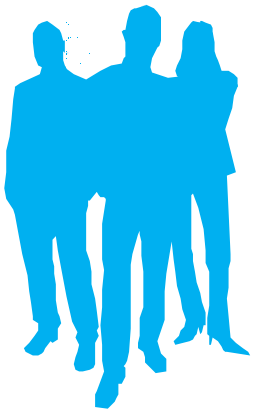


Cyber Security Day – Ancona, ITALY

Un caso di studio: il progetto Nu.Sa. di FIMMG e FEDERSANITA' ANCI

Emanuele Frontoni, Adriano Mancini, Primo Zingaretti
Marco Baldi, Franco Chiaraluce
Dipartimento di Ingegneria dell'Informazione – DII
Università Politecnica delle Marche

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Stato dell'arte MMG

- Condivisione di dati tra MMG
  (medicine associate, aggregazioni, AFT …)
- Le Reti del Sistema
- Patient Summary – Fascicolo Sanitario Elettronico

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Enorme eterogeneità

Your Emergency Care Summary

What does it mean for you?

NHS SCOTLAND

Your Emergency Care Summary contains the following information.

- Your name
- Your date of birth
- The name of your GP surgery
- An identifying number called a CHI number (there is more about the CHI number later)
- Information about any medicines prescribed by your GP surgery
- Any bad reactions you've had to medicines that your GP knows about

Your Emergency Care Summary is copied from your GP's computer system and stored electronically. NHS staff can then find it quickly if they need to see it.

UNIVERSITÀ POLITECNICA DELLE MARCHE

FONDAZIONE NU.SA
NUVOLA SANITÀ PER LE CURE INTEGRATE

Cloud Netmedica

DATI CRITTOGRAFATI

Cloud

NETMEDICA "APP STORE"

"CERTIFY"

VERIFICA E CERTIFICAZIONE DATI IN INGRESSO

"IMPORT"

STANDARD XML SOAP/WSDL

"TRAIN"

PALESTRA PER IL TESTING DEI SERVIZI E DELLE INTEGRAZIONI

AUTENTICAZIONE
AUTORIZZAZIONE

FIMMG Federazione Italiana Medici di Famiglia

SISTEMI FRONT END

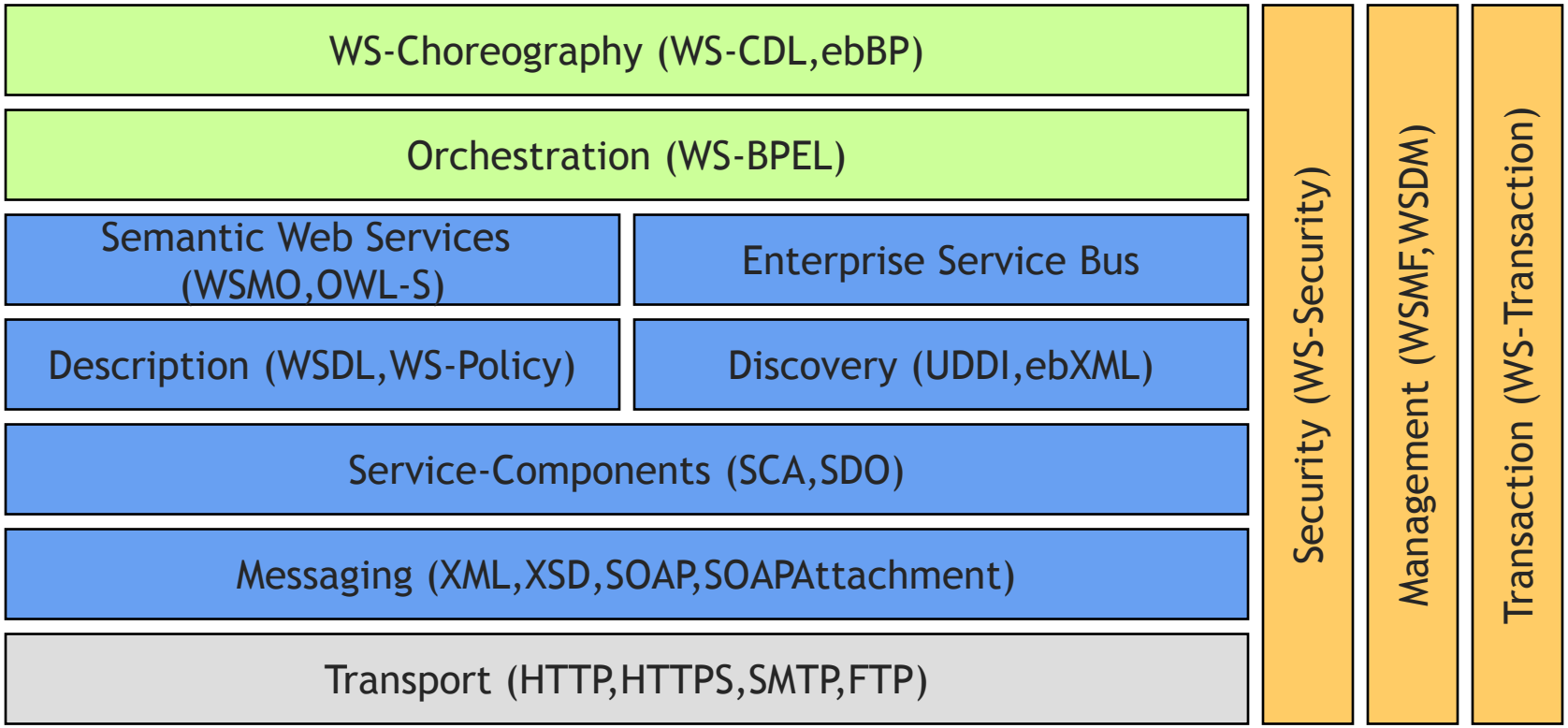
DATI ASSISTITI

UNIVERSITÀ POLITECNICA DELLE MARCHE

Internet Protocols
Service-Composition
Foundations
Quality of Service

Web Services

Current State-of-the-art in Web Service Technologies



FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

ALTRE BANCHE DATI ED OPERATORI DI SISTEMA

SOAP - WSDL

Box "WEB 2.0" per il paziente

APPLICATIVI E SERVIZI

NETMEDICA store

Self- audit
EBM al punto di cura
Rendicontazione
Aggiornamenti
Telemedicina …

SOAP - WSDL

XML XML XML
XML XML XML
XML XML XML
XML XML XML

SOAP - WSDL

CRITTOGRAFIA "FORTE"

"IMPORT"

"TRAIN"
PALESTRA PER IL TESTING DEI SERVIZI E DELLE INTEGRAZIONI

"CERTIFY"
VERIFICA E CERTIFICAZIONE DATI IN INGRESSO

SOAP - WSDL

SOAP - WSDL

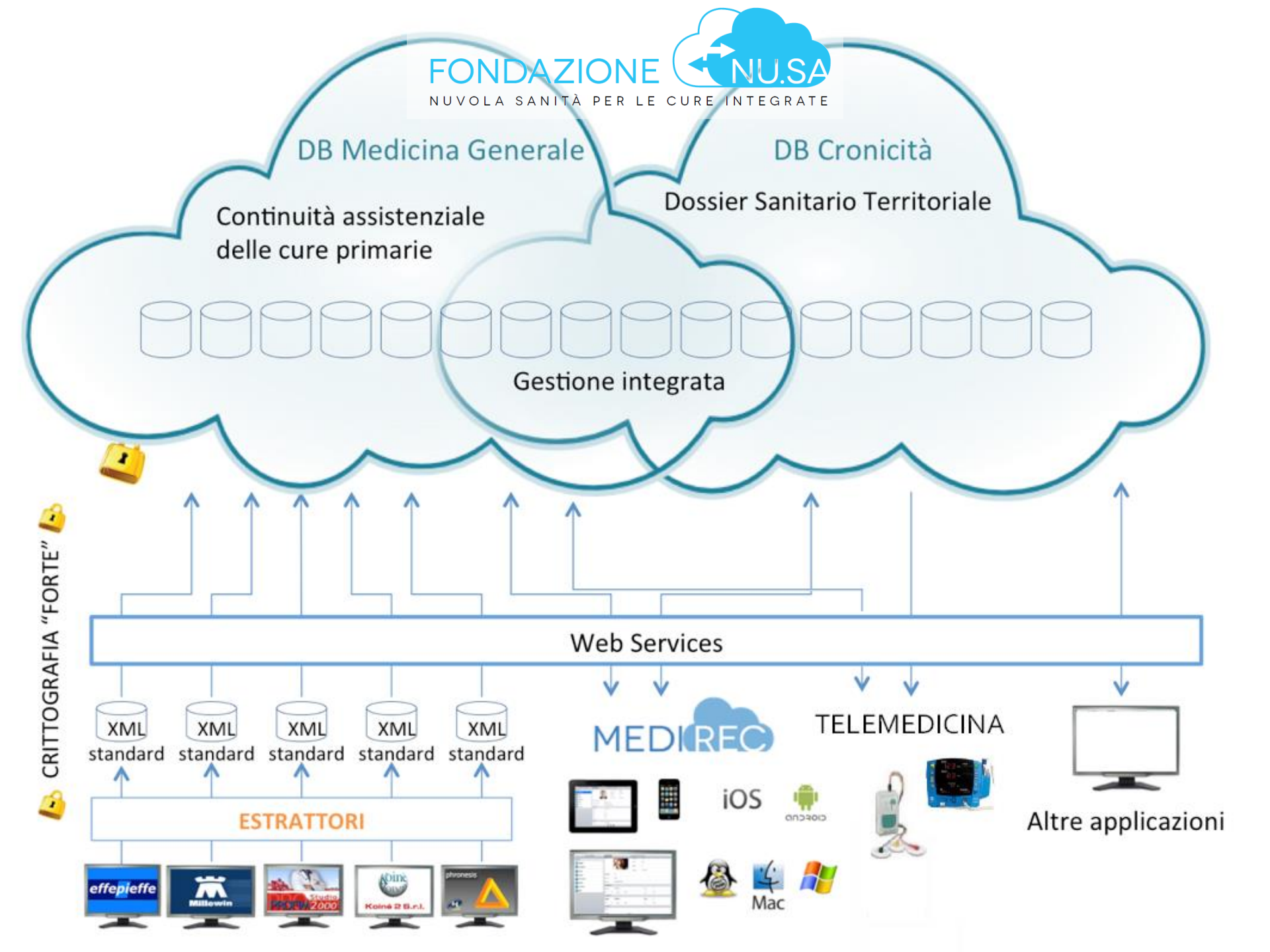
XML standard | XML standard | XML standard | XML standard | XML standard

ESTRATTORI

AUTENTICAZIONE / AUTORIZZAZIONE
"FORTE " – SSO – UN, PW, Secret

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE


FONDAZIONE NU.SA
NUVOLA SANITÀ PER LE CURE INTEGRATE
DB Medicina Generale
Continuità assistenziale
delle cure primarie
DB Cronicità
Dossier Sanitario Territoriale
Gestione integrata
CRITTOGRAFIA "FORTE"
Web Services
XML standard
XML standard
XML standard
XML standard
XML standard
ESTRATTORI
effepieffe
Millewin
Koinè 2 S.r.l.
MEDIREC
iOS
TELEMEDICINA
Mac
Altre applicazioni

IL CLOUD

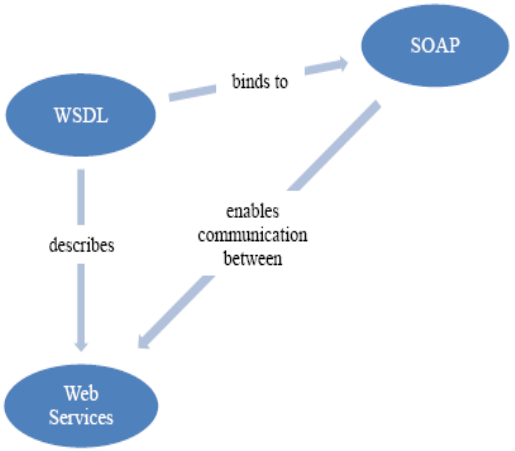
- Architettura SaaS (SOA)
- Scalabilità
- Sicurezza
- Nomi “noti”: Nuvola Italiana
- Tecnologia con disponibilità costante e dati protetti
- Condivisione dati multi-dispositivo

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

I WEB SERVICES

- Descrizione del dato in formato WSDL / SOAP
- Convergenza verso HL7
- Validazione del dato
- Disponibilità di formati e “palestra” condivisa
- Accesso autenticato
  e dati crittografati
- Servizi di analisi condivisi
- Futuro utilizzo di un indice
  dei servizi FIMMG (UDDI)
- **42 servizi e 93 metodi**



FIMMG Federazione Italiana Medici di Famiglia

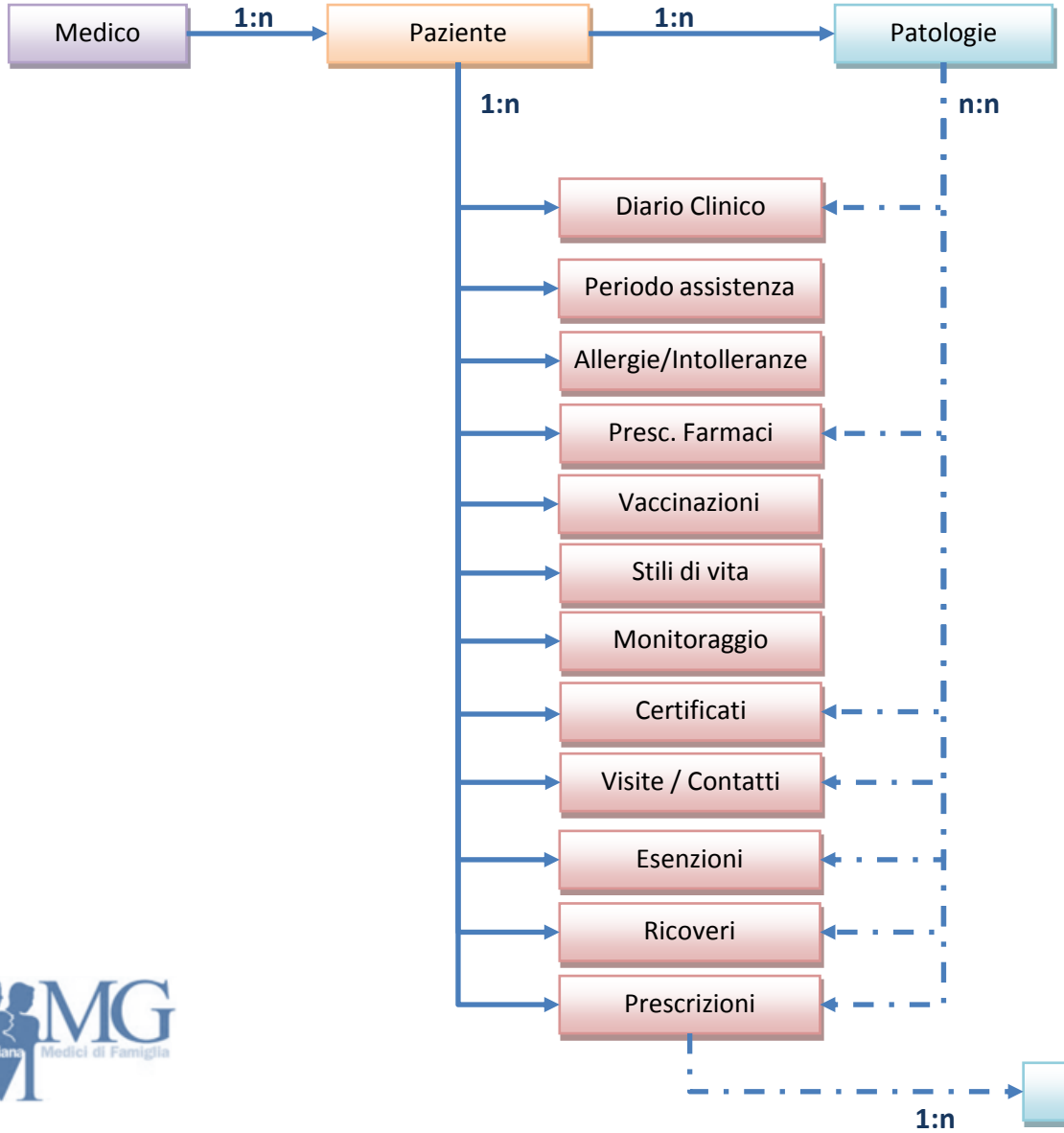
UNIVERSITÀ POLITECNICA DELLE MARCHE

AUTENTICAZIONE

IL DATO PASSA AL CLOUD SOLO SU AUTORIZZAZIONE DEL MEDICO

- Autenticazione forte
- Federazioni SAML 2.0
- Dato crittografato (per la parte non anonima) su base utente
- No ad attività massive

STRUTTURA DATI



FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Paziente

Contiene in forma criptata in dati anagrafici del paziente. Leggibili solo dal medico proprietario o dai colleghi con i quali decide di condividere le informazioni.

Patologie

Contiene i problemi dei pazienti con i relativi stati, e le date di apertura e chiusa. Viene mantenuta l'informazione di origine anche in assenza del codice ICD-IX. La tabella è relazionata con altre tabelle per favorire le ricerche per problema.

Diario Clinico

Contiene le valutazioni storiche legate all'evoluzione delle patologie, con la classificazione SOVP.

Periodo di assistenza

Contiene i periodi di inizio e fine assistenza del paziente, con la relativa motivazione. Vengono gestiti periodi di assistenza multipli.

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Allergie ed intolleranze

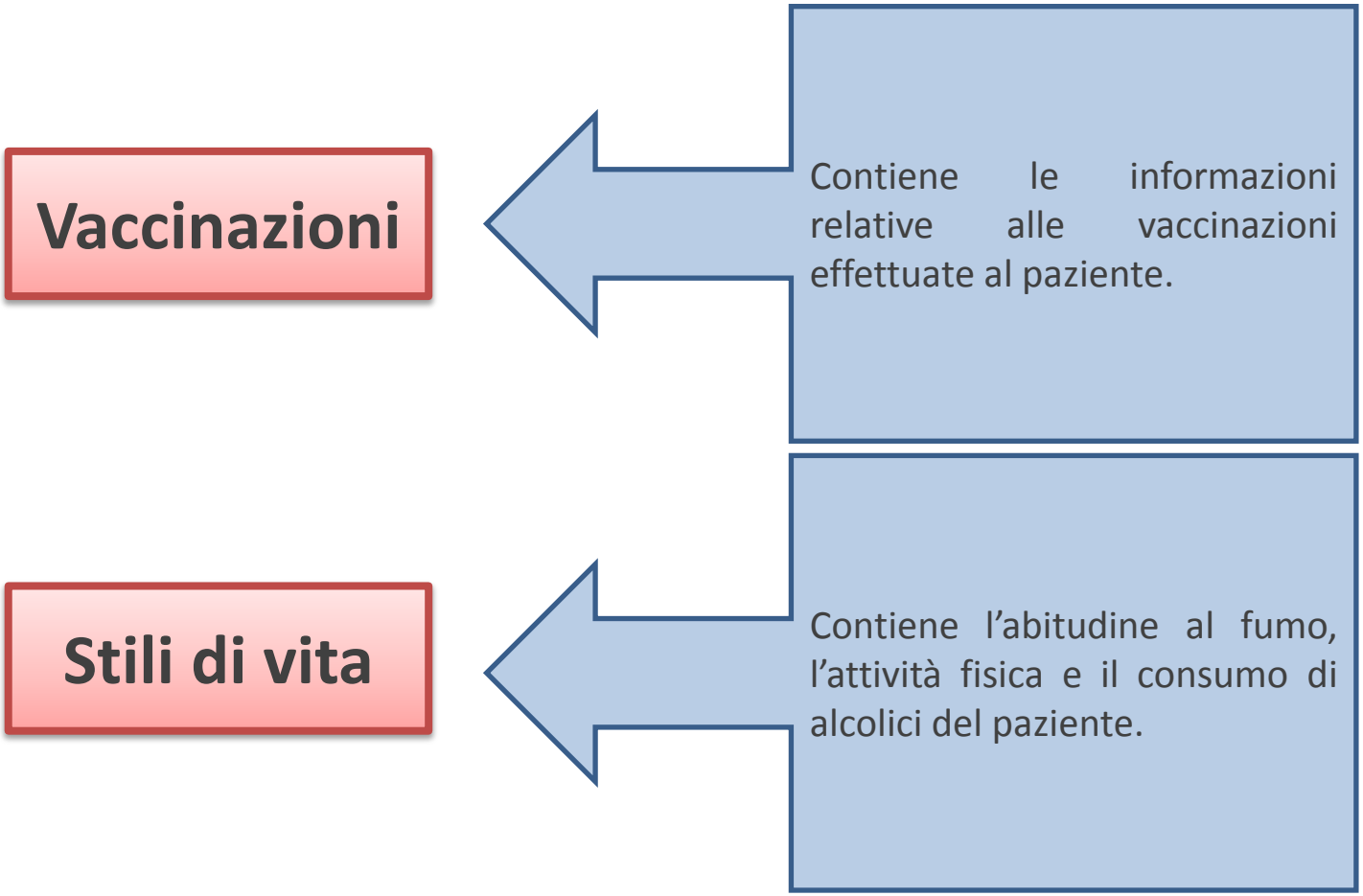
Contiene allergie ed intolleranze definite per farmaco / principio attivo / ATC oppure definite in testo libero.

Prescrizione farmaci

Contiene la terapie prescritte ai pazienti con tutte le informazioni contenute nella ricetta. Vengono acquisite anche le ricette non stampate se salvate nel software di cartella.

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE



FIMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Monitoraggio

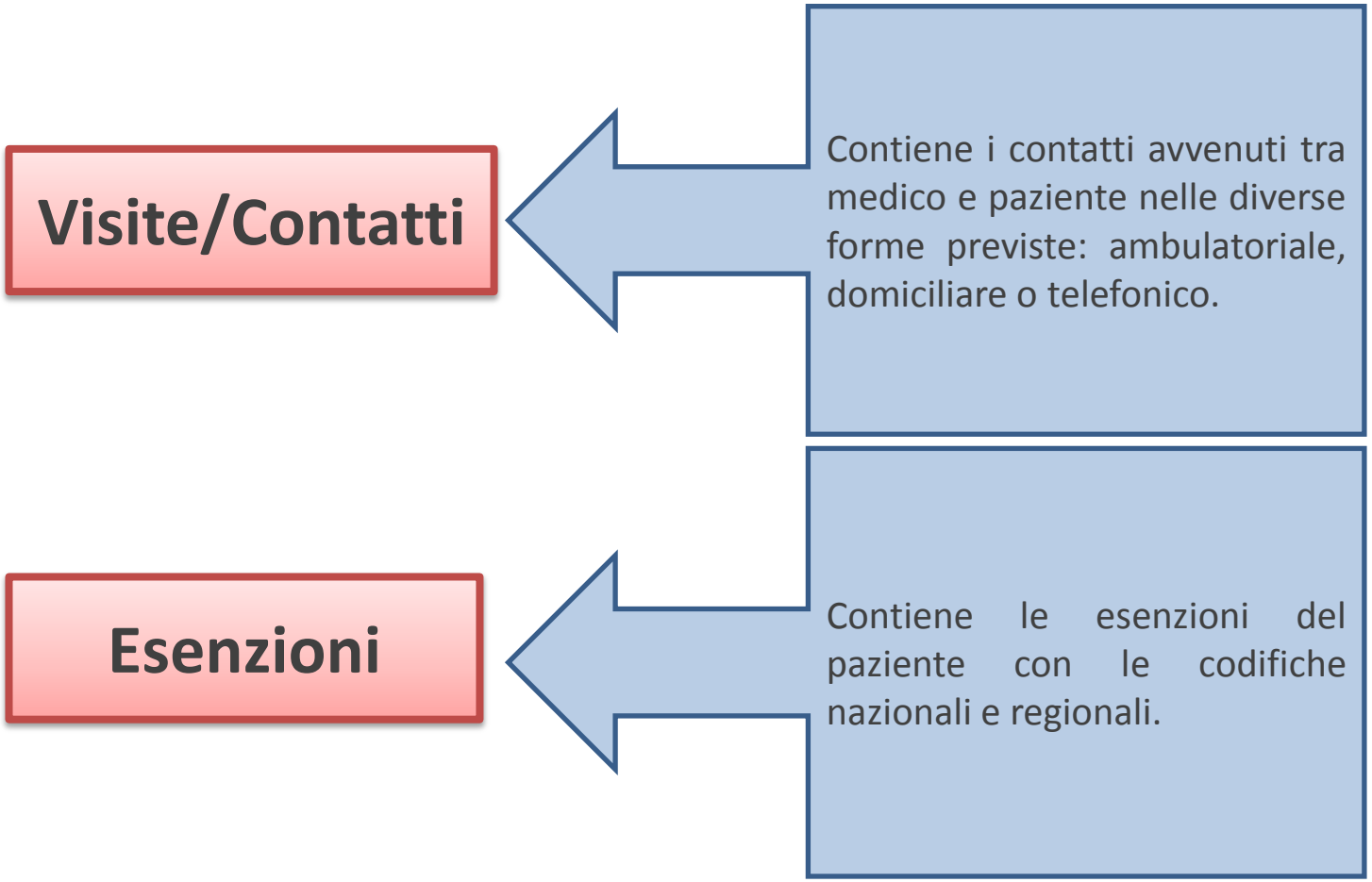
Contiene i dati di pressione: minima, massima, frequenza cardiaca, ritmo e somatometrici: peso, altezza, circonferenza.

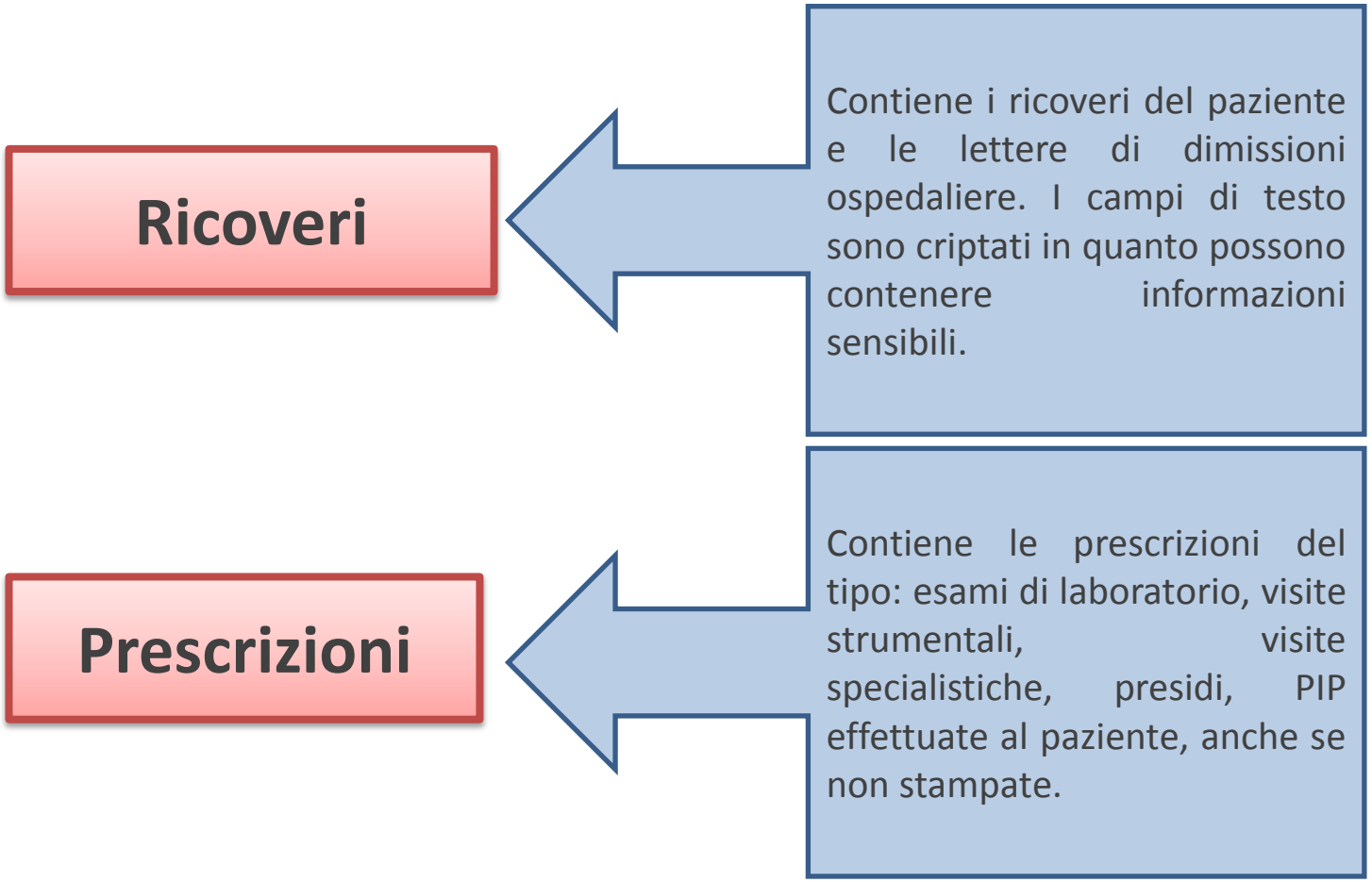
Certificati

Contiene i certificati inail e di malattia del paziente. I campi di testo sono criptati in quanto possono contenere informazioni sensibili.

FIMMG Federazione Italiana Medici di Famiglia

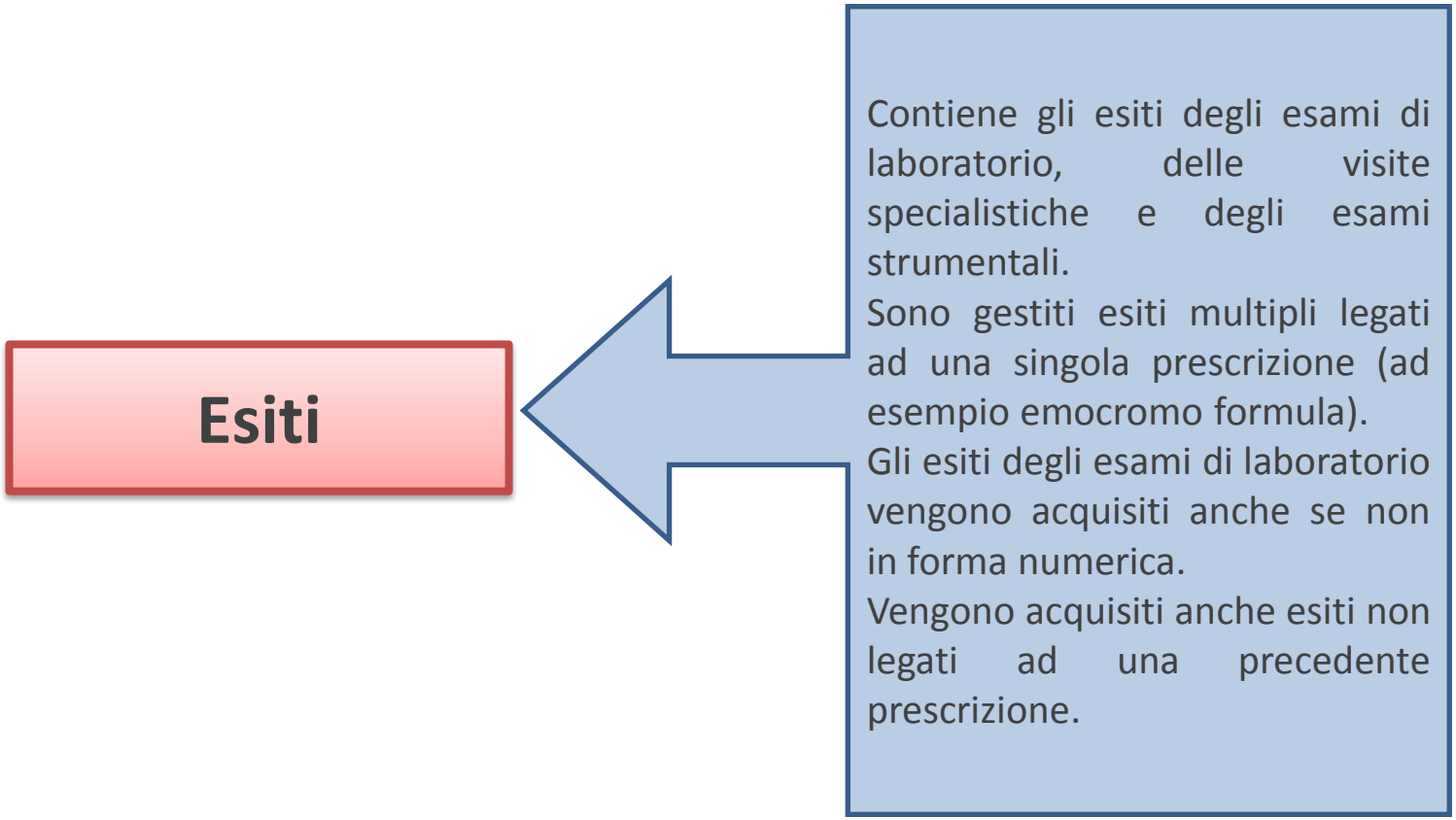
UNIVERSITÀ POLITECNICA DELLE MARCHE


Visite/Contatti
Contiene i contatti avvenuti tra medico e paziente nelle diverse forme previste: ambulatoriale, domiciliare o telefonico.
Esenzioni
Contiene le esenzioni del paziente con le codifiche nazionali e regionali.



FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

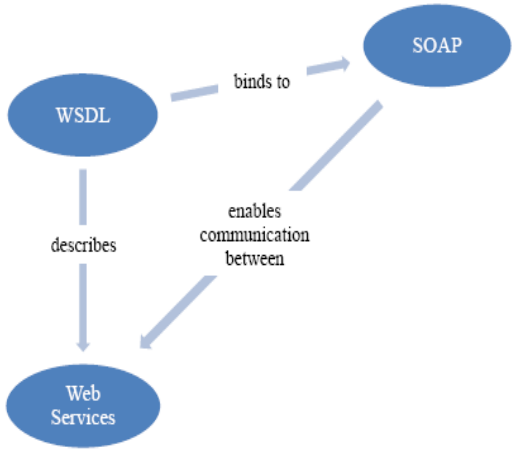

Esiti
Contiene gli esiti degli esami di laboratorio, delle visite specialistiche e degli esami strumentali.
Sono gestiti esiti multipli legati ad una singola prescrizione (ad esempio emocromo formula).
Gli esiti degli esami di laboratorio vengono acquisiti anche se non in forma numerica.
Vengono acquisiti anche esiti non legati ad una precedente prescrizione.

I NUMERI

- 3300 MMG
- 5.5 MLN di pazienti

140.000.000
di prescrizioni

Dati al 27.03



FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

I CASI NAZIONALI

Toscana – ASL Arezzo

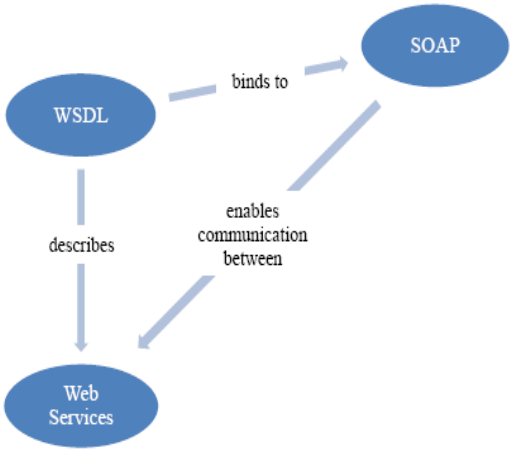
Interoperabilità & telemedicina

Campania – ARSAN

Progetto cronicità (diabete)

Oltre 1.4 MLN € di ricadute su MMG

INDICATORI E SELF AUDIT



FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Sicurezza e Privacy

Requisiti:

- Sicurezza/Confidenzialità
  - Evitare qualsiasi accesso non autorizzato ai dati sanitari dei pazienti
- Privacy
  - Consentire solo al medico curante di associare i dati sanitari di un paziente alla sua identità

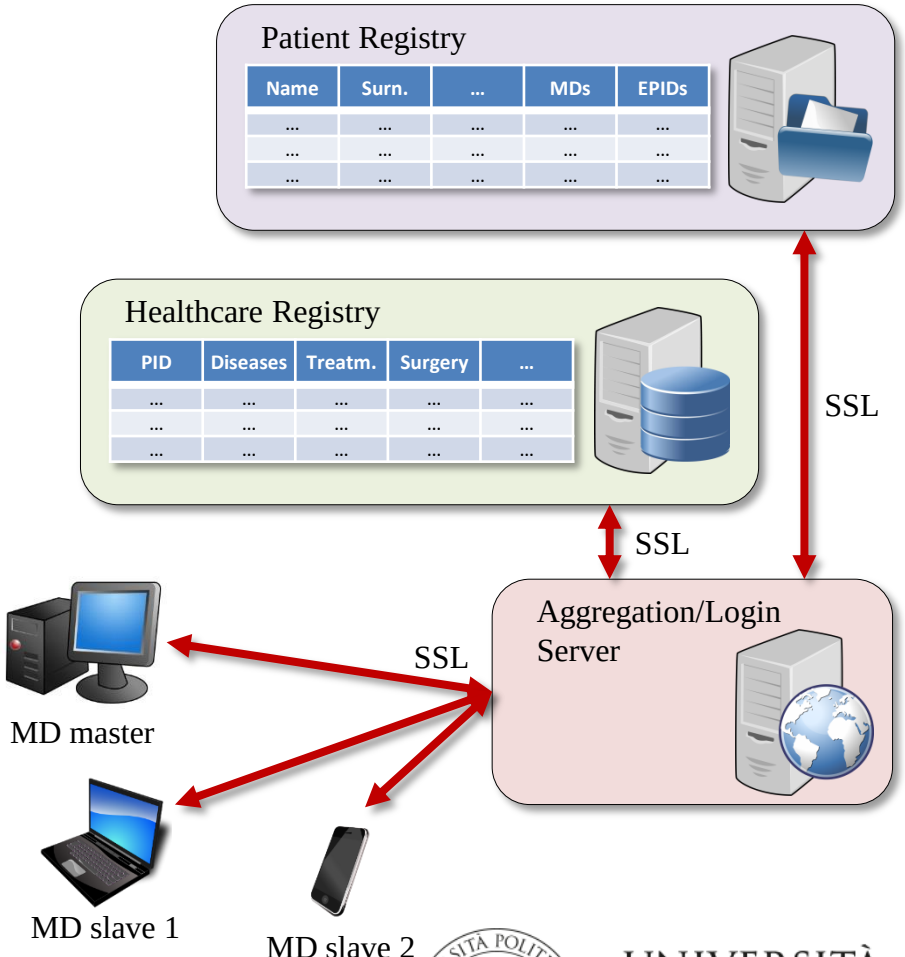
FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Sicurezza e Privacy - Architettura

Componenti:

- **Registro Pazienti:** solo dati anagrafici
- **Registro Sanitario:** solo dati sanitari
- **Server di Aggregazione/Login:** interfaccia per i terminali del medico generale
- Un terminale principale e vari terminali secondari per ciascun medico



FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Sicurezza e Privacy - Strumenti

- A **ciascun paziente** è associato un **identificativo numerico** (PID) **unico e generato casualmente**
- Il PID compare **in chiaro** nel Registro Pazienti
- Il **Registro Sanitario contiene una versione cifrata del PID** di un paziente per ciascun medico che lo segue
- **L'associazione tra PID in chiaro e PID cifrato avviene solo all'interno del terminale del medico** che segue il paziente
- Accedendo ai dati online da un qualsiasi altro terminale, non c'è modo di associare i dati sanitari all'identità del paziente
- **Tutti i dati sono conservati in database cifrati** (Transparent Data Encryption)
- **Tutte le connessioni avvengono su tunnel cifrati** (SSL)

FIMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Sicurezza e Privacy – Sviluppi futuri

- Con il **modello cloud** si va verso la **decentralizzazione delle basi di dati**
- Con la **decentralizzazione** si può ottenere **sicurezza**, tramite **algoritmi di manipolazione e dispersione dei dati**
- Si pone il problema di **effettuare ricerche su dati cifrati** (e dispersi) → **searchable encryption**
- Nel modello cloud la capacità di calcolo è trasferita dal client al cloud
- Si pone il problema di **effettuare calcoli** (ad es. statistici) **sui dati cifrati** (e dispersi) → **homomorphic encryption**

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

Sicurezza e Privacy

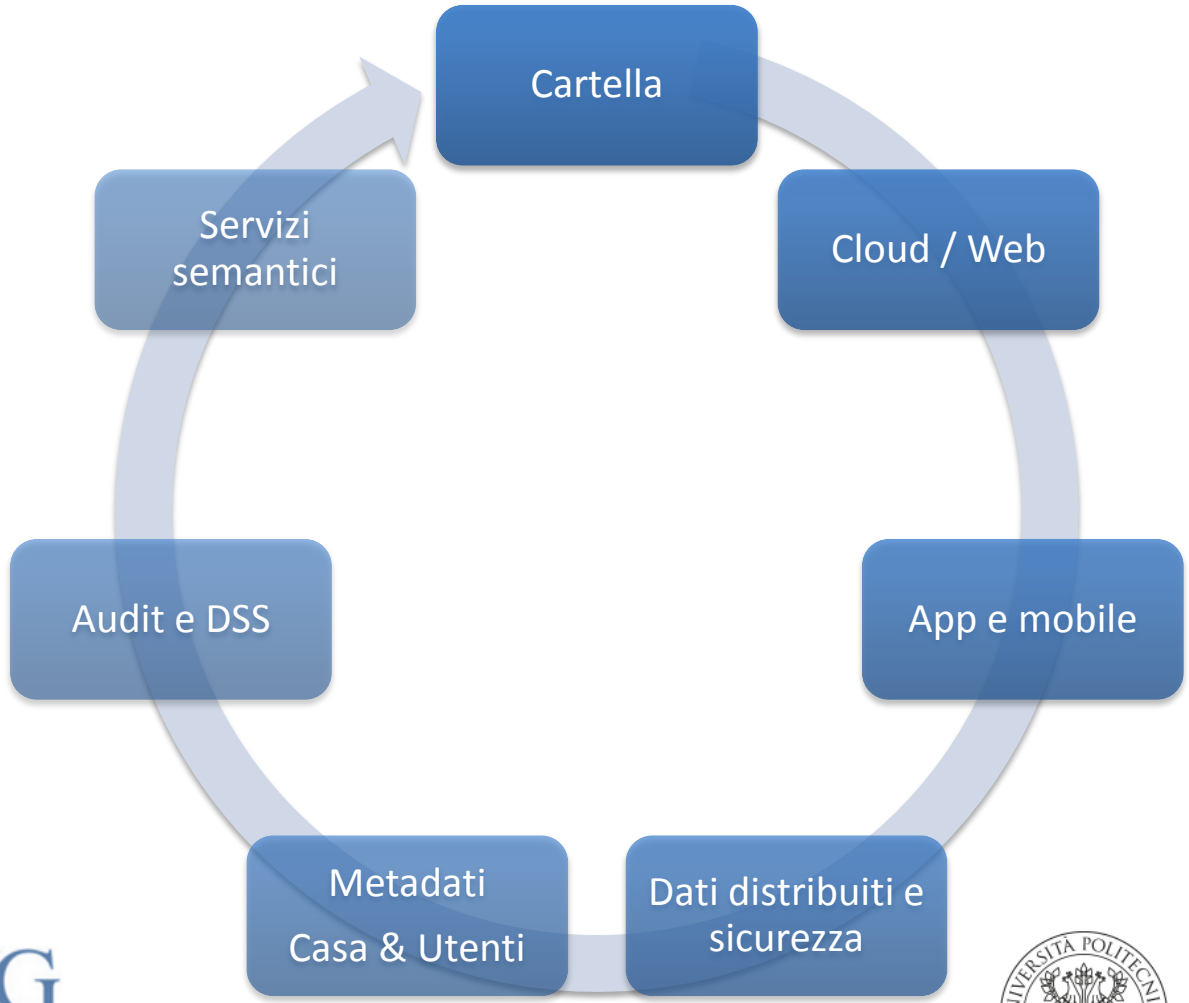
Anglano, C.; Gaeta, R.; Grangetto, M., **"Exploiting Rateless Codes in Cloud Storage Systems,"** *Parallel and Distributed Systems, IEEE Transactions on* , vol.PP, no.99, pp.1,1

M. Baldi, N. Maturo, E. Montali, F. Chiaraluce, **"AONT-LT: a Data Protection Scheme for Cloud and Cooperative Storage Systems"**, to be presented at the 2014 High Performance Computing & Simulation Conference (HPCS 2014) - Workshop on Security, Privacy and Performance in Cloud Computing, Bologna, Italy, July 2014.

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE

EVOLUZIONE

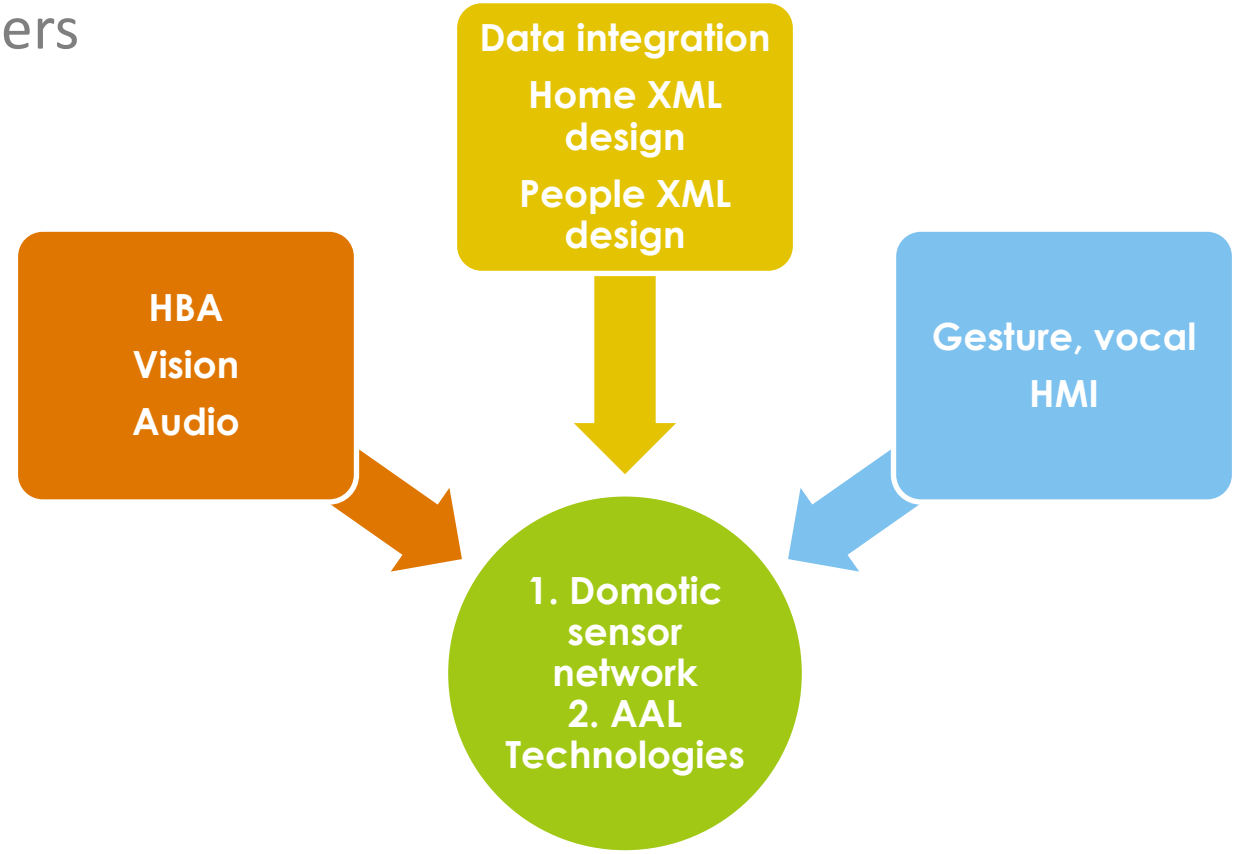


FIMG Federazione Italiana Medici di Famiglia

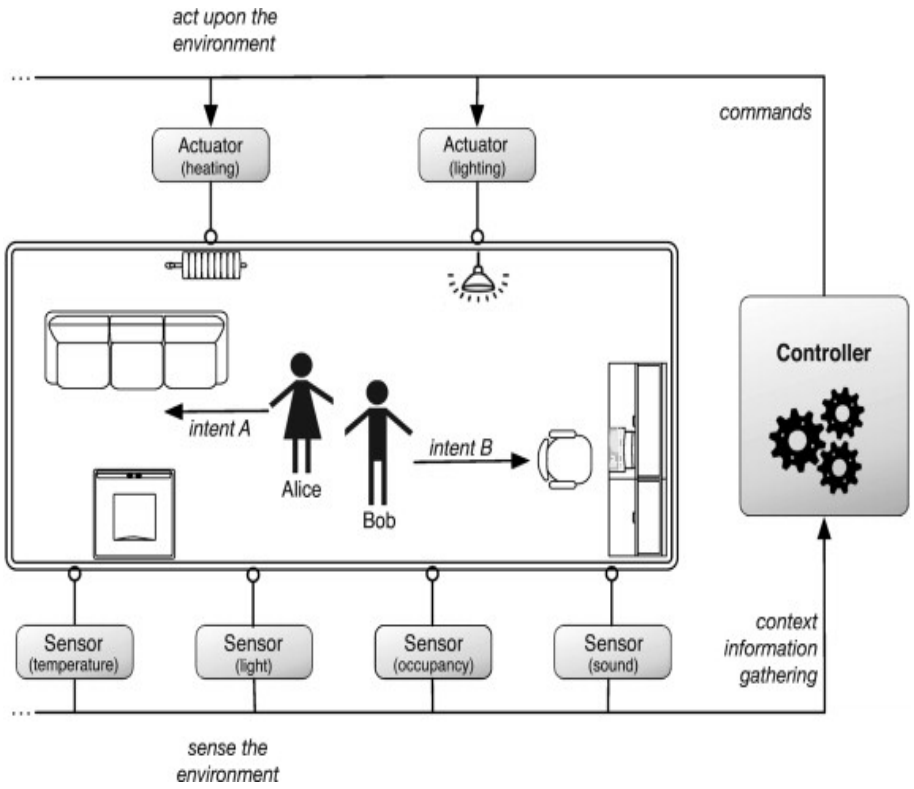
UNIVERSITÀ POLITECNICA DELLE MARCHE

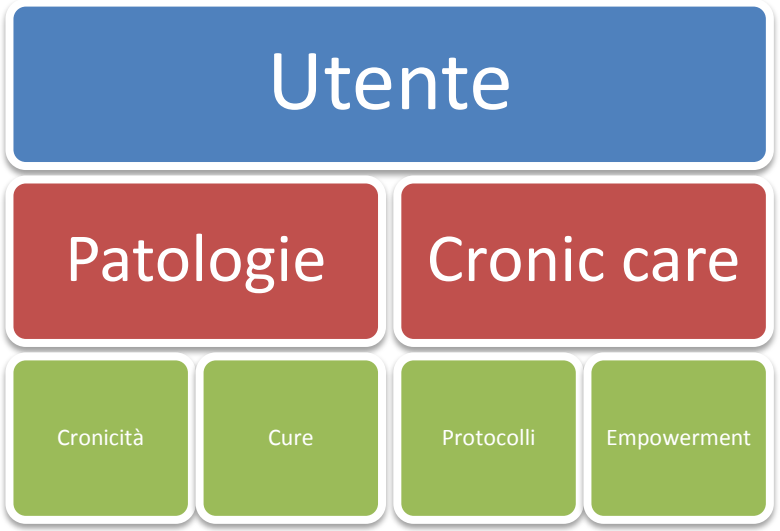
19 partners

2 RC



Chi abita la casa del futuro?





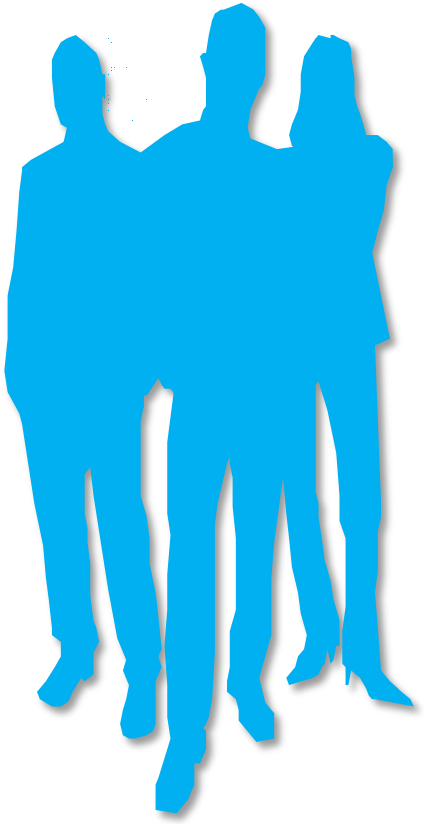
Un patient summary per l'AAL

Scenari aperti

- La frammentazione del dato come opportunità per la sicurezza
- L'accesso del paziente ai suoi dati & l'urgenza di identità digitali ampiamente diffuse
- Necessità di linee guida per la gestione sicura dei dati "moderne" (i.e. produttori software)
- Necessità di standard dati condivisi e completi
- La condivisione e l'accesso (normative)

FIMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE



Emanuele Frontoni
e.frontoni@univpm.it
@efrontoni

Thanks!

FIMMG Federazione Italiana Medici di Famiglia

UNIVERSITÀ POLITECNICA DELLE MARCHE