V Conferenza Nazionale sui Dispositivi Medici
Garantire efficienza, sicurezza e innovazione per una crescita sostenibile
ROMA 5 / 6 Dicembre 2012 Auditorium Antonianum - Viale Manzoni 1

CONFERENZA NAZIONALE CNDM SUI DISPOSITIVI MEDICI

"La sicurezza dei sistemi di apparecchiature elettromedicali: dalla sicurezza elettrica alla sicurezza delle reti IT"

ing. Vincenzo Ventimiglia

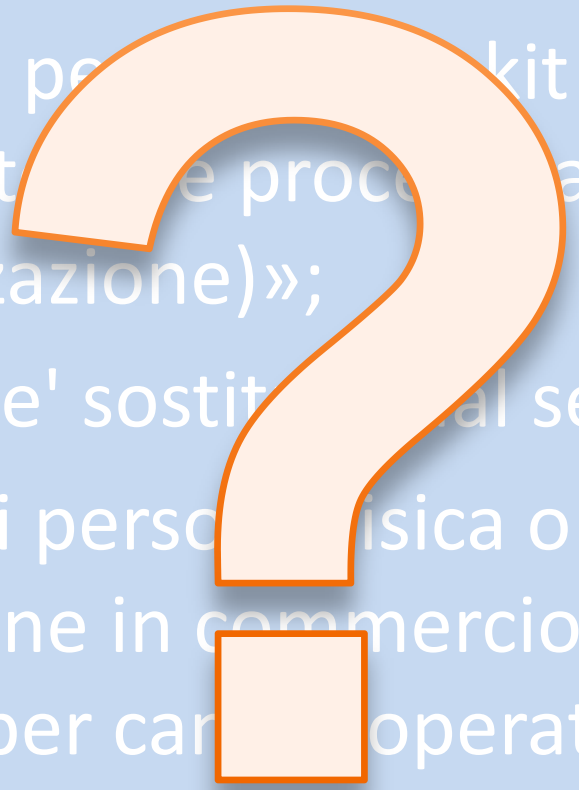
Nella direttiva…

p) all'articolo 12:

1) la rubrica e' sostituita dalla seguente: «(Procedura particolare per [illegible] kit completi per campo operat[illegible]e proc[illegible]a di sterilizzazione)»;

2) il comma 4 e' sostit[illegible]al seguente:

«4. Qualsiasi perso[illegible]isica o giuridica che, ai fini dell'immissione in commercio, sterilizzi sistemi o kit completi per ca[illegible]operatorio ….. omissis



NORME DI RIFERIMENTO

EN 60601-1
ISO EN 14971 “Gestione del rischio”

Requisiti per il fabbricante ma vanno ad impattare

anche sul ciclo di vita del dispositivo…..

SISTEMA ELETTROMEDICALE (SISTEMA EM)

ART. 16 CEI EN 60601

L'articolo sui SISTEMI EM è inteso per essere utilizzato dai COSTRUTTORI di insiemi di apparecchi elettrici che comprendono uno o più APPARECCHI EM, oppure possono avere elementi separati tra loro, o essere contenuti in un unico INVOLUCRO o essere una combinazione dei due casi.

L'articolo è destinato ad essere utilizzato anche dal personale che assembla o adatta il SISTEMA EM, i quali, così facendo, assumono la funzione di fabbricante.

In questo caso è richiesta l'esperienza tecnica nell'applicazione delle Norme di

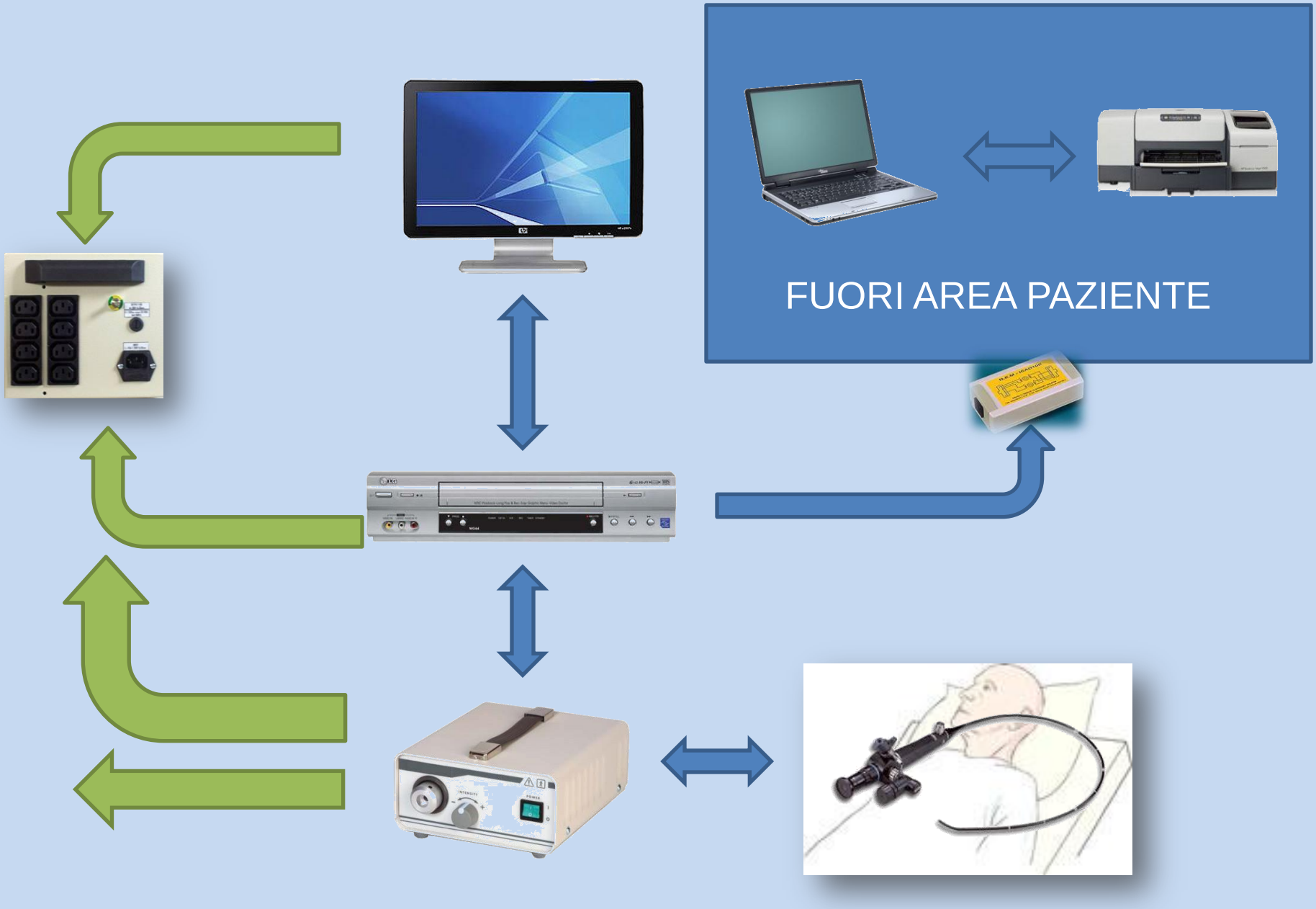
progetto sugli apparecchi elettrici, per assicurare che il SISTEMA EM sia conforme a tutte le prescrizioni della presente Norma.

PROBLEMA 1: APPARECCHIATURE MEDICALI E NON COLLEGATE TRA LORO E RIENTRANTI IN AMBIENTE PAZIENTE (sistema EM)

PROBLEMA 2: APPARECCHIATURE NON MEDICALI IN AMBIENTE PAZIENTE

- Apparecchi per la tecnologia dell'informazione - **CEI EN 60950** (CEI 74-2)

- Apparecchi d'uso domestico e similare - **CEI EN 60335-1** (CEI 61-150)


FUORI AREA PAZIENTE

E per la parte informatica?

CEI EN 80001-1

Applicazione della gestione del rischio per reti IT che incorporano

dispositivi medicali

Parte 1: Ruoli, responsabilità e attività

Inquadramento

- La massiccia diffusione di Dispositivi Medici (DM) dotati di interfaccia di rete (o comunque capaci di interagire con l'infrastruttura informatica) ha profondamente cambiato lo scenario riguardante non solamente le funzionalità dei dispositivi stessi, ma ancora di più la loro gestione e l'interazione e interoperabilità con altri elementi costituenti il patrimonio tecnologico e informativo all'interno delle aziende sanitarie ("organizzazioni responsabili").

- Introdotto dalla norma CEI EN 60601-1 3° edizione

Peculiarità e Criticità

La “rete dati” (e più in generale l’infrastruttura IT) di una azienda sanitaria ha almeno due **peculiarità** significative:

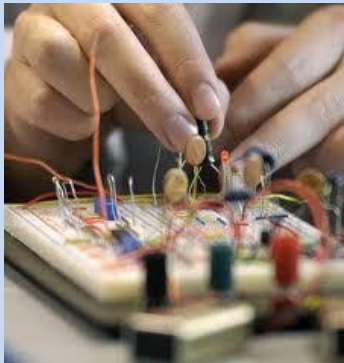
- presenza in rete di DM, che possono essere anche apparecchi elettromedicali o DM software, con tutte le specificità che queste classi di dispositivi comportano,
- e – per *mission* – il trattamento di dati personali e perlopiù sensibili e protetti da alcune leggi specifiche del settore sanitario (int. volontaria di gravidanza, HIV).

Criticità nella gestione dei DM in rete e dell’infrastruttura IT:

- per i DM, la gestione del rischio non deve essere solo “safety” ma anche “data and system security” e “privacy”,
- per l’infrastruttura IT, la sicurezza informatica (“data and system security”), non può prescindere da considerazioni di privacy e di “safety”.

Integrazione competenze

- L'evoluzione ha portato a dover integrare in un unico processo professionalità fino a pochi anni fa completamente autonome, con evidenti difficoltà nell'amalgamare ruoli e competenze tradizionalmente focalizzate su problematiche e approcci distinti. Tale integrazione è oramai indispensabile e "obbligatoria".
- *"Skill culturale" e "sensibilità professionale" differenti:*
  - **Ingegnere Clinico**, tra l'altro:
    - Elettronica, elettrotecnica, meccanica, chimica, fisiologia: principi fisici di funzionamento dei dispositivi medici (apparecchi, strumentazione, tecnologie)
    - DM e gestione del rischio, in particolare *safety*
    - Valutazione e acquisizione tecnologie



- **Informatico** (rete dati, sistemi, applicativi), tra l'altro**:**
  - Elettronica, informatica e telecomunicazioni: principi alla base delle tecnologie dell'informazione e della comunicazione (ICT)
  - Gestione del rischio, in particolare *data and system security* e *privacy*
  - Valutazione e acquisizione tecnologie

- Nel prossimo futuro le aziende sanitarie saranno portate ad individuare figure che fungano da integratori delle conoscenze proprie dei due "mondi", costantemente impegnate nella valutazione del rischio legato alle reti dati medicali (introduzione di nuovi DM e non DM, gestione ciclo di vita dell'intera rete)
- Le aree di comune conoscenza: piattaforma di avvio dell'integrazione professionale, insieme ad una base di conoscenza comune del contesto legislativo-normativo.

- IEC 80001-1:2010 (20120/10)

"Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities"

- "Key properties":
  - **safety,**
  - **effectiveness,**
  - **data and system security**;
- "Medical IT-Network";
- "Medical IT-Network Risk Manager".

CEI EN 80001-1

- La presente Norma definisce le funzioni, le responsabilità e le attività necessarie alla gestione dei rischi delle reti IT che incorporano dispositivi medicali ai fini della sicurezza, dell'efficienza e della sicurezza dei dati e del sistema.
- La Norma non specifica i livelli di rischio accettabili.
- La presente Norma si applica quando un dispositivo medicale è stato acquisito da un'organizzazione responsabile ed è previsto di incorporarlo in una rete IT.

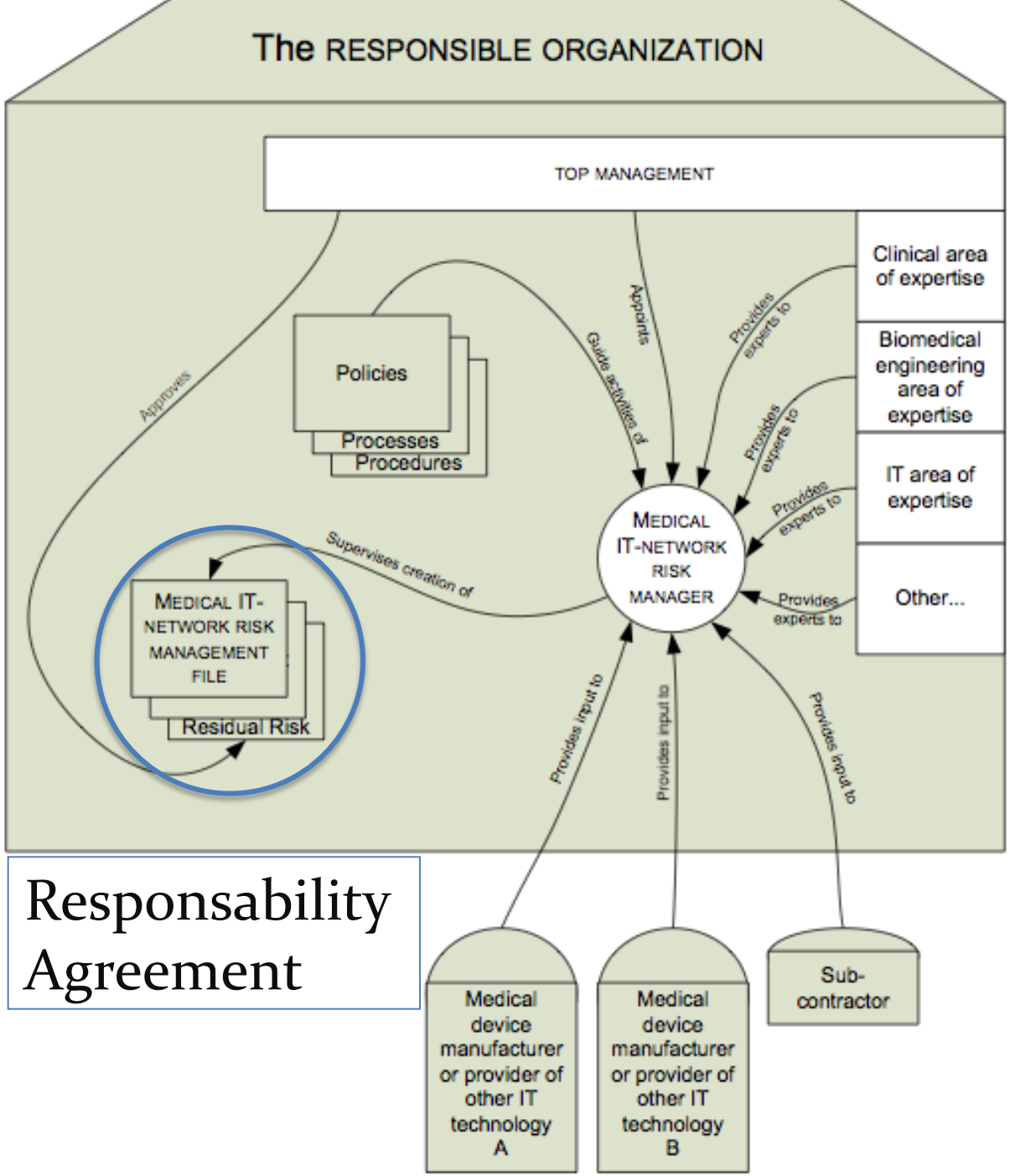
- **Si applica a tutto il ciclo di vita delle reti che incorporano dispositivi medicali**

3.1 Generale
3.2 Organizzazione responsabile
3.3 Responsabilità del TOP MANAGEMENT
3.4 RISK MANAGER della rete IT-Medicale
3.5 Costruttore del DISPOSITIVO MEDICO
3.6 Altri fornitori IT
4 Gestione del rischio durante il ciclo di vita delle reti IT-Medicali
4.2 Gestione da parte della organizzazione responsabile
4.3 Gestione del rischio della rete IT-Med.: pianificazione-documentazione
4.4 Gestione del rischio della rete IT-Medicale
- 4.4.2 ANALISI DEL RISCHIO
- 4.4.3 VALUTAZIONE DEL RISCHIO
- 4.4.4 CONTROLLO DEL RISCHIO
- 4.4.5 Validazione e rapporti sul RISCHIO RESIDUO

4.5 Gestione della “CHANGE-RELEASE e della configurazione
4.6 Gestione del rischio della rete in essere
5 Controllo documentazione
5.1 Procedure di controllo della documentazione
5.2 File di gestione del rischio della rete IT-MEDICALE

Potenziali problemi associati all'incorporazione di dispositivi medici in una rete informatica

- Mancanza di considerazione sul rischio dell'utilizzo della rete IT durante la valutazione del rischio clinico
- Mancanza di supporto dal fabbricante del Dispositivo Medico durante l'incorporazione del prodotto nella rete IT-Medicale (es. Mancanza di informazioni);
- Incorretta operatività o prestazioni degradate (es. Incompatibilità o scorretta configurazione) risultanti dalla combinazione di dispositivi in rete
- Incorretta operatività risultante dalla combinazione di software DISPOSITIVI MEDICI e altre applicazioni SW (internet, mail, giochi!!)
- IL CONFLITTO TRA LA NECESSITA' DI UN CONTROLLO SUI DISPOSITIVI MEDICI E LA NECESSITA' DI UNA RAPIDA RISPOSTA AGLI ATTACCHI DI " malware".



Responsability Agreement

Riassumendo attori, ruoli, flussi e KEY PROPERTIES:

- SAFETY
- EFFECTIVENESS
- DATA AND SYSTEM SECURITY

SAFETY

- Immunità da rischi inaccettabili per il paziente di danni fisici al paziente (ma anche agli operatori ed a terzi) o danni alla proprietà o all'ambiente

possono essere provocati da:

- rischi legati a malfunzionamenti del DM derivanti
  - da "guasti" o "errate configurazioni" degli interfacciamenti o
  - da interazioni non desiderate tra il DM e il "mondo informatico esterno"
- rischi legati alla sicurezza elettrica

SAFETY

- La “documentazione annessa” (labeling) fornita dal fabbricante contempla la connessione di rete?
  - SI, è prevista la connessione durante l’uso sul paziente -> OK
  - SI, ma non è prevista la connessione durante l’uso sul paziente: si applicano le limitazioni del fabbricante o si segue il caso “NO”
  - NO: l’organizzazione responsabile deve fare la valutazione del rischio (ASSEMBLAGGIO/MODIFICA di SISTEMA EM)
    - Collegamenti o connessioni funzionali “dati” sono tipicamente TEMPORANEI e non PERMANENTI
    - Si rientra nel caso della “modifica” del sistema ogni volta che si connette e disconnette il DM alla rete dati
    - Uso di dispositivi di separazione: varie configurazioni possibili

EFFECTIVENESS

- Capacità di produrre il risultato atteso per il paziente e l'organizzazione responsabile

.

- L' obiettivo è perseguibile principalmente tramite l'adozione di best practice internazionali e l'impiego degli standard (IHE, DICOM, HL7, SOA, ICD-9, Snomed, LoInc, ecc) per realizzare il flusso dati a partire dal DM in rete/dal software DM, al fine dell'interfacciamento, dell'integrazione e dell'interoperabilità con l'infrastruttura IT, nell'ottica di un più generale sistema di qualità dell'informazione/dato clinica/o.

EFFECTIVENESS

- Inoltre,ulteriori strumenti a garanzia della qualità dell'informazione/dato al fine della valutazione clinica sono:
  - strumento "informatico"
    firma digitale e sistema di conservazione legale dei documenti, a garanzia di *integrità* e *non modificabilità* degli stessi,
    - un documento firmato e correttamente conservato può essere ritenuto "sicuro" dal clinico;
  - strumento "normativo"
    la marcatura CE DM per il software medicale,
    - un dato fornito da un dispositivo medico (usato correttamente) può essere ritenuto "sicuro" dal clinico.

DATA AND SYSTEM SECURITY

- Garantire la sicurezza di dati e di sistemi che insistono sulla rete dati aziendale è un obbligo di legge definito a più livelli e sotto vari punti di vista (crimini informatici e CP, CAD e quadro normativo di riferimento, privacy e quadro normativo di riferimento) e va perseguito con una logica di sistema e non con interventi a spot.

DATA AND SYSTEM SECURITY

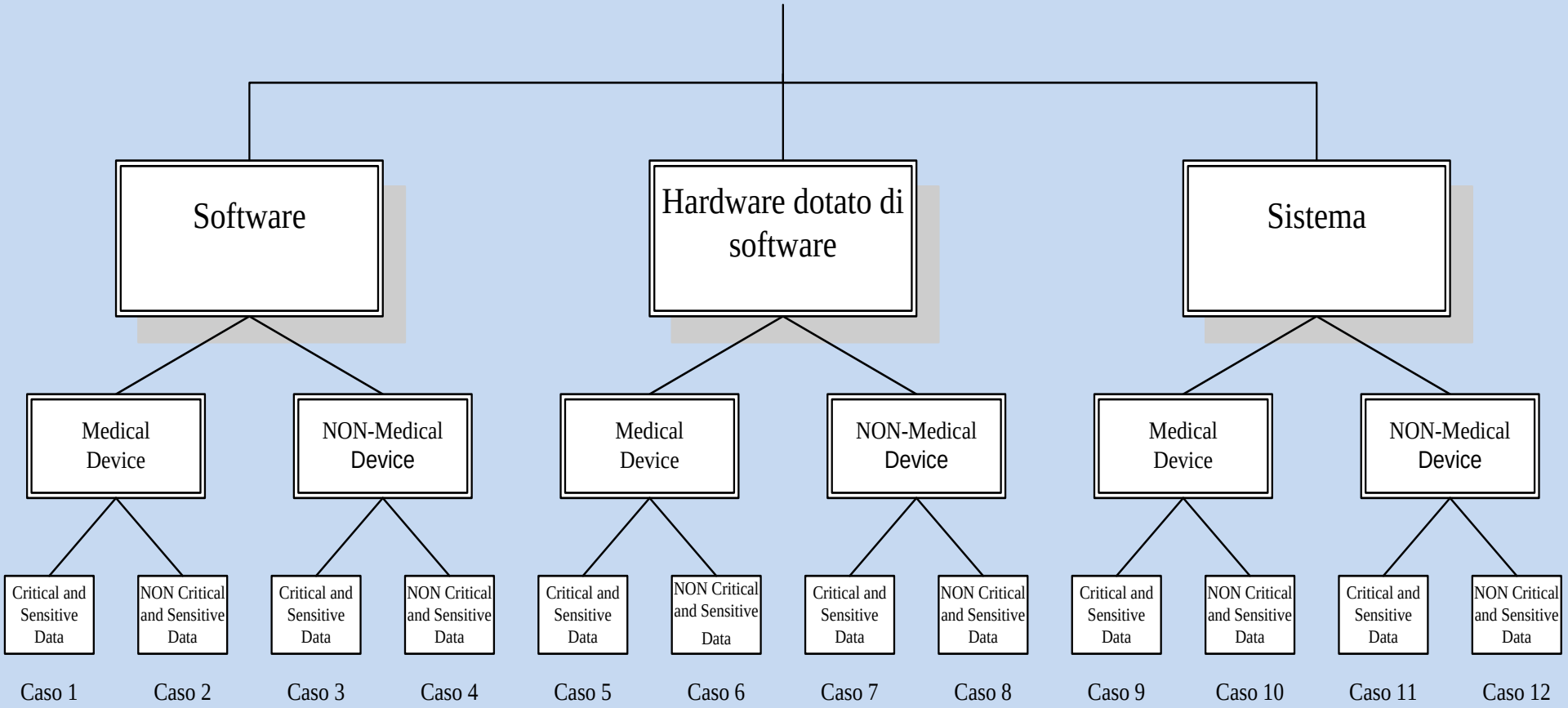
- Medical IT network: il punto di vista IT
  - *In generale*,
    sulla base dei principi della sicurezza informatica, vanno definite e applicate **policy aziendali** in tal senso
    - non è possibile fare "eccezioni" in quanto la sicurezza è come una catena: l'anello debole definisce la sicurezza dell'intero sistema.
  - *In particolare*,
    i DM connessi alla rete dati
    - possono essere oggetto di attacchi informatici,
    - ma anche punti di partenza per azioni della stessa natura;

    i fabbricanti e distributori
    - non danno risposte, o
    - danno risposte non competenti oppure
    - pongono soluzioni che sono vincoli e perciò molto probabilmente non attinenti alle policy IT della singola azienda.

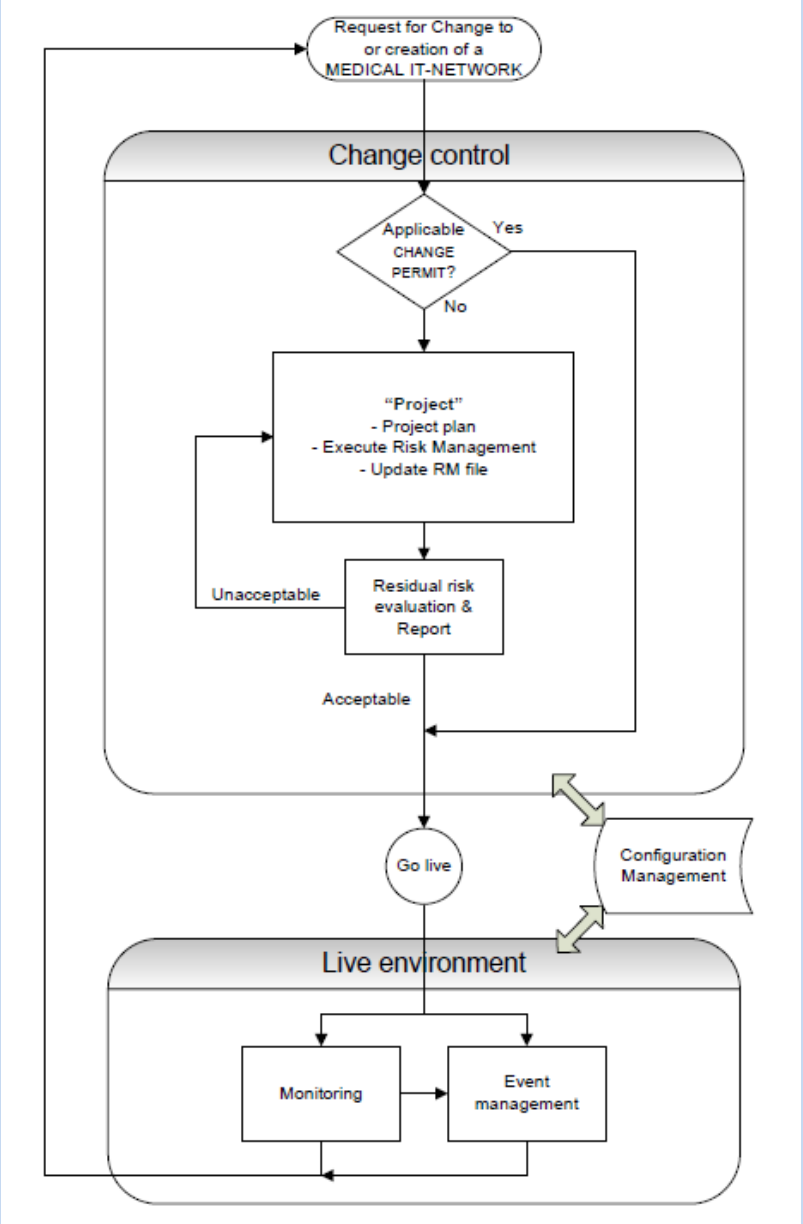
DATA AND SYSTEM SECURITY

- Medical IT network: il punto di vista IC
  - *In generale,*
    vale quanto previsto dalle direttive DM: è indispensabile il rispetto dei requisiti essenziali di sicurezza per tutti i DM (anche quelli connessi alla rete dati); è il fabbricante che definisce nelle istruzioni per l'uso e nella documentazione annessa i **limiti di impiego** e la **destinazione d'uso**
    - non è possibile fare "eccezioni"
  - *In particolare,*
    per i DM connessi alla rete dati
    - non devono essere inficiati i requisiti essenziali di sicurezza a causa dell'applicazione di policy di sicurezza informatica **nel tempo**

DATA AND SYSTEM SECURITY



4 Gestione del ciclo di vita in una rete IT-medicale



Allegato C Guida all'applicazione

System Config.		Scenario Description	Network Components	Network	Network Responsibility	Std.
1	a	MEDICAL DEVICES from one MEDICAL DEVICE manufacturer and non-MEDICAL DEVICES incorporated by the same MEDICAL DEVICE manufacturer and installed as required by that MEDICAL DEVICE manufacturer on an isolated IT-NETWORK.	MEDICAL and non-MEDICAL DEVICE(S) from single MEDICAL DEVICE manufacturer	Physically isolated	MEDICAL DEVICE manufacturer	14971
	b	MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers and non-MEDICAL DEVICES incorporated by one MEDICAL DEVICE manufacturer and installed as required by that MEDICAL DEVICE manufacturer on an isolated IT-NETWORK	MEDICAL DEVICES and non-MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers	Physically isolated	MEDICAL DEVICE manufacturer	14971
2	a	MEDICAL and non-MEDICAL DEVICES incorporated by one MEDICAL DEVICE manufacturer and MEDICAL and non-MEDICAL DEVICES incorporated by other MEDICAL DEVICE manufacturers interconnected on the same IT-NETWORK by a 3rd party (such as a hospital).	Medical and non-MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers	Shared	RESPONSIBLE ORGANIZATION	80001-1
	b	MEDICAL and non-MEDICAL DEVICES incorporated by one MEDICAL DEVICE manufacturer and MEDICAL and non-MEDICAL DEVICES incorporated by other MEDICAL DEVICE manufacturers as well as non-MEDICAL DEVICES and applications interconnected on a shared IT-NETWORK by a 3rd party.	MEDICAL and non-MEDICAL DEVICES from multiple MEDICAL DEVICE manufacturers plus multiple non-MEDICAL DEVICE manufacturers	Shared	RESPONSIBLE ORGANIZATION	80001-1
3		Installations with non-MEDICAL DEVICES from multiple manufacturers using the IT-NETWORK for transmission of electronic Protected Health Information (ePHI).	Multiple non-MEDICAL DEVICE manufacturers	Shared	RESPONSIBLE ORGANIZATION	Out of 80001-1 scope [a]

Allegato D Relazione con la ISO IEC 20000 (Gestione dei servizi di IT)

Table D.1 – Relationship between IEC 80001-1 and ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005

IEC 80001-1	ISO/IEC 20000-1:2005 or ISO/IEC 20000-2:2005
2.4 CONFIGURATION MANAGEMENT In IEC 80001-1, CONFIGURATION MANAGEMENT is a PROCESS that stores in the CMDB.	**2.5 configuration management database** The CMDB is the database used for configuration management. [ISO/IEC 20000-1:2005]
2.7 EVENT MANAGEMENT The nature of events is not defined in 80001-1. They relate to both the IT-NETWORK and the MEDICAL DEVICE	**2.7 incident** Incident and problem both relate to events that are managed by EVENT MANAGEMENT in IEC 80001-1. [ISO/IEC 20000-1:2005]
2.21 RESPONSIBILITY AGREEMENT An agreement between e.g. suppliers, manufacturers, service provider, system integrator and the RESPONSIBLE ORGANIZATION	**2.13 service level agreement (SLA);** **2.14 service management** Defines the relation between owner of an IT network and the service provider. [ISO/IEC 20000-1:2005]
2.22 RESPONSIBLE ORGANIZATION	**2.15 service provider** The RESPONSIBLE ORGANIZATION shall certify the IT-NETWORK service provider as part of its policy. [ISO/IEC 20000-1:2005]
2.29 RISK MANAGEMENT FILE	**2.9 record; 2.3 change record; 2.11 request for change** element(s) of the RISK MANAGEMENT FILE **2.5 configuration management database (CMDB)** element of the RISK MANAGEMENT FILE (asset description). NOTE The RISK MANAGEMENT FILE can be stored in a database that includes the CMDB. [ISO/IEC 20000-1:2005]
3.3 TOP MANAGEMENT responsibilities	**3.1 Management responsibility** Both standards address senior management responsibilities. ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005 leave more organizational freedom.
3.4 MEDICAL IT-NETWORK RISK MANAGER The RISK manager is responsible for the RISK MANAGEMENT PROCESS.	**3.1 Management responsibility** RISK MANAGEMENT is not specifically assigned as a task for management. **6.6.7 Documents and records** Records should be analyzed. In IEC 80001-1, this is the responsibility of the MEDICAL IT-NETWORK RISK MANAGER. [ISO/IEC 20000-2:2005]
3.5 MEDICAL DEVICE manufacturer(s); **3.6 Providers of other Information Technology** These sections specify information to be provided via the suppliers to the RESPONSIBLE ORGANIZATION	**7.1 Relationship process – general** **6.6.5 Security and availability of information** [ISO/IEC 20000-2:2005] **7.3 Supplier management** Both standards require relationships to be formalized via contract. Sections 6.6.5 and 7.3 relate to suppliers of components of the MEDICAL IT-NETWORK.
4.2.1 Policy for RISK MANAGEMENT for incorporating MEDICAL DEVICES	**3.1 Management responsibility**
4.2.2 RISK MANAGEMENT PROCESS Covers SAFETY, EFFECTIVENESS and DATA AND SYSTEM SECURITY	**6.6.3 security risk assessment practices** [ISO/IEC 20000-2:2005] Security is a subset of the KEY PROPERTIES of a MEDICAL IT-NETWORK. IEC 80001-1 provides the general RISK MANAGEMENT PROCESS for the IT-NETWORK.

4.3 MEDICAL IT-NETWORK RISK MANAGEMENT planning and documentation	**4.1 Plan service management (Plan);** **4.4.2 Management of improvements;** **5.1 Topics for consideration** ISO/IEC 20000 can include risk management. IEC 80001-1 defines the requirements to service management for medical IT-networks.
4.3.2 Asset description	**6.6.2 Identifying and classifying information asset** The scope should include all key properties
4.3.3 IT-NETWORK documentation This section specifies information relating to the RISK MANAGEMENT PROCESS.	**4.1.1 Scope of service management; 6.6.2 Identifying and classifying information asset** The content of the information has overlap with IEC 80001-1 section 4.3.3.
4.3.4 RESPONSIBILITY AGREEMENT	**7.3 Supplier management (1st paragraph)** Both sections aim to clarify the intentions of collaboration to all relevant stakeholders
4.3.5 RISK MANAGEMENT Plan for the MEDICAL IT-NETWORK	**6.6.3 Security risk assessment practices** Security is a subset of the key properties of a medical IT-network. IEC 80001-1 provides the general risk management process for the IT-network.
4.4 CHANGE-RELEASE MANAGEMENT and CONFIGURATION MANAGEMENT	**9 Control processes; 10 Release process** Change and configuration management as well as release and go-live are covered in sections 9 and 10. IEC 80001-1 section 4 describes the risk management activities as included in these processes
4.4.2.4 RISK CONTROL	**9.1.5 Configuration verification and audit; 9.2.2 Planning and implementation** ISO/IEC 20000 covers a broad scope of items that require verification. Verification of risk control measures is elaborated in IEC 80001-1
4.4.3.3 Establishing a project plan Major changes need a project to assess RISK prior to implementing change.	**9.2.1 Planning and implementation** ISO/IEC 20000 indicates all changes to be planned before implementation. IEC 80001-1 requires all changes to be risk managed which includes planning.
4.4.4 Authority in CHANGE-RELEASE MANAGEMENT	**9.2.1 Planning and implementation; 10.1.6 Release verification and acceptance** IEC 80001-1 assigns the responsibility for sign-off to the risk manager
4.5.1 Monitoring	**10.1.8 Roll-out, distribution and installation; 10.1.9 Post release and roll-out** Monitoring can relate to both organizational or technical risk control measures
5.1 Document control procedure	**3.2 Documentation requirements**
5.2 MEDICAL IT-NETWORK RISK MANAGEMENT FILE	**5.2 Change records; 6.6.7 Documents and records; 10.1.7 Documentation**

Tecnical report applicativi

- IEC/TR 80001-2-1 Edition 1.0 (2012-07-10) Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step by step risk management of medical IT-networks – Practical applications and examples
- IEC/TR 80001-2-2 Edition 1.0 (2012-07-10) Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- IEC/TR 80001-2-3 Edition 1.0 (2012-07-10) Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks

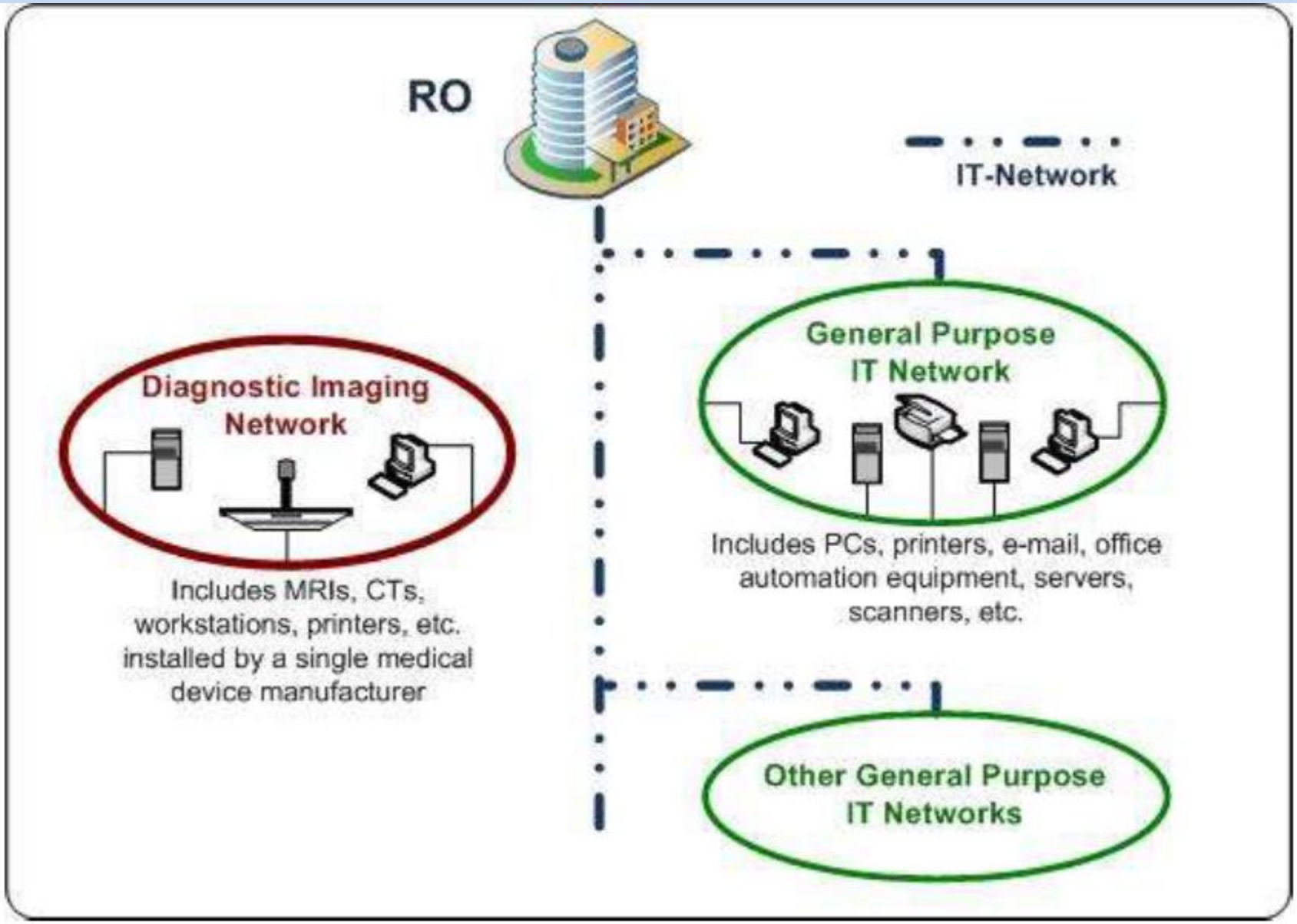
Tecnical report applicativi in sviluppo

- **IEC/TR 80001-2-4 Ed. 1.0 (62A/818/CDTR) Application of risk management for IT-networks incorporating medical devices – Part 2-4: General implementation guidance for Healthcare Delivery Organizations**

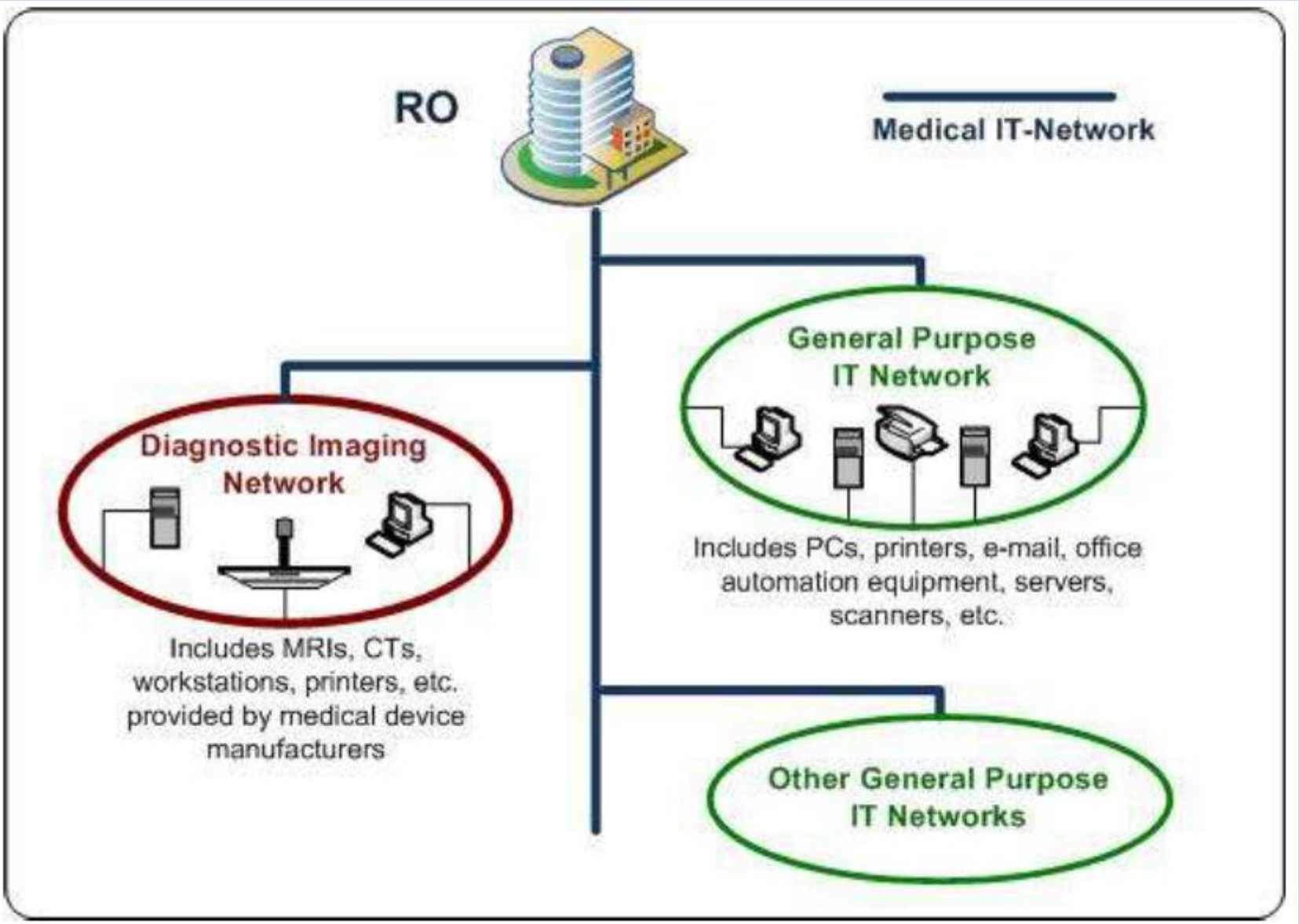
  The draft technical report (DTR) will be registered as a Technical Report by (date) 2012-12

- IEC/TR 80002-1 Edition 1.0 (2009-09-23) Medical device software – Part 1: Guidance on the application of ISO 14971 to medical device software
- ISO/TR 80002-2 Ed. 1.0 (62A/770/RVN – FDIS expected within October 2014) Medical device software – Part 2: Validation of software for regulated processes

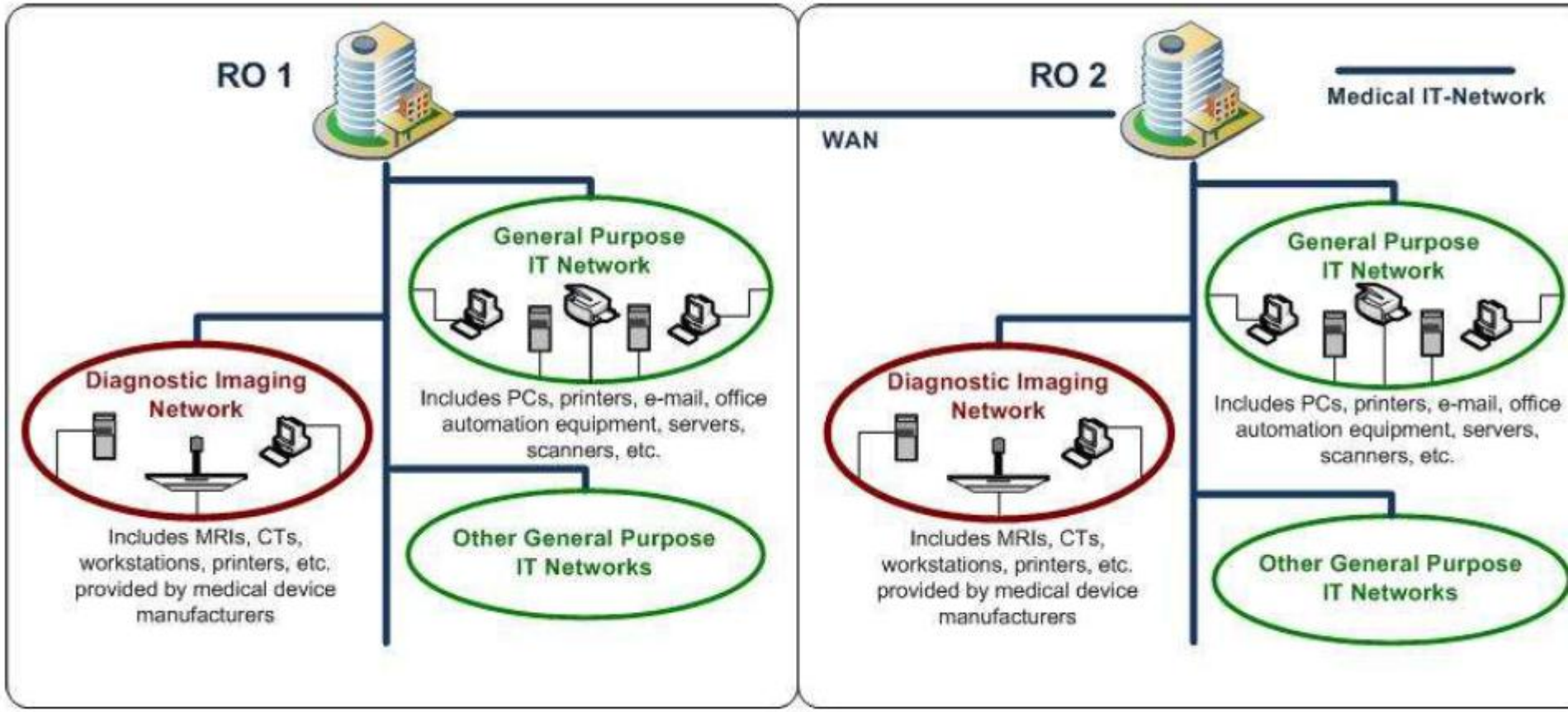
Da IEC/TR 80001-2-4→ rete non gestita da OR



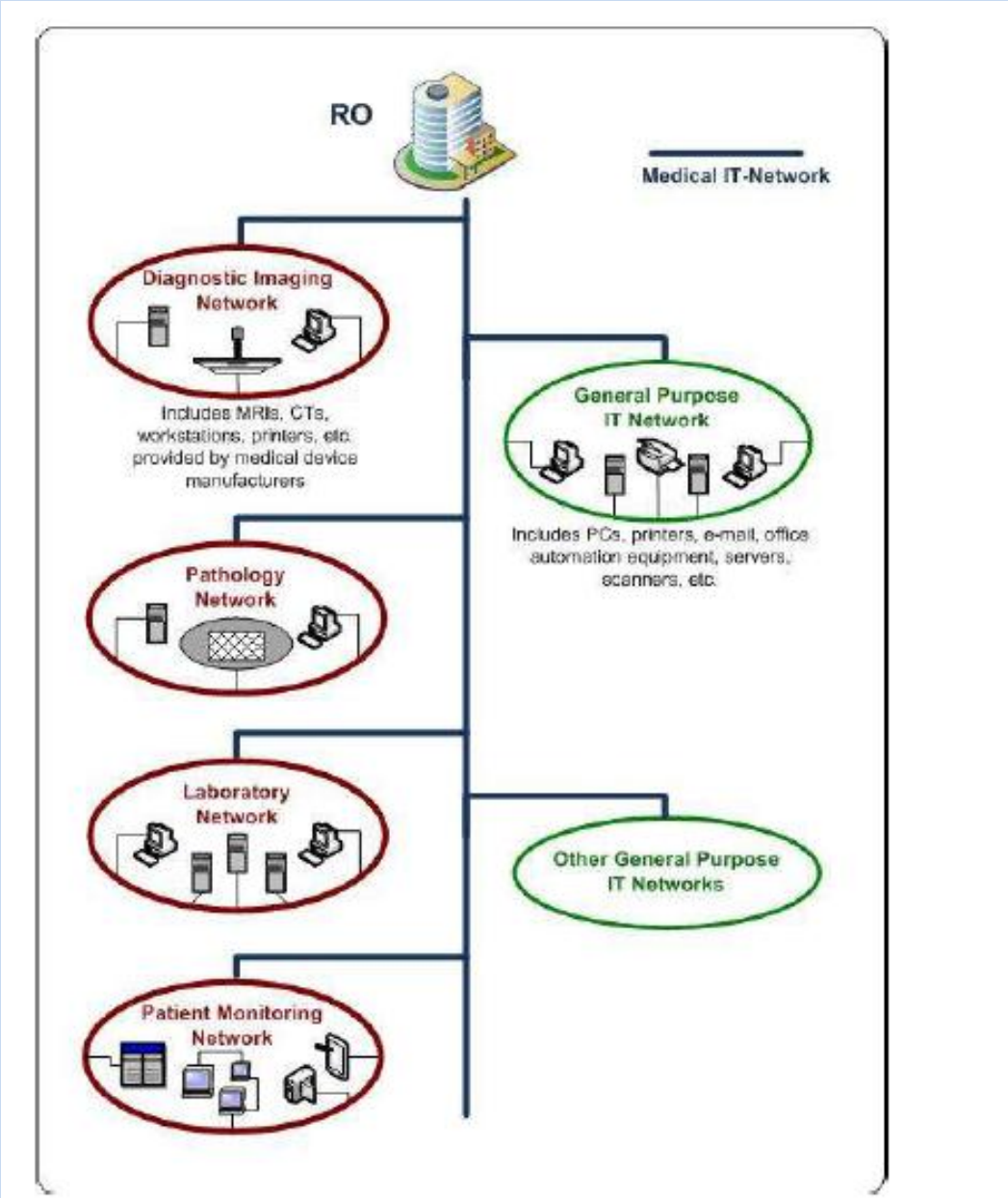
Da IEC/TR 80001-2-4→ rete IT-Medicale a sè



Da IEC/TR 80001-2-4→ rete IT-Medicale in collaborazione



Da IEC/TR 80001-2-4→ rete IT-Medicale centralizzata



Grazie per l’attenzione