The European Institute For Innovation Thr~ugh Health Data

GOVERNANCE & CODES OF PRACTICE

Peter Singleton
Cambridge Health Informatics Ltd

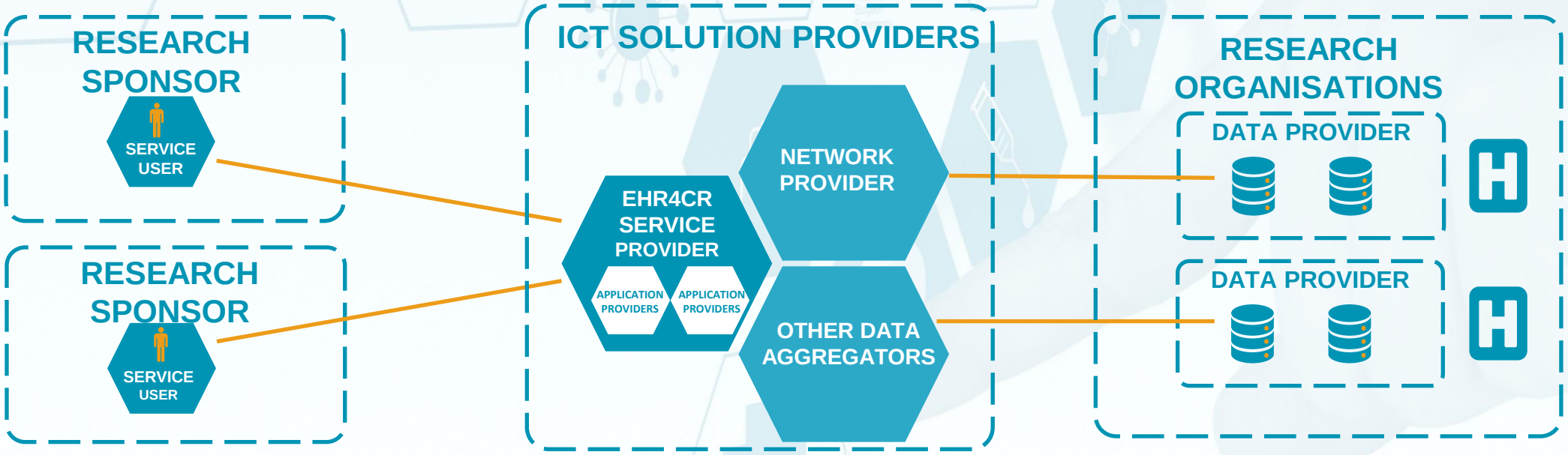
Ensuring the trustworthy reuse of health data for research – EHR4CR approach

Educate and train research and ICT staff

Accredit staff and organisations

Certify service providers and EHR systems

Oversee and audit governance & security

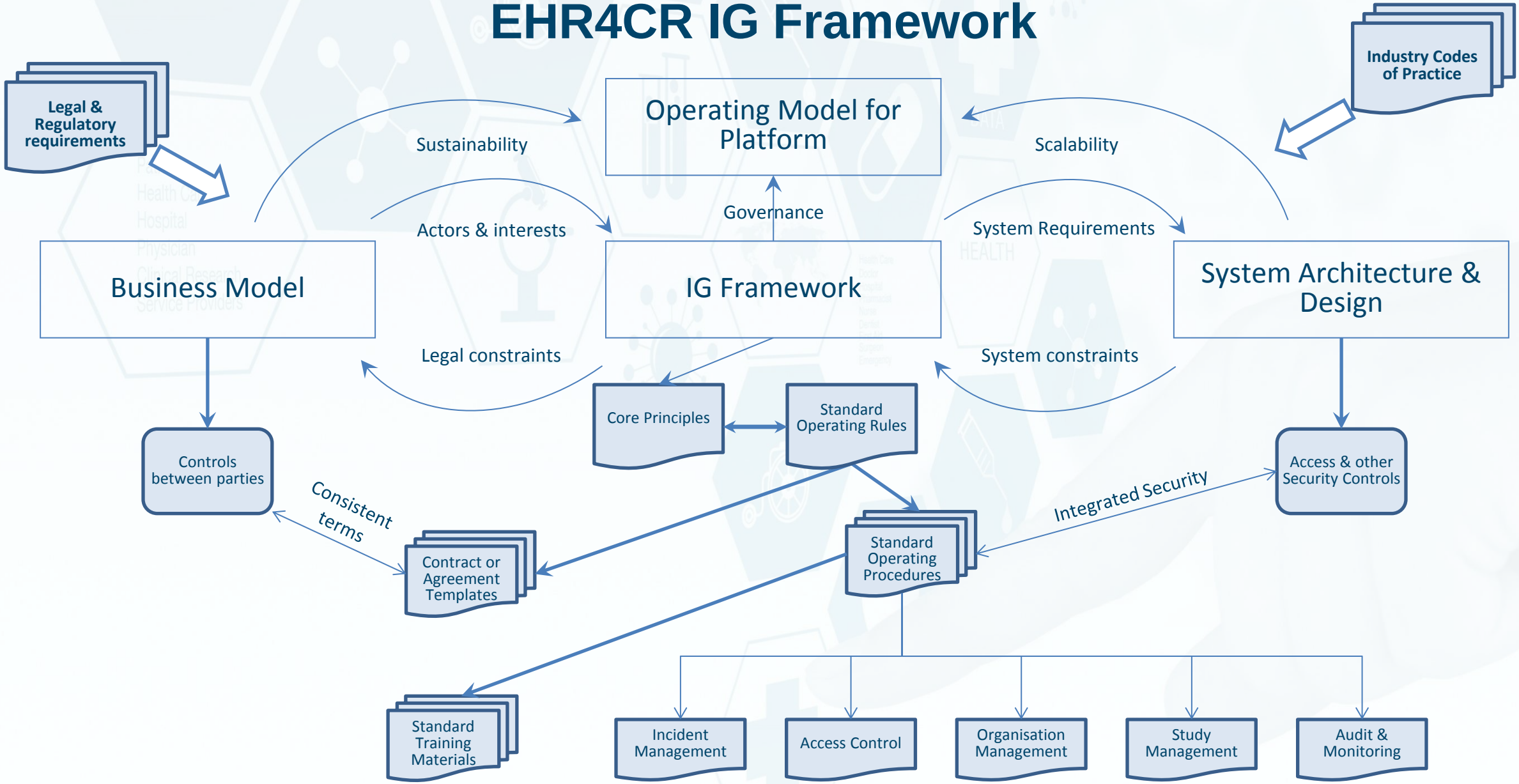


Governance controls are vital to safeguard data

Ensures consistent application of principles and legal requirements and to aid adoption of best practice

- High-level Principles – detailed in:
- Standard Operating Rules – elaborated in:
- Standard Operating Procedure templates
- Staff competence checklist for hospital, research, & service provider staff
- Code of practice on data management and privacy protection when using the platform
- Standard training materials
- Quality-labelling criteria for the platform and services, including components deployed at hospitals

EHR4CR IG Framework



Privacy protection is delivered on multiple levels

- Personal data is only processed by original data controller
- The Clinical Data Warehouse holds only pseudonymised data
- The EHR4CR Platform only handles aggregate data, with additional protections
- Role-based access controls to limit access to aggregate data
- Extensive audit trails with reporting
- Integration of organisational controls (e.g. Operating Procedures) with system functionality

EHR4CR Core Principles:

- Data minimisation
- Data exchange protocols
- Strong Information Security
- Risk management controls
- Appropriate access control facilities
- Adequate Audit trails
- Ensure appropriate use
- Operational effectiveness
- Effective Information Governance
- Proper Training & Resourcing
- Clarity of authority
- Effective enforcement
- Legal conformance

EHR4CR Governance Principles

Introduction

These principles cover the appropriate operation of the EHR4CR platform, services, tools and applications by various parties:

- Research Centres (RCs) carrying out feasibility studies and commissioning clinical trials.
- Recruitment Sites/Data Providers, usually hospitals, which make their data available for distributed queries to determine possible numbers of patients matching the eligibility criteria of tentative trial protocols with the aim of participating in subsequently commissioned clinical trials, and make use of supplied applications and services to identify potentially eligible patients within their site.
- Service Providers (SPs) which provide the infrastructure, tools, applications and services to allow the exchange of distributed queries and aggregate statistics between Research Centres and Recruitment Sites, and supply applications for use within a Recruitment Site to locally identify potentially eligible patients.
- The *European Institute For Innovation Through Health Data* (i~HD) which provides oversight and standards for the appropriate governance of the overall Platform

These principles are a high-level articulation of requirements which are further codified in other documents as rules to be followed and standard operating procedures to be implemented.

The principles are grouped as those relating to the design of systems, the operational procedures, and organisational structures.

Systems

Data minimisation: only minimum form of information should be used at each stage of processing – *to support subsequent processing, particularly avoiding identifiers or partial identifiers; obsolete data should be removed from repositories as soon as is practicable*

Data Interchange standards: only i~HD approved dictionaries or formats should be used for communication of queries and results across the EHR4CR platform – *to ensure consistent operations and avoid accidental exposure of personal data*

Strong Information Security: information must be held securely against unauthorised access, corruption, or loss – *and therefore requiring adequate identification and authentication of authorised users*

Appropriate access control facilities: to assign access privileges to identified users in a controlled manner – *privileges should only be assigned where needed and revoked as soon as the user no longer has a legitimate role within the organisation to use the services, and should be fine-grained enough to limit privacy risks without becoming burdensome or unworkable*

Risk management controls: Systems should provide configurable options to prevent or limit data-flows – to support gradual phasing in or out of facilities and also to support suspension of processing at specific points, whether for maintenance, investigation of any incident, or to allow another actor to limit their risks

Adequate Audit trails: systems should record sufficient user activity and information flow detail to permit appropriate checks on use and to support possible forensic investigations – *particular consideration is needed where user activity may extend across multiple systems, so that a consistent end-to-end view is available where necessary; systems need to provide reporting mechanisms to allow appropriate users make effective use of the audit trails available.*

EHR4CR Principles – main objectives

- Building on legal requirements
- Basis for building and establishing trust between partners
- Provide solid, though flexible, foundations for initial operations
- Articulate the level of controls to data providers, regulators, patients, and the public at large
- Guide further development of standard operating rules and procedures
- Provide a governance framework for other EU healthcare projects in the future