integrate with the rest of the HSE estate. |

|  |
| --- |
| DP #4 National Core Components are Foundational  |
| The national core components are the foundation for all other components which integrate with the core.  Point of care systems and system processes, integrate and use these core systems.  |
| **Rationale:**A stable core is important, as changes to the core in future would have the potential to disturb many systems. |
| **Implications:*** The core will define the interfaces for all non-core systems to integrate with, and enable the integration of these other systems.
* Local and central point of care applications will integrate with core systems to provide functionality and a connected view of information to end users.
* System processes will integrate with and use the core systems to automate and connect processes across multiple care applications and care settings.
 |

|  |
| --- |
| DP #5 Patient Centric eHealth |
| Patient-centricity represents an emerging vision for improved health care delivery via empowerment through greater transparency, access to services and information for patients. |
| **Rationale:**The traditional view is that “patient centricity” means that the patient is at the centre of healthcare delivery services, but that the energy and decision-making still rely upon the expertise of their healthcare provider. From now on patients will be empowerment through greater transparency, access to services and information. |
| **Implications:** * Emphasis should be on access to information.
* User’s access includes both patient and their healthcare provider(s).
* Designs should consider two way interactions between the healthcare provider and their patients.
* Solution design should consider provider activities in terms of how its supports patient health management.
* Designs should consider systems availability in terms of global and local access, anywhere, anytime.
* Designs should support patients having direct access to their records.
 |

# Business - Architecture Principles

|  |
| --- |
| BP #1 Hierarchy of Standards |
| Overcoming integration and interoperability challenges allows the HSE to connect systems internally and externally. Without agreed standards shared by at least two systems, processes or other actors, integration and interoperability is not possible. Therefore, standardisation at a technical, semantic and organisation level is a precondition to address both integration and interoperability. |
| **Rationale:*** The principle of hierarchy of standards provides a practical framework in which standards can be created in the context of diversity, and provides a means of flexibility as against central control, which standards apply.
* Business Process Integration (BPI) allows for the automation of management, operational, and supporting processes. The enterprise spends less time concerned about the challenges of integration and more time and energy on driving new service initiatives.
 |
| **Implications:*** BPI is essential for businesses looking to connect systems and information efficiently. BPI allows for automation of business processes, integration of systems and services, and the secure sharing of data across numerous applications.
* Integration requirements must take users’ needs and organisation perspectives into consideration and relate them to the goals of better efficiency, effectiveness and co-ordination.
* Integration can be conceptualised across vertical and horizontal dimensions. (Horizontal involves increasing the number of business domains, which in turn increases the differences between views. Vertical is concerned with levels of hierarchy /interoperability (the ability to use and share information). Both dimensions must be considered when designing future state blueprints and roadmaps.
* There are three levels of standardisation of increasing complexity: - technical/syntactic, semantic and organisational. All levels must be considered when designing reference architectures.
* Allow for variations and flexibility in service delivery and supporting administration systems.
 |

|  |
| --- |
| BP #2 Information Management is Everybody’s Business |
| Information management decisions are made to provide maximum benefit to the enterprise as a whole. |
| **Rationale**: * Information users are the key stakeholders, or customers, in the application of technology to address a business need.
* To ensure information management is aligned with the business, all organizations in the enterprise must be involved in all aspects of the information environment.
* The business experts from across the enterprise and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of IT.
 |
| **Implications:** * To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment.
* Commitment of resources will be required to implement this principle.
 |

|  |
| --- |
| BP #3 Common Use Applications |
| Development of national applications used across the HSE enterprise is preferred over the development of similar or duplicative applications which are only provided to a particular organization/service. Exceptions are only by agreement via the Architectural Review Board or equivalent Board. |
| **Rationale:*** Duplicate capability is expensive and proliferates conflicting data.
* National and cross-organisational application solutions considerably reduce the cost to the business versus the high cost and effort or resources required for development, support, management and interoperability of duplicative or local specific applications, systems and tools.
* Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular departmental or organizational perspective.
 |
| **Implications:** * Solutions which use bespoke applications or depend on a capability which does not serve the entire enterprise should plan to change over to the enterprise-wide capability if and when available.
* Organisations will not be allowed to develop capabilities for their own use which are similar/duplicate of enterprise-wide capabilities. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
* The business should champion and continuously remind their services of the need to adhere to this principle
* Application development priorities should be established by the entire enterprise for the entire enterprise.
* Some departments may have to concede their own preferences for the greater benefit of the entire enterprise.
* Data and information used to support enterprise-wide decision making should be standardised to ensure quality, complete and appropriate information is collected by Common Use Applications across the enterprise.
* Applications components should be shared across organizational boundaries.
 |

|  |
| --- |
| BP #4 Reuse of Non- Core Functions  |
| Promote reuse of non-core functions across the enterprise for effective and effective back-office management execution. Consideration should be given to using separate applications/systems for non-core functions. |
| **Rationale:**Non-core functions although not key to service provision, are essential to the smooth running of the enterprise.  |
| **Implications:*** Provide seamless integration of back-office administration services to other parts of application architecture.
* Avoid the need to implement non value-adding functionality to core applications.
* Decouple enterprise management activities and systems (finance/accounting, HR, facilities, procurement, audit and compliance).
 |

|  |
| --- |
| BP #5 Insight from Analytics |
| Simplify information flows and enable insights from analytics. |
| **Rationale**: * The global healthcare industry is experiencing fundamental transformation as it moves from a volume-based business to a value-based business.
* Analytics can provide the mechanism to sort through this torrent of complexity and data, and help healthcare organizations deliver on these demands.
* It takes big plans, discrete actions, and some very specific management approaches to gain the benefits of analytics.
 |
| **Implications:*** Data analytics is dependent on good quality data.
* Focus on an integrated workflow healthcare system with simplified data access and analytics.
* Design and implement information architectures and governance to enable the efficient use, transfer and analysis of information.
* Development and use of integrated information services across the enterprise.
* Where appropriate, leverage cloud architecture to facilitate analytical processing of large data.
* Simplify and enable collaboration across community and acute healthcare settings through data sharing and analytics.
* Develop and communicate various data, terminology and interoperability standards with various stakeholders.
* Segregate data to provide decision makers with the right information at the right time.
* Implement greater use of health It and health system connectivity/exchange to lower costs and improve health quality.
* Tools should be used to aggregate data at category level (disease, population, group, hospital)
* Support strategic planning with data models that can import current data and allow planners to do ‘what if’ scenarios.
 |

|  |
| --- |
| BP #6 Business Continuity |
| Business continuity refers to the ability of an organisation to maintain essential services during and following disruption.  |
| **Rationale**: * As system operations become more pervasive, the design of IT Systems should be aligned with the criticality of the services as determined by a business impact analysis.
* Business areas throughout the enterprise should be provided with the capability to continue their business functions in line with service criticality.
* The architecture of the IT solution should have appropriate design and controls in place to enable the delivery of healthcare or enterprise activities.
* The enterprise business functions must be capable of operating on alternative information delivery mechanisms or through manual fall back or workaround.
* The availability of IT services will be based on agreed recovery point and time objectives (RTO,RPO), aligned with a risk/value matrix for the organisation.
* In reality no system can operate 24/7/365 and none should be depended upon to do so.
 |
|  **Implications:*** Recoverability, redundancy, and maintainability should be addressed at the time of the design
* Applications must be assessed for criticality and impact on the enterprise mission. In order to determine what level of continuity is required and what corresponding recovery plan is required
* Dependency on shared system applications mandates that the risks of the business interruption must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure or designing mission-critical services to assure business function continuity through redundant or alternative capabilities.
* Best practice would mean that Business Continuity plans be developed, tested and agreed before any key systems go-live and at least annually after that.
* If adequate Business Continuity plans cannot be devised serious consideration should be undertaken before going moving forward
 |

|  |
| --- |
| BP #7 Open System Theory |
| Open System Theory is used to enable business architecture design and description. |
| **Rationale**: Open System Theory enables the construction of a comprehensive and coherent set of models in which all aspects of the enterprise are included. It represents a conceptual service that a group of processes and people, supported by the relevant application, information and underlying technology, will perform.  It aids adoption of ISO 42010:2011. |
| **Implications** : * Business Modelling / Value Stream Maps (VSM) should be conducted as a part of the design phase
* Modelling languages permitted include BPMN2 and Archimate
* Value Stream Maps should be built using Lean Sigma palate
* Business modelling/VSM should inform the solutions :

(a) data capture requirements (b) functionality requirements (c) Interface requirements to ensure alignment between business and technology* Business Model Design should be included in procurement Statement of Requirements.
 |

|  |
| --- |
| BP #8 Adaptive Organisation |
| **Adaptive organizations require** work structures that are designed smartly, based upon the delivery of solutions and services (work streams) and the expected variability herein. |
| **Rationale**: Business processes construction (process and people) represent the ‘how’ the organisation works – people, systems and more, so that complexity can be understood. |
| **Implications** : * Work (processes) should be created and viewed in a holistic way, so that all organisational aspects are related directly to processes **(sub systems) and their contribution to solution and service delivery, which ensures a focus on value creation**
* **Reuse existing work flows wherever possible**
* **BPA and quality reviews are required**
 |

# Application - Architectural Principles

|  |
| --- |
| AP #1 End of Life or Obsolescence |
| Proactively plan for and manage ICT systems and solutions end of life or obsolescence. All existing and new systems must be identified by the business owner for end of life or obsolescence and proactive projects and plans established to address the risks of such systems. |
| **Rationale:*** Business service delivery risk is considerably reduced via proactive management of business ICT dependant solutions and technology end of Life (EOL). By rationalising and standardising the considerably large and varied software and hardware desktop tools and versions will allow the business use and share the same data via the same tools across the organisation, regardless of location or user. Staff training, changes and dependencies on legacy or disparate ICT desktop systems are considerably reduced.
* Through standardisation, the costs for ICT support and implementation capability are considerably reduced especially for new system implementations and support.
* OoCIO management and projects can prioritise and plan based on technology life cycles, suppliers and manufacturers’ recommendations in regard to HSE list of obsolete technologies, plus consideration of the list of technologies going obsolete in the next 1 to 2 years. They can make service/system/application retirement assessments based on objective technology plans and risk assessments.
* The business benefits are considerable in terms of standardisation and flexibility of business solutions interoperability and integration. From a business perspective, Business leaders can see the risk and exposure of using outdated applications to understand where the business service risks are if an application isn’t upgraded or replaced.
* Having a clear view of what applications or technologies are approaching end of life helps to redirect investment into the appropriate longer term solutions.
* The risk to the business of legacy solutions, especially security or incompatibility is considerably reduced.
 |
| **Implications:*** Systems should be migration to National enabled systems or new solutions acquired, rather than restricting new or existing systems integration and development, acquisition of systems, or holding back systems capability to facilitate legacy applications/technology platforms or nonstandard data structures and configurations
* There is a high risk to the HSE and business services for legacy systems that may not be supported or even function, as ICT systems and services change and modernise.
* EOL is very important in supportability and procurement of ICT enabled solutions. EOL also drives a number of projects like Migrations (e.g. Windows 7 Migration) and dictates solutions (e.g. Web enabled legacy browser specific requirements such as NIMIS).
* Organisational mandates should be developed to manage investment in systems targeted for retirement, systems requiring technology replacements or upgrades in advance of vendor end-of-support dates.

National approved and business enforced organisational mandates should be developed to ensure only National OoCIO approved suppliers, products, investment or other ICT dependant services are acquired. |

|  |
| --- |
| AP #2 Technology independence |
| Applications are independent of specific technology choices and therefore can operate on a variety of HSE approved technology platforms. |
| **Rationale:**Independence of applications from underlying technology allows applications to be developed, upgraded, and operated in the most cost effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence, becomes the driver rather than the user requirements themselves. |
| **Implications:*** This principle will require standards which support portability.
* API’s (Application Program Interfaces) will need to be developed to enable legacy systems to interoperate with applications and operating environments developed under the enterprise architecture.
 |

|  |
| --- |
| AP #3 Maximise Access to Applications |
| Embrace devices and portals for interoperability and client access. |
| **Rationale:**The healthcare "system" is now better understood as an ecosystem of interconnected stakeholders, each one charged with a mission to improve the quality of care while lowering its cost. To ensure patient safety and quality care while realising savings, these stakeholders are building new relationships.  |
| **Implications:*** Key applications should be enabled for most popular mobile and tablet operating systems in order to support technologies such as e-prescribing, EHRs, consumer-directed healthcare applications and insurance agent mobility systems (VHI, AVIVA.)
* Provide architectural reference models to encourage mobile technologies and everything it offers.
* Enable devices and portals to communicate with back-end applications that are deployed on premise and through cloud based architectures.
* Ensure mobile transactions are secure and encrypted.
* Leverage standard messaging formats for integration between all channels and devices.
 |

|  |
| --- |
| AP #4 Design Together - Products and Service |
| Switch the focus from technology to people and work together to make a health system great for its most important users. |
| **Rationale:** End users have difficulty in adopting software solutions because they have not been involved in the design process.The focus is often greater on delivering the technology and not enough on the needs of the end user.  |
| **Implications:** * Subject matter Expert (SME) or Domain expert should be a part of the delivery Team.
* End users should be involved in every step of the process and monitoring all stakeholder requirements throughout the project lifecycle.
* Applications should align with the organisations service and support strategy.
 |

|  |
| --- |
| AP #5 Reduce Complexity |
| Reduce complexity of the application portfolio and shift towards standardisation. |
| **Rationale**: Establish initiatives to rationalise the process, data, and application landscape as an effort to increase value, improved user experience and operational efficiencies. |
| **Implications:*** Rationalise supply chain processes and tools to optimise quality, coordination of care and engagement with participants/patients (e.g. ID cards, training materials etc)
* Eliminate data redundancies to reduce or prevent medical errors
* Rationalise the application landscape e.g. SAP instances
* Reduce manual interfaces; embrace automation
* Increase integration between operational and enterprise systems
* Leverage Software as a Service or Platform as a Service when appropriate to assist with demand management and operational efficiencies
* Create Centres of Excellence (CoEs) and governance structures to manage application development and portfolio demand
* Justify make versus buy decisions with the goal of reducing administrative costs
* Leveraging outsourcing models where appropriate for cost advantages
* Investigate the benefits and limitations of commercially available versus proprietary solutions
* Implement formal change management to assist with changes brought on by new technologies. Some stakeholders might be resistant to new ways of collecting and processing healthcare information through these new applications and technologies (e.g. clinician order-entry systems, etc.)
 |

# Security - Architectural Principles

|  |
| --- |
| SP #1 Data Security |
| Data shall be protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. |
| **Rationale** The sharing of information and the release of information via relevant legislation must be balanced against the need to restrict availability of classified, proprietary, and sensitive information.  |
| **Implications** * In order to adequately provide access while maintaining the security of data, data security requirements must be identified and developed at a data level, not at an application level.
* Data should be assigned a classification in accordance with HSE Policy by the appropriate Data Trustee.
* Data should be handled and processed in accordance with HSE Policy.
* Access to data is ascribed by the appropriate Data Trustee.
 |

|  |
| --- |
| SP #2 Privacy and Security Safeguards |
| Appropriate technical and organisational controls must be implemented to protect data and keep it confidential.  |
| **Rationale**The privacy and security of data is everyone’s responsibility. Data protection legislation requires organisations that process personal data to ensure they maintain the security and privacy of this data. It is necessary to have policies and security safeguards implemented to protect health information whether stored on paper or electronically. |
| **Implications:**Implementation of the following controls should be considered:* Access controls – Access to information should be on a need to know basis, role based access.
* Technical controls – the implementation of robust IT security controls such as password authentication, encryption, anti-malware software, patch management, firewalls, IDS, mobile device management, secure code reviews etc.
* Auditing – Audit systems should be enabled by default.
* Incident detection & response – continuous monitoring in order to indentify and respond to threats.
 |

|  |
| --- |
| SP #3 Security Design |
| Architectures should employ security measures to ensure integrity, confidentiality and availability of IT services and applications. Security needs to be designed into the architecture in a scalable and efficient manner. The security architecture design should follow a modular design where the overall technology infrastructure is divided into functional layers / modules.  |
| **Rationale**The layered / modular approach allows the architecture to address the security relationship between the various functional blocks of the infrastructure and, it permits designers to evaluate and implement security on a module-by-module basis, instead of attempting to complete the architecture in a single phase.  |
| **Implications:**Comprehensive published security standards for each layer / module of the IT architecture is a pre-requisite for all security designs.  |

|  |
| --- |
| SP #4 Least Privilege  |
| Each system or application must incorporate the principle of least privilege thus the baseline is the bare minimum privileges necessary to perform functions, actions and access. |
| **Rationale:** The baseline for functions, actions and access is the minimum required to complete the task, thus protecting users and the data they are using from inadvertent errors, exploitation or attempts at deliberate misuse.Adhering to the principle of least privilege reduces the risk of attackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.  |
| **Implications:** * Part of solution design should ensure the principle of least privilege is incorporated into the solution to enhance the protection of data and functionality from faults and malicious behaviour.
* Contains compromises to their area of origin, stopping them from spreading.
* The scope of audits can be reduced dramatically thus ensuring the efficient use of scarce resources.
* Users, clients, business and the enterprise are better protected.
 |

# Technology - Architecture Principles

|  |
| --- |
| TP #1 Requirements based Change |
| Changes to applications and technology are in response to the business or legislative needs of the Enterprise. |
| **Rationale:*** The purpose of this principle is to keep us focused on business, not technology needs — responsive change management is also a business need.
* This principle will foster an atmosphere where the technology environment changes in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the technology support (delivery of eHealth/the transaction of business) — is the basis for any proposed change.
* Unintended effects on business/delivery of care due to IT changes will be minimized.
* A change in technology may provide an opportunity to improve the business process and, hence, change business needs.
* A change in technology may provide an opportunity to improve security and, hence, change or improve an existing business need.
* A change in technology may ensure the maintainability of a service supporting a business function and, hence, support an existing business need.
* The only exception to this principle is technology driven change to support modernisation of aging technology platforms. See TP #2 Technology Based Change.
 |
| **Implications:*** There is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.
* Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.
* Change management processes will be developed or modified and implemented to conform to this principle.
* This principle may conflict with TP #4 Responsive Change Management. We must ensure the requirements documentation process does not hinder responsive change management to meet legitimate business needs.
* This is one of four closely-related principles regarding change: TP #1 Requirements-Based Change; TP #2 Technology-Based Change, TP #3 Changes Are Planned and TP #4 Responsive Change Management. These four principles work together to ensure that change is well-managed.
 |

|  |
| --- |
| TP #2 Technology Based Change |
| Changes to applications and technology are only in response to business needs of the Enterprise, except in the case of modernization of aging technology platforms, or research & development projects that are evaluating new technologies or approaches. |
| **Rationale:**Modernisation of an aging technology platform should ensure the maintainability of a service supporting a business function and, support conformance to IT enterprise standards. |
| **Implications:*** Changes in technology will follow full examination of the proposed changes using the enterprise architecture.
* This is one of four closely-related principles regarding change: TP #1 Requirements-Based Change; TP #2 Technology-Based Change, TP #3 Changes Are Planned and TP #4 Responsive Change Management. These four principles work together to ensure that change is well-managed.
* There is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.
 |

|  |
| --- |
| TP #3 Changes are Planned |
| Changes to the Enterprise Technology Environment are planned and communicated. |
| **Rationale:**Planning changes provides a greater guarantee of successful and stable implementation. When changes are planned and communicated, conflicts are avoided and appropriate resources are made available. |
| **Implications:*** All relevant stakeholders will have to be involved in change management.
* IT should be aware of business plans that require changes to the Enterprise information environment.
* The implication is that there is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.
* A process should be developed for managing and implementing change that provides assurance of success.
* This is one of four closely-related principles regarding change: TP #1 Requirements-Based Change; TP #2 Technology-Based Change, TP #3 Changes Are Planned and TP #4 Responsive Change Management. These four principles work together to ensure that change is well-managed.
 |

|  |
| --- |
| TP #4 Responsive Change Management |
| Changes to the enterprise information environment are implemented in a timely manner. |
| **Rationale:**The implication is that there is an education task to ensure that all agencies understand the relationships between the need for change, planning changes, and responsiveness of change management.If people are expected to work within the enterprise environment, that information environment must be responsive to their needs. |
| **Implications:*** Processes should be developed for managing and implementing change that does not create unnecessary delays.
* If changes are made, architectures should be kept updated strictly in line with the architecture processes, policies and procedures.
* This is one of four closely-related principles regarding change: TP #1 Requirements-Based Change; TP #2 Technology-Based Change, TP #3 Changes Are Planned and TP #4 Responsive Change Management. These four principles work together to ensure that change is well-managed.
 |

|  |
| --- |
| TP #5 Control Technical Diversity |
| Technological diversity is controlled to minimise the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments. |
| **Rationale:*** There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments.
* There are further costs incurred to keep multiple processor constructs interconnected and maintained. Limiting the number of supported components will simplify maintainability and reduce costs.
* Common technology across the enterprise brings the benefits of economies of scale to the enterprise.
* Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.
 |
| **Implications:*** Policies, procedures and standards that govern acquisition of technology must be tied directly to this principle.
* Technology choices will be constrained by choices available within the technology blueprint.
* Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.
* Technology blueprints should be developed by the supplier or HSE architect by agreement with the Architecture Review Board.
* Technology blueprints should be changed when compatibility with the current infrastructure, improvement in operational efficiency, or required capability has been demonstrated.
 |

|  |
| --- |
| TP #6 Decoupling the Distribution Channels |
| Enable organisational agility by decoupling the distribution channels from operating systems. |
| **Rationale:**To provide the ability to respond to a rapidly evolving healthcare market (e.g. M&A, divestures, consolidation, regulatory changes) by deploying service based architecture that simplifies integration with legacy systems, new applications and commercial off-the-shelf (COTS) software. |
| **Implications:*** Define an integrated architecture that embraces new digital media, including mobile, social and cloud data sources with variable structures and unstructured data models.
* Deploy a common enterprise data model.
* Implement a shared interface approach to monitor, manage and securely deliver governance requirements while reducing the cost and time to release new services
 |

|  |
| --- |
| TP #7 Enterprise-accessible On-demand Services |
| Employ an architecture that uses enterprise-accessible on-demand services. |
| **Rationale:*** On-demand services are essential for IT to contribute to and even drive strategic goals of the business through efficiency, agility, and reliability.
* Cloud computing can meet these demands because it transforms the way the health service consumes and delivers IT services.
* Cloud is about transformation, and on-demand services are a key enabler, supporting improved efficiency, agility, and reliability as the IT organization transforms from a reactive provider, to an engaged service broker, and finally a strategic partner for the business.
* On-demand services deliver increased efficiency through the shift from interactive, manual processes to automated, self-service deployment of resources. Improved agility is the result of reducing the delay and cycle time from an identified business need to delivering the required IT resources.
* Reliability comes from a more standardized set of services and tools, with well-defined and -executed service-level agreements between IT and the business.
 |
| **Implications:*** Enable on-demand access to IT services through a cloud service catalogue and self-service portal.
* Leverage cloud models for non-critical business/IT functions.
* Legislation regarding data access, storage and sovereignty should be respected.
* Make cloud services available on mobile platforms.
* Shift to ‘cloud’ as an overarching paradigm that seeks value from SaaS, PaaS, IaaS and other as-as service technologies and help determine how they can be best become a part of the OoCIO’s delivery mechanisms.
* Apply the use of hybrid cloud capabilities to combine the best of cloud’s elements, mixing on premise and off premise IT and integrated cloud with legacy systems and traditional software. Use of hybrid/public cloud extensively will require changes to the underlying IT is managed and sourced.
* Select a cloud first based software services approach that must closely align to existing business requirements. Evaluate vendors on their maturity, viability, ability and credibility.
* Develop in-house architecture with a modular component to ease integration with cloud based systems.
* Ensure reliable public-private cloud connectivity with robust network architecture.
* Promote scalability, availability, redundancy and disaster recovery of applications, especially for key customer-facing applications that must be guaranteed to be up and running especially during peak periods.
 |

|  |
| --- |
| TP #8 Resiliency and Availability |
| All technology components including data centre physical and virtual infrastructure are designed in such a way as to avoid any single point of failure. A standardised, consolidated infrastructure is used which helps to minimize risk, maximize network, storage and compute availability and support business continuity. |
| **Rationale:*** The Enterprise technology investment supports mission-critical patient/end user services, and resiliency and availability must be designed in at inception.
* Implementation of this capability will be dependent upon a risk assessment or business need for each system.
 |
| **Implications:*** Resiliency and availability requirements should be identified at the time of design.
* Applications must be assessed for criticality and impact on service delivery, in order to determine what level of resiliency and availability is required.
* This is linked to the principle BP #6 Business Continuity.
 |

|  |
| --- |
| TP #9 Scalability and Modularity |
| Application architectures should be scalable, flexible and modular to meet ongoing and dynamic business growth. |
| **Rationale:**Application architectures should support a variety of legacy and emerging systems and technologies. |
| **Implications:**Standard scalability design patterns for each architectural domain should be published and periodically updated. |

|  |
| --- |
| TP #10 Industry Standard Technology |
| Proposed architectures and technologies must support industry standards, and avoid proprietary technologies and interfaces unless specifically required for specialised applications or business needs. |
| **Rationale:**Industry standard technology and interfaces will reduce development cost, integration costs, and the time required to implement new functionality. |
| **Implications:*** Technology standards should be published and freely available to external parties.
* All standards are maintained in the [Design Authority Standards Catalogue](http://www.ehealthireland.ie/Library/Document-Library/Standards-Catalogue-v1_0.pdf).
 |

|  |
| --- |
| TP #11 Technology Will Not Be Deployed Before Its Time |
| The technology may be leading edge, but will certainly be proven in production before being deployed in the field. |
| **Rationale**: Ensuring timely deployment of technology will minimise risk in delivery, minimize risk in operations and maximize user perceived quality. |
| **Implications:*** Appropriate testing is conducted prior to live deployment.
* Working with the Architecture Review Board and Design Authority to ensure time of deployment is consistent with Enterprise Strategic Technology Viewpoint.
 |

# Information - Architecture Principles

|  |
| --- |
| IP #1 Data is an Asset |
| Data is an asset that has value to the enterprise and is managed accordingly. |
| **Rationale:** * Data is a valuable corporate resource; it has real measurable value.
* The purpose of data is to aid decision making.
* Accurate, timely data is critical to accurate, timely decisions.
* Most corporate assets are carefully managed, and data is no exception.
 |
| **Implications:*** Data must be carefully managed to ensure we know where it is, can rely on its accuracy, and can obtain it when and where we need it.
* This is one of the three closely related principles regarding data; data is an asset; data is shared, and data is easily accessible. There is an education task to ensure that all organisations within the enterprise understand the relationship between value of data, sharing of data and accessibility of data.
* There must be a cultural transition from ‘data ownership’ thinking to ‘data stewardship’ thinking.
* The role of data steward is critical because obsolete, incorrect or inconsistent data could be passed to the enterprise personnel and adversely affect decisions across the enterprise.
* Procedures should be developed and used to prevent and correct errors in the information and to improve on those processes that produce flawed or incomplete information.
* Data quality will need to be measured and steps taken to improve data quality.
* Since data is an asset of value to the entire enterprise, data stewards accountable for properly managing the data must be assigned at an enterprise level.
 |

|  |
| --- |
| IP #2 Data is Sharable Across & Between Institutions  |
| Users have access to data necessary to perform their duties; therefore data is shared across enterprise functions and organisations in accordance with legislation. |
| **Rationale:*** Timely access to accurate data is essential for improving the quality and efficiency of enterprise decision making.
* It is less costly to maintain timely, accurate data in a single application and then share it, then to maintain duplicate data in multiple applications.
* The speed of data collection, creation, transfer and assimilation is driven by the ability of the organisation to efficiently share islands of data across the organisation.
* Electronically shared quality data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.
 |
| **Implications:*** To enable data sharing, a common set of policies, procedures and standards governing data management must be developed and applied.
* For the short term, to preserve the significant investment in legacy systems, wherever possible, investment in software capable of migrating legacy system data into a shared environment should be adhered to.
* Need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing meta data to make it accessible.
* For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers/vendors to ensure that the data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by all new applications.
* Under no circumstances should the data sharing principle cause confidential data to be compromised or disregard relevant legislation or agreed best practice.
* Shared data will become the enterprise-wide ‘virtual single source’ of data.
 |

|  |
| --- |
| IP #3 Data is Accessible  |
| Data should be accessible for all users to perform their work. Users should have access to local and core national records relevant to their role and within legislative parameters. |
| **Rationale**: Wide access to data leads to efficiency and effectiveness in decision making, and affords timely response to information requests and service delivery |
| **Implications:*** User accessibility and data traceability are part of solution design.
* Implementing this principle will require data interconnectivity between relevant systems to ensure appropriate data is accessible in a timely manner and in the location it is needed.
 |

|  |
| --- |
| IP #4 Information is Everyone’s Business |
| All organizations in the enterprise participate in information management decisions needed to accomplish business objectives. |
| **Rationale:*** Information users are key stakeholders or customers, in the application of technology to address a business need.
* In order to ensure information management is aligned with the business, all organisations in the enterprise must be involved in all aspects of the information environment.
* The business experts from across the enterprise and the technical staff responsible for developing and sustaining the information environment need to come together as a team and jointly define the goals and objectives of IT provisioned information.
 |
| **Implications:*** To operate as a team, every stakeholder, or customer, will need to accept responsibility for developing the information environment
* Commitment of resources will be required to implement this principle
* Everyone must be responsible for meeting legislative requirements and data standards levied upon the data for which the person is accountable
* Information should be captured electronically once, contemporaneously if possible and immediately validated as close to the source as possible.
* Information Governance and associated Quality Control measures must be implemented to ensure the availability and integrity of the data.
 |

|  |
| --- |
| IP #5 Common Vocabulary and Data Definitions |
| Data is defined consistently throughout the enterprise, and the definitions are understandable and available to all users. |
| **Rationale:*** The data that will be used in the development of applications must have a common definition throughout the enterprise to enable sharing of data.
* A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.
 |
| **Implications:** * The enterprise must establish a common vocabulary for the business. The definitions will be used uniformly throughout the enterprise via the National Data Dictionary.
* Whenever a new data definition is required, the definition effort will be co-ordinated and reconciled with the corporate ‘glossary’ of data descriptions. The business domain owner will be responsible for providing this co-ordination.
* Ambiguities resulting from multiple parochial definitions of data must give way to accepted enterprise-wide definitions and understanding.
* Multiple data standardisation initiatives must be carefully co-ordinated.
 |

|  |
| --- |
| IP #6 Data Trustee |
| Each data element has a trustee accountable for data quality. |
| **Rationale:**One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the enterprise. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only the data trustee makes decisions about the content of data. Since data can lose its integrity when it is entered multiple times, the data trustee will have sole responsibility for data entry which eliminates redundant human effort and data storage resources. |
| **Implications:** * Real trusteeship dissolves the data "ownership" issues and allows the data to be available to meet all users' needs. This implies that a cultural change from data "ownership" to data "trusteeship" may be required.
* The data trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable.
* It is essential that the trustee has the ability to provide user confidence in the data based upon attributes such as "data source".
* It is essential to identify the true source of the data in order that the data authority can be assigned this trustee responsibility. This does not mean that classified sources will be revealed nor does it mean the source will be the trustee.
* Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data.

As a result of sharing data across the enterprise, the trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, subsequently, must then recognize the importance of this trusteeship responsibility. |

# Interoperability - Architectural Principles

|  |
| --- |
| IOP #1 Technical and Syntactic Interoperability |
| Solutions should conform to defined standards that provide interoperability for technology, applications and information. |
| **Rationale** Standards help ensure consistency, thus improving the ability to manage systems and improve user satisfaction and project existing IT investments, thus maximising return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products e.g. facilitate sharing of Clinical Documents nationally and internationally through the use of IHE Profiles.  |
| **Implications*** Interoperability standards and industry standards must be followed unless there is a compelling business reason to implement a non-standard solution.
* Adopt a process for setting standards, renewing and revising them periodically, and for granting exceptions via the Architectural Review Board or equivalent Board.
* Existing IT platforms must be identified and documented.
* Adopt a standardised metadata registry framework that enables participant/patient records to be used/assembled for different purposes by different care providers
* Interoperability testing of eHealth Information systems will be conducted via the HSE EA Test Harness  in each of the following areas as applicable to the use case:
1. validation and conformance of messages and documents produced to agreed terminologies, profiles and standards,
2. information exchange between systems consistent with interoperability specifications,
3. adherence to  agreed security protocols,
4. simulation of system against IHE profiles/actors.
 |

|  |
| --- |
| IOP #2 Semantic Interoperability |
| Semantic interoperability is achieved through the use of SNOMED CT in all clinical information systems. |
| **Rationale:**Semantic interoperability provides interoperability at the highest level, which is the ability of two or more systems or elements to exchange information and to use the information that has been exchanged. Semantic interoperability takes advantage of both the structuring of the data exchange and the codification of the data including vocabulary so that the receiving information technology systems can interpret the data. |
| **Implications:*** All applications will include a design that will make SNOMED CT available to clinical teams
* All suppliers/vendors will have the capacity to upload the 6 monthly RF2 files from SNOMED International
* SNOMED CT, National release Centre will advise and assist clinical teams to define reference and sub sets

SNOMED International will supply all mappings to other terminologies and classifications such as* ICPC2,
* LOINC,
* DICOM,
* ICD-10,
* ICD-11,
* Orphanet codes
* ICD-0,

and all other mapping that will be available for use in any EHR, these  may  be used for data analysis and aggregating data for statistical purposes. The national Release Centre, will through the managed service give capacity to create an Irish extension of SNOMED CT, which will include the capacity to create and edit content to include all clinical concepts and terms as well as drug content. |

# Appendix 1 – EA Principles Management Process



