hisSA health information system Security Assessment

ANALYSIS METHODOLOGY AND CLASSIFICATION MODEL FOR THE SECURITY IN HEALTHCARE INFORMATION SYSTEMS

BASED ON A HEALTH TECHNOLOGY ASSESSMENT APPROACH

UNIVERSITÀ CATTOLICA del Sacro Cuore
ALTEMS
ALTA SCUOLA DI ECONOMIA E MANAGEMENT DEI SISTEMI SANITARI

Ministero della Salute
DIREZIONE GENERALE della DIGITALIZZAZIONE, del SISTEMA INFORMATIVO SANITARIO e della STATISTICA

The healthcare information system

- is widely used in all processes of the healthcare organization, therefore has a direct and indirect influence on
  - → the health and conditions of the patient
  - → the effectiveness and optimization of the organization
- has a non marginal influence on the overall costs
- represents (should represent) a strategic instrument to manage and improve the organization and the quality of the services provided

- cannot (anymore) be considered as a –more or less homogeneous- mix of technologies and software, connected each other to solve individual, separated and contingent requirements
- must be planned, implemented, evaluated and managed on the basis of an integrated vision taking care both of the strategy of the organization and of the care, economic, ethical and legal aspects

Security in healthcare information system

Security, including aspects related to «privacy» regulation

is not a just technological issue, limited to individual sectors

but involves all aspects of the entire information system

… to ensure safety and quality of the medical activities and of the overall processes in the organization, in terms of

safety	to be protected from unlikely cause danger
protection	to be protected from malicious actions
resilience	to be able to operate in all situations
trust	to be able to operate with confidence and respecting regulations

In an overall scenario of appropriateness, effectiveness and economy of the services provided to the patient

risk factors....

.. from the patient's safety point of view
- Secure identification of the person
- Correctness of the therapy
- Error/incompleteness of communications between care givers
- Lapse
- Disregard relevant information
- Un-availability of relevant information
- Error in manual data-entry
- Prompt reaction according to situations

.. from the ethical and legal point of view
- Control to the access to information
- Traceability of the author of one action
- Identification of an information at a certain (past) moment
- Loss of information

.. from the regulatory point of view
- Compliance to privacy regulations
- Compliance to laws
- Compliance to funders requirements

.. from the economic point of view
- Increasing in the length of stay
- Un-necessary repetition of exams/activities
- Un-appropriateness of exams / activities
- Time and resources needed for executing activities
- Costs for insurances
- Legal costs also due to reimbursements

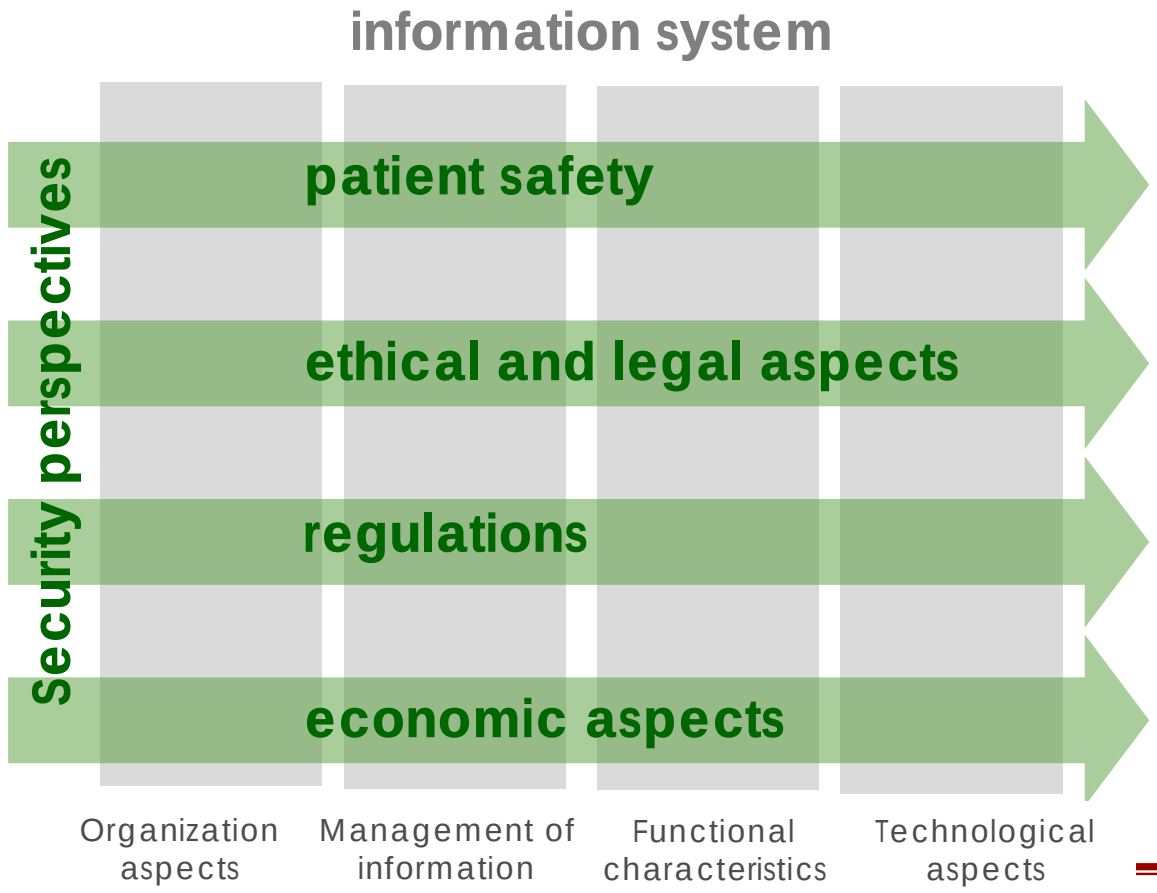
are influenced by the characteristics of the information system

with respect to information
- **Availability** of necessary information
- **Accessibility** to existing and relevant information
- **Proactivity** in highligting important information

with respect to processes
- **Completeness** of the support, without needing verbal and/or paper complements
- **Continuity** of the support, without needing to manually re-enter existing data

A multi-dimensional approach is necessary ...

in all phases, to ensure the respondennce of the information system to the overall requirements of security



Assessement

Strategy

Pianning

Adopting an «HTA approach»

ICT methodologies and standards

To represent characteristics of information systems by means of indicators homogeneous and independent from specific technologies and products

ISO 10746 – Open data processing – Reference model

- *Methodological framework for the analysis of the information system according to different complementary perspectives*

ISO 12967 – Health Informatics – Service Architecture

- *Reference model for the continuity of processes and the integration of data*

ISO 27001- Information security management

- *"requirements for an Information Security Management System (ISMS)."*

HiMSS EMR Adoption Model

- *Levels for characterising the HIS accoridng to the processes neing supported and the spreading of utilization*

+

Health Technology Assessment

To identify and evaluate aspects specifically relevant in the healthcare scenario

- Health-related aspects
- Clinical effectiveness
- Patients' perspective
- Direct and indirect economic aspects
- Organization aspects
- Ethical, social and cultural aspects
- Regulatory and legal aspects

hisSA health information system Security Assessment

The national survey on the characteristics of the healthcare information systems

On the basis of this «holistic» approach,

a survey has been carried out at national level

on some characteristics of the healthcare information systems

relevant to security and privacy issues

UNIVERSITÀ CATTOLICA del Sacro Cuore
ALTEMS
ALTA SCUOLA DI ECONOMIA E MANAGEMENT DEI SISTEMI SANITARI

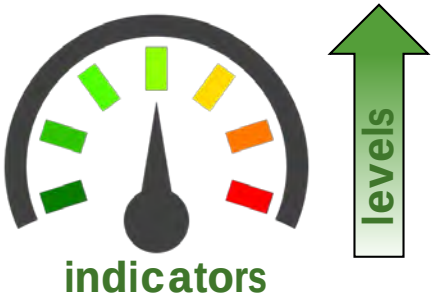
Ministero della Salute
DIREZIONE GENERALE della DIGITALIZZAZIONE, del SISTEMA INFORMATIVO SANITARIO e della STATISTICA

The national survey on the characteristics of healthcare information systems

Objectives

To get a homogeneous picture of the characteristics of the information systems of the Italian healthcare organizations, with respect to the security aspects, in such integrated vision

To define a methodology for the analysis and a model for the classification of information system through “security levels”, based on measurable indicators independent from specific technologies and products, usable also for planning and benchmarking purposes

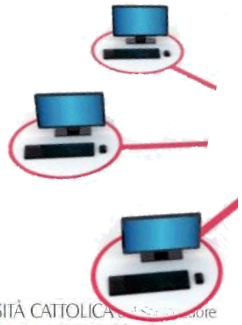


The working method

ICT + HTA

Questionnaire on various aspects of the healthcare information system

National survey with the collaboration of 46 HC organizations and 113 hopitals



Picture of the current situation by means of homogeneous parameters

Set of indicators and model for the classification of «levels of security» in HC information systems

The questionnaire on the characteristics of the healthcare information systems

Distributed to a sample of healthcare organizations throughout Italy, consisting of 40 items articulated in

Organization aspects

How is the organization structured with respect to the management of the aspects relating to safety, security and privacy in the information system

Structural aspects

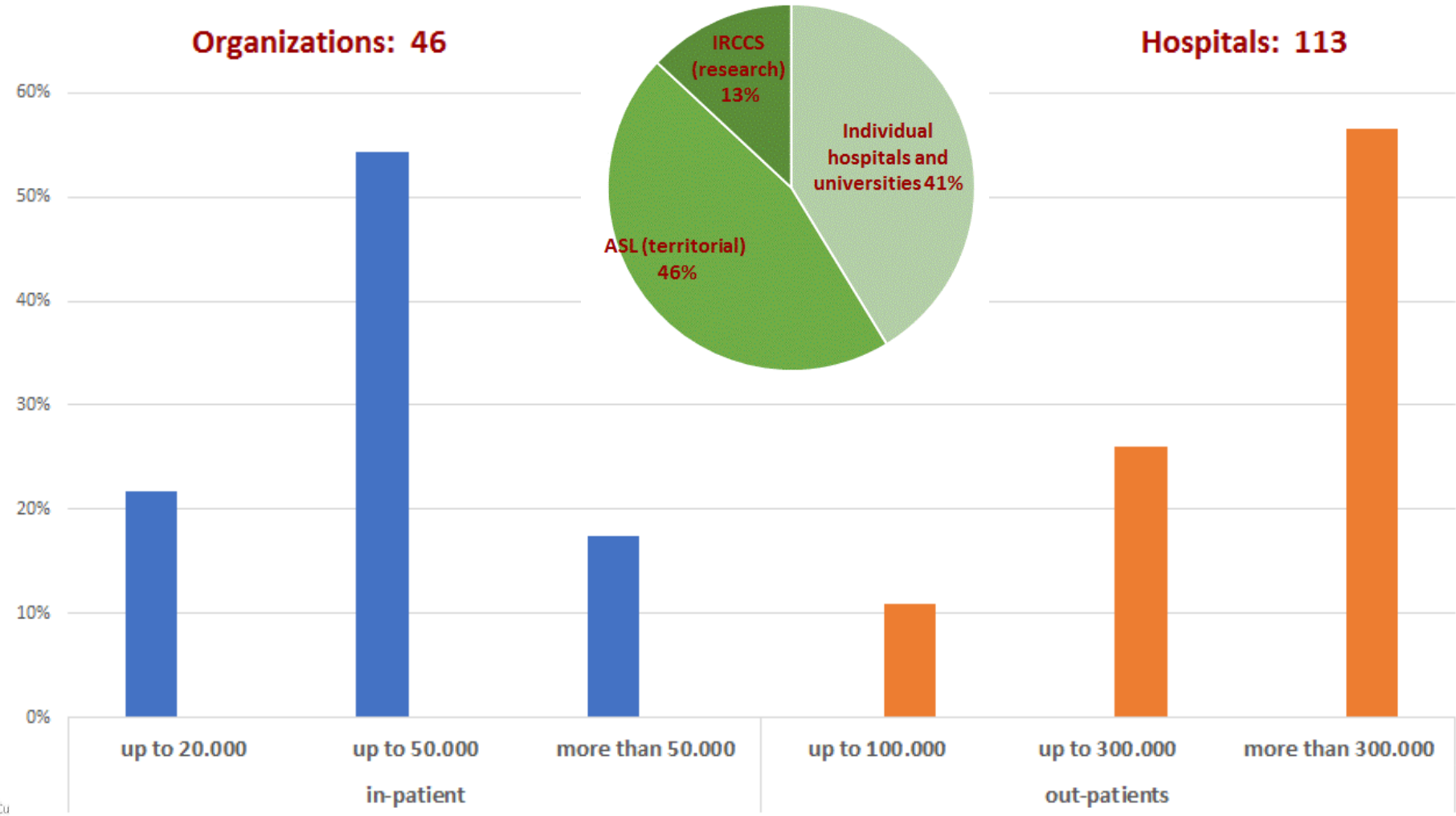
The architectural aspects of the overall system, of paramount and common relevance for all sectors and processes (e.g. availability and normalisation of information, access control and authorizations, privacy, etc.)

Implementation aspects

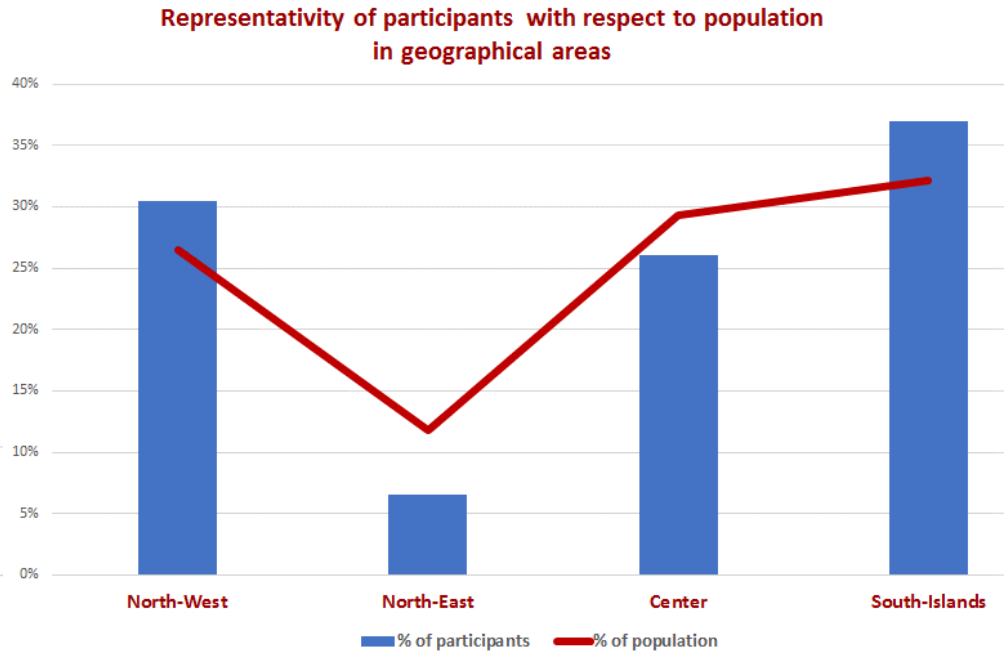
Which functionalities are actually implemented, how they operate and how much are they used in the daily activities

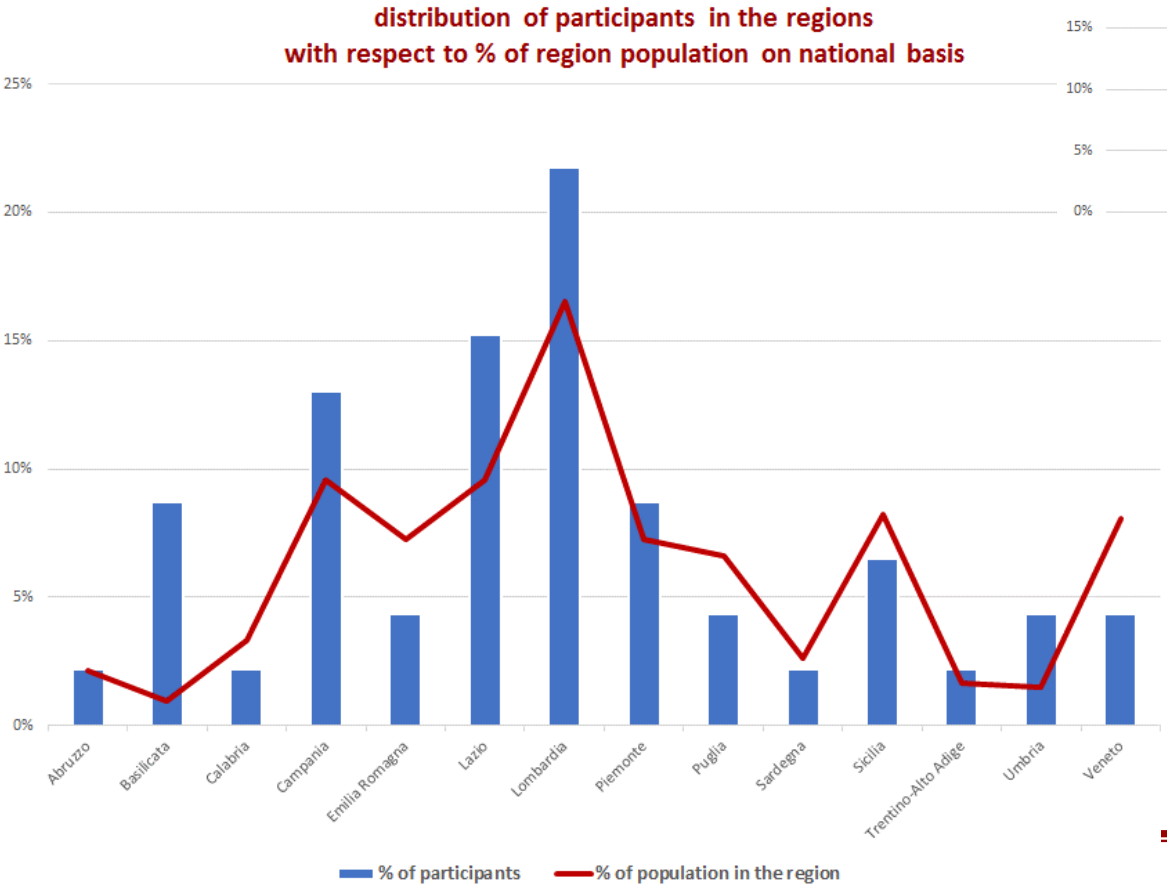
HC organizations participating to the survey

Type and volume of activities of the participants



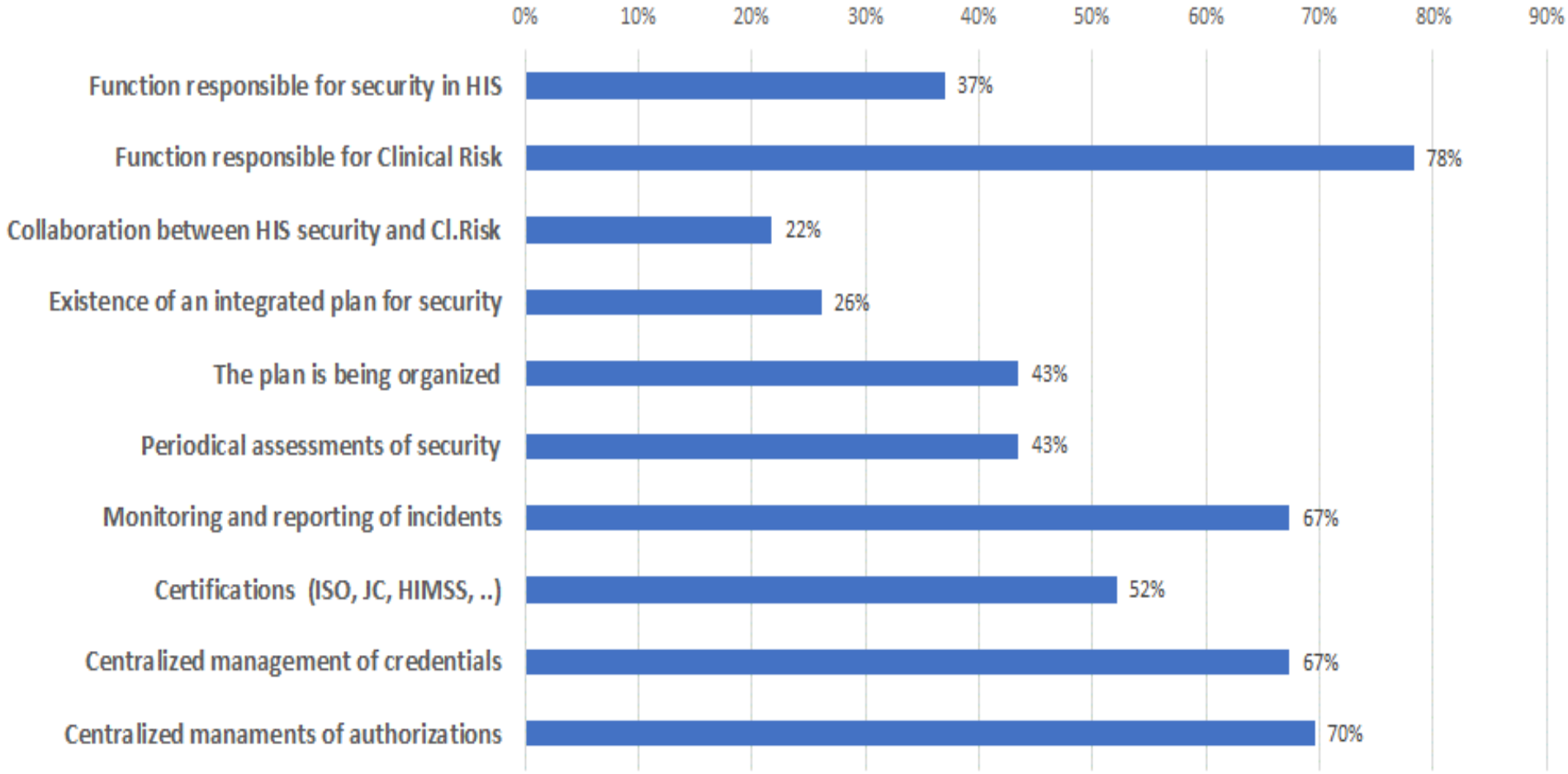
HC organizations participating to the survey



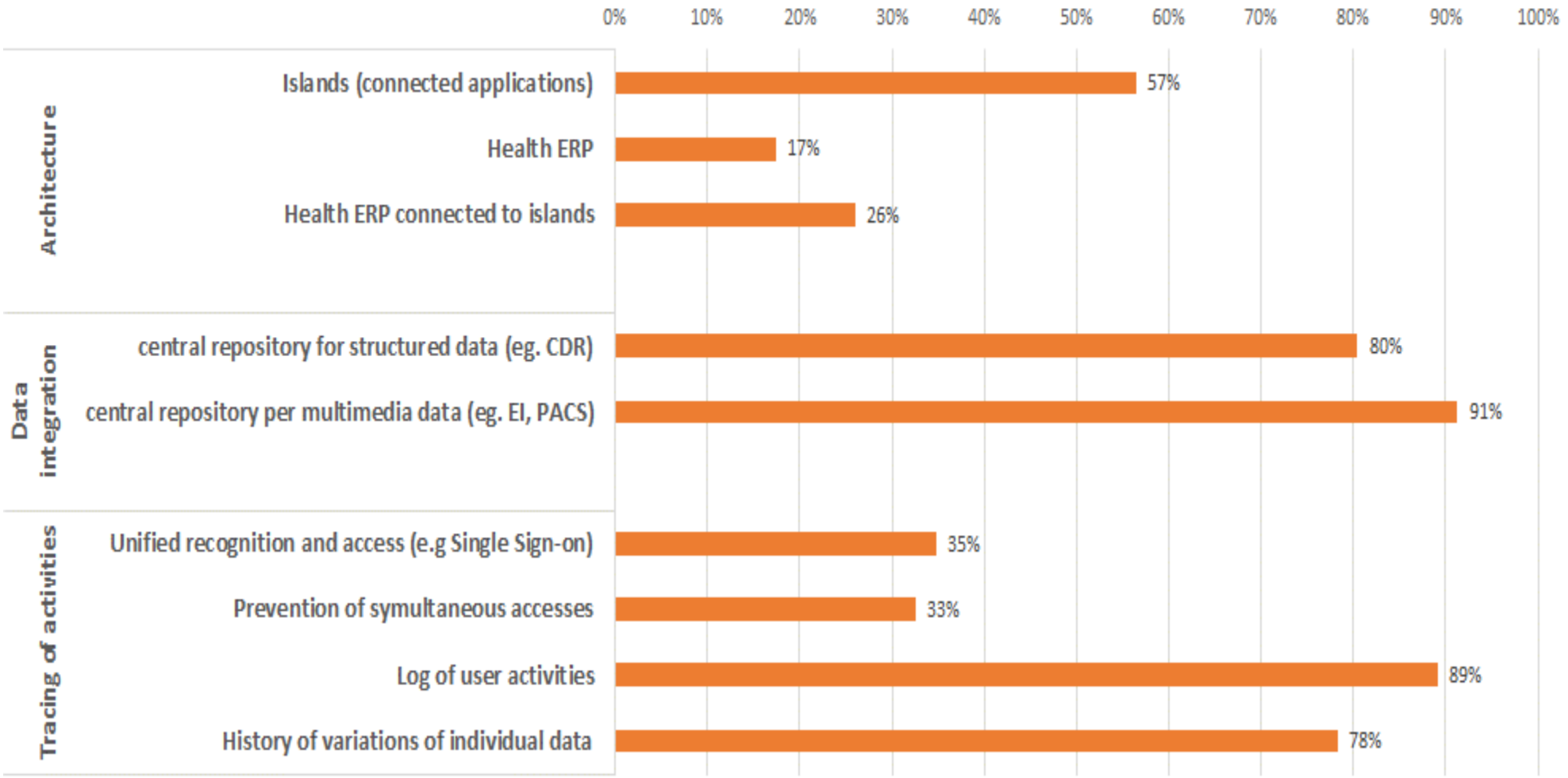


Survey results

Organization aspects

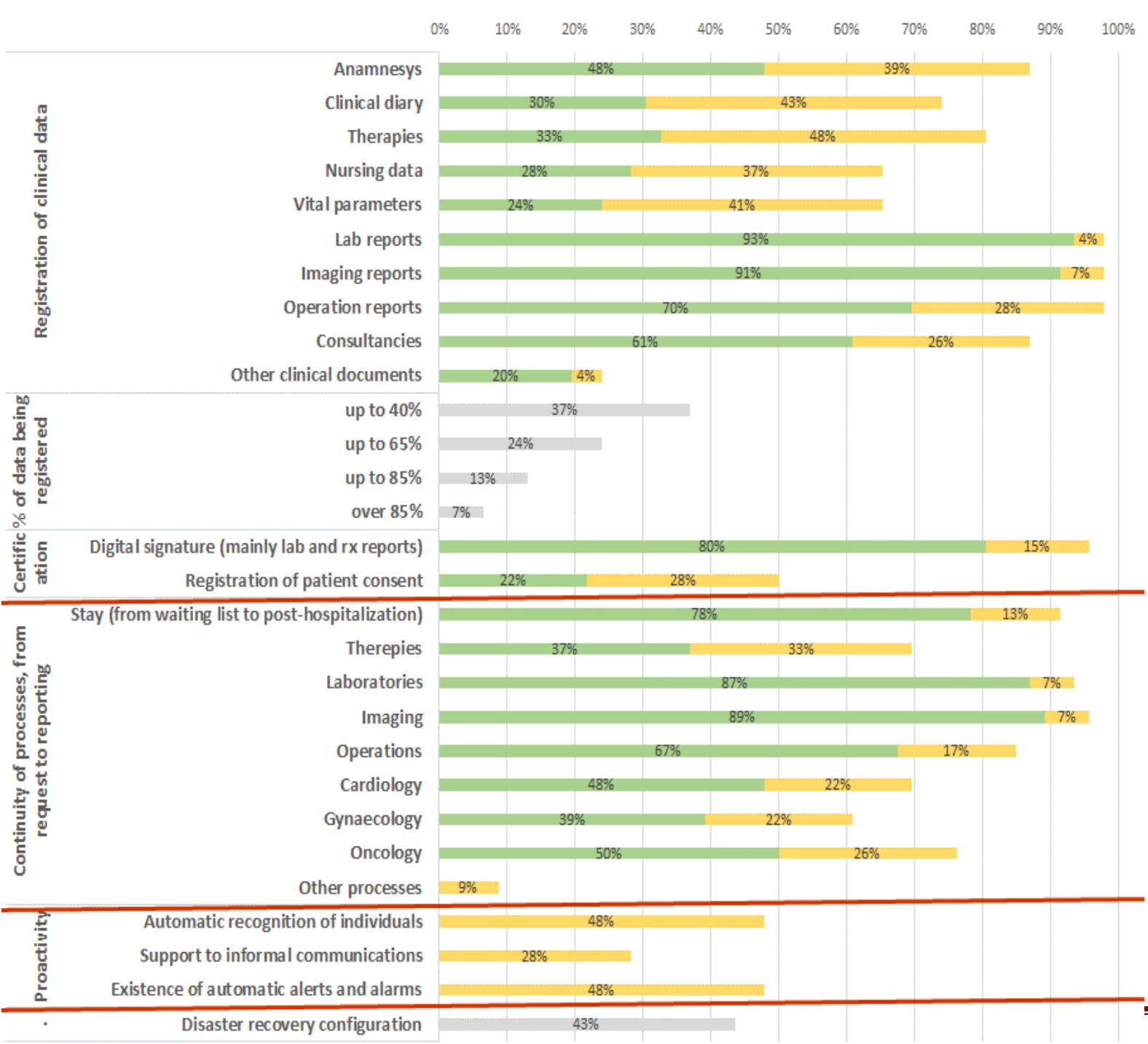


Structural aspects: architecture and characteristics relevant for the whole system



Survey results

Implementation aspects



The survey is still active

survey.sicurezza.his@gmail.com

Other organizations may participate by filling the on-line questionnaire

The indicators

Each organization has its own peculiarities, in relation to the medical disciplines with consequent requirements and characteristics

Not often the healthcare information system is used and evolves in the same way in all sectors

Simple binary indicators «ON / OFF» would be reductive and poorly representative of the actual situations

Indicators are therefore related to the «**relevance**» and to the «**dissemination**» of data and processes in the specific organization and clinical context

Relevance and dissemination indexes

relevance

Shows how much the measured aspect is relevant in the specific clinical and organization scenario, as a percentage of the total number of patients cared

eg.
Registering the anamnesis is very relevant, since it is done for all patients being cared; a chemotherapy process may be more or less relevant depending on the percentage of the total patients that receive this treatment

Relevance index % with respect to total cases (patients)

A	**High**	**over 70%**
B	**Medium**	**up to 70%**
C	**Low**	**up to 30%**

dissemination

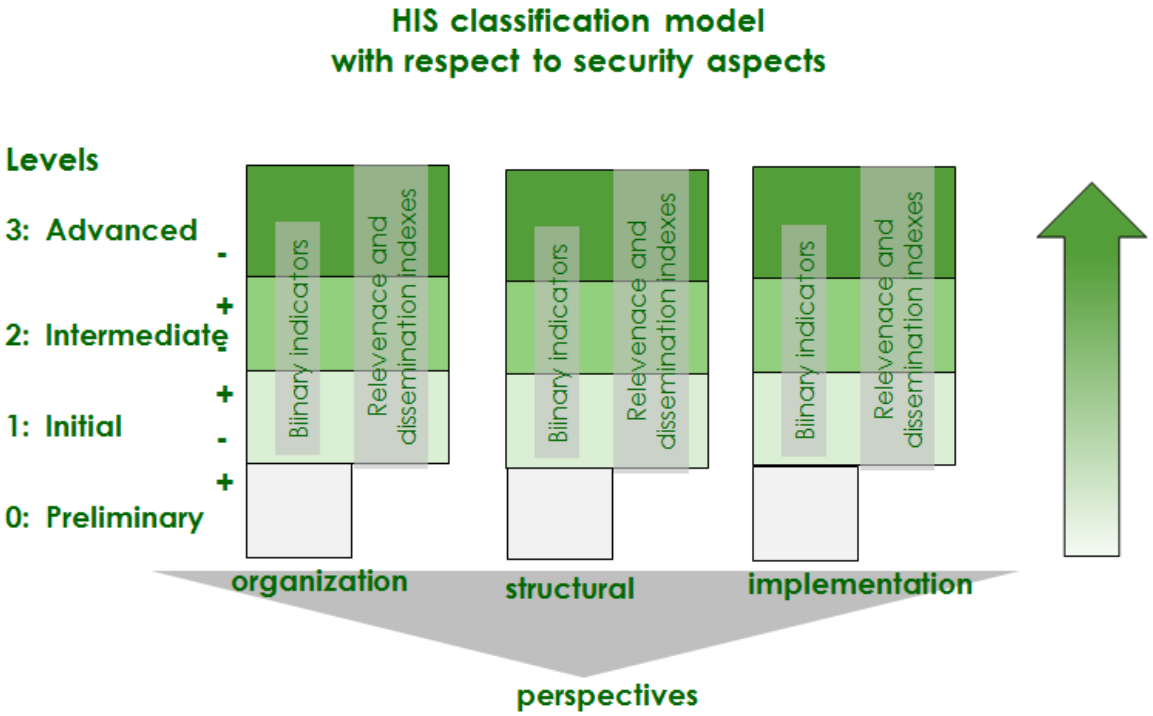
Shows how much the measured aspect is spread in the overall organization, as a percentage with respect to the total number of cases

eg.
The dissemination of computer-supported compilation of the operation report is the percentage of the operation reports registered with the HIS with respect to the total number of compiled operation reports

Dissemination index % with respect to total occurrences

A+	**Very high**	**over 85%**
A	**High**	**up to 85%**
B	**Medium**	**up to 65%**
C	**Low**	**up to 35%**
C-	**Very low**	**less than 10%**

Classification model
for the «*security level of the information system*»



«+» and «-» suffixes to take into account marginal differences with respect to the main characteristics of the level

Indicators related to dissemination and relevance indexes to take into account different requirements and characteristics of individual organizations

Relevance index % with respect to total cases (patients)

A	High	over 70%
B	Medium	up to 70%
C	Low	up to 30%

Dissemination index % with respect to total occurrences

A+	Very high	over 85%
A	High	up to 85%
B	Medium	up to 65%
C	Low	up to 35%
C-	Very low	less than 10%

Classification model
for the «*security level of the information system*»

Level 0 - Preliminary

Represents a scenario where the security aspects are still managed mainly at the sole technological level, on the basis of fragmented criteria and solutions, without an integrated vision in the organization.

Level 1 - Initial

Represents a scenario where the organization shows awareness of the requirements and has started addressing the security aspect according to an integrated vision. However, the necessary organization and structural aspects are still at an initial level, limited to a few processes and business sectors.

Classification model
for the «*security level of the information system*»

Level 2 - Intermediate

Represents a scenario where the organization shows to address security aspects according to a systematic and integrated approach.
The information system presents some structural features, capable to contribute to the security of information and processes, also by means of the centralization of data, functionalities and rules.
Operations are however not widely and homogeneously spread in all sector.

Level 3 - Advanced

Represents a scenario where the organization shows to address security aspects according to a systematic and integrated approach, taking into account also the aspects relating to clinical risk and evolving through an incremental approach with continuous improvements.
The information system presents consolidated structural features, capable to contribute to the security of information and processes, also by means of the centralization of data, functionalities and rules.
Operations are widely and homogeneously spread in the various sectors.
Proactive mechanisms are implemented to automatically highlight relevant information and risk situations.

Organization perspective

Organization perspective				Level			
				0	1	2	3
Existence of a function responsivle for the security in the HIS		YES/NO		NO	YES	YES	YES
Collaboration between security and clinical risk functions		YES/NO					YES
Definition and management of a integrated plan for security		YES/NO		NO			
Monitoring of HIS and registration of incidents		YES/NO			YES	YES	YES
Periodical assessments		YES/NO		NO		YES	SI
	frequency						1 / year
Management of a "white book" of possible improvements		YES/NO					YES
Centralized management of access credentials		YES/NO			YES	YES	YES
Centralized management of authorization profiles		YES/NO					YES
Adoption of common vocabularies and coding criteria		YES/NO				YES	SI
	High-relevant data	dissemination index				*medium*	*high*
	Medium-relevant data	dissemination index					*high*
	Low-relevant data	dissemination index					

Structural perspective

Structural perspective				Level			
				0	1	2	3
Existence of a central repository for structured data (eg. CDR)		YES/NO		NO	YES	YES	YES
Existence of a central repository for multimedia data (eg. EI)		YES/NO		NO		YES	YES
Existence of a centralised mechanism for accessing the system (eg Single Sign-On)		YES/NO		NO	YES	YES	YES
Existence of a centralised contect for the definition of authorization profiles		YES/NO				YES	YES
Log registration of users accesses and activities	concise	YES/NO				YES	
	detailed	YES/NO					YES
Registration of last variation of each record		YES/NO				YES	
Registration of full history of variations of each record		YES/NO					YES

Implementation perspective				Level			
				0	1	2	3
Continuity of patient pathway across each episode		YES/NO			YES	YES	YES
Registration of clinical data	High-relevant data	dissemination index		*very low*	*low*	*medium*	*high*
	Medium-relevant data	dissemination index			*very low*	*low*	*medium*
	Low-relevant data	dissemination index					
Registration of nursing data	High-relevant data	dissemination index					
	Medium-relevant data	dissemination index					
	Low-relevant data	dissemination index					
Continuity of therapy prescription and administration process		YES / NO				SI	YES
	Dissemination						*medium*
Continuity of order entry/planning/executing/reporting process for laboratory and imaging		YES/NO			YES	YES	YES
Continuity of order entry/planning/executing/reporting process of (extra-) operation process		YES/NO				YES	YES
	Dissemination	dissemination index				*high*	*very high*
Continuity of order entry/planning/executing/reporting process for other activities		SI/NO				YES	YES
	High-relevant activities	dissemination index				*high*	*very high*
	Medium-relevant activities	dissemination index				*medium*	*high*
	Low-relevant activities	dissemination index					*medium*
Utilization of qualified digital signature		YES/NO				YES	SI
	Dissemination					*low*	*medium*
Utilization of centralized access mechanism (eg single sign-on)		YES/NO				YES	SI
	Dissemination	indice di diffusione				*low*	*medium*
Utilization of centralized context for the definition of authorization profiles		YES/NO					YES
	Dissemination	indice di diffusione					*medium*
Integration of structured (detailed) data in the common repository						YES	YES
	High-relevant data	dissemination index				*high*	*very high*
	Medium-relevant data	dissemination index				*medium*	*high*
	Low-relevant data	dissemination index					*medium*
Existence of proactive features (alarms and automatic connetions among data)		YES/NO					YES
	Dissemination	number of processes					
Existence of mechanisms for the automatic identification of the patient		YES/NO					YES
	Dissemination	number of processes					
Existence of mechanisms supporting informal communications among care givers		YES/NO					YES
	Dissemination	number of processes					
Mobile consultation of data		YES/NO				YES	YES
	High-relevant data	dissemination index				*medium*	*high*
	Medium-relevant data	dissemination index					*medium*
	Low-relevant data	dissemination index					
Mobile execution of complete transactions		YES/NO				YES	YES
	High-relevant data	dissemination index				*medium*	*high*
	Medium-relevant data	dissemination index					*medium*
	Low-relevant data	dissemination index					
Existence of a business-continuity infrastructurue	critical processes	YES/NO		NO		YES	YES
	all patient-caring processes	YES/NO					YES
Existence of a disaster recovery infrastructure		YES/NO					YES

Indicators and security levels

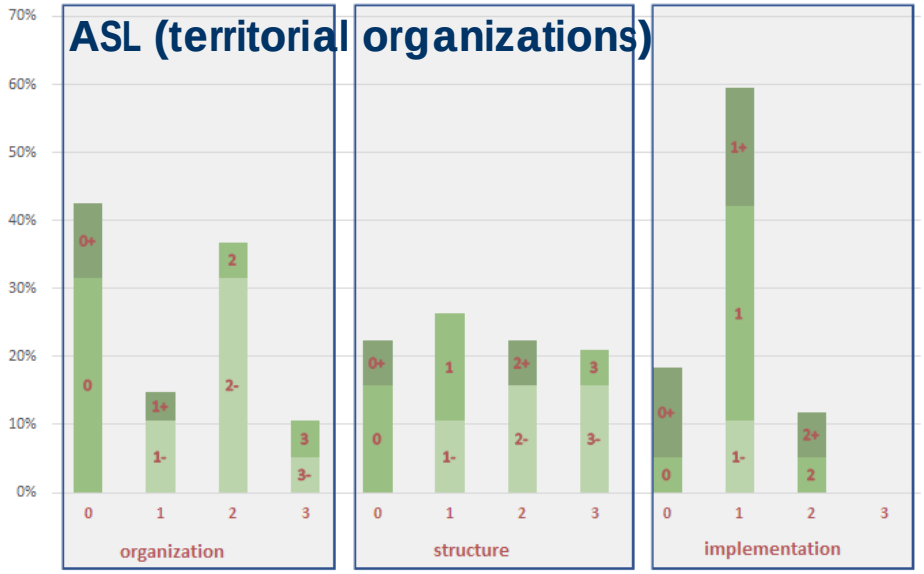
Implementation perspective

Application of the model to the organizations that participated to the survey

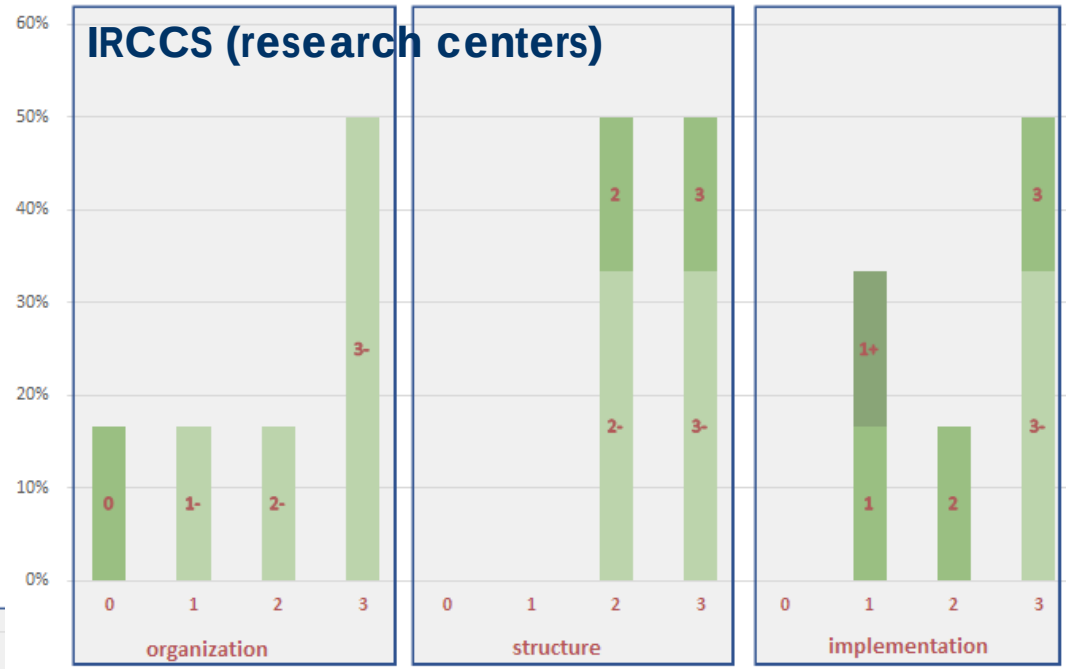
«+» and «-» suffixes
to take into account marginal differences with respect to the main characteristics of the level

Application of the model to the organizations that participated to the survey

ASL (territorial organizations)



IRCCS (research centers)



Individual hospitals and universities