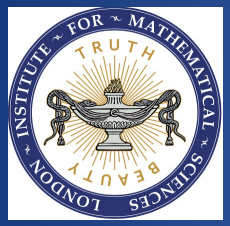
Gregorio D'Agostino *gregorio.dagostino@enea.it*

Agenzia per l'Energia le Nuove tecnologie e lo Sviluppo Economico sostenibile



London Institute of Mathematical Sciences
Lims.ac.uk

Network of Networks *www.netonets.org*

Univ. Roma II "TorVergata"
(questo corso)

Attività di Ricerca in atto:

- *Infrastrutture Critiche*
  - *Interdipendenza*
  - *Sicurezza e Resilienza*
  - *Reti di flusso (reti elettriche, comunicazione etc)*
  - *Systemic Risk*
  - *Resilienza*

- *Scienza della Complessità (Complexity Science):*
  - *Reti di reti (proprietà spettrali)*
  - *"Interest Diffusion in Social Network"*
  - *Analisi semantica dei linguaggi e corpus linguistici settoriali (esempio emergenze, incidenti etc)*
  - *Ricognizione automatizzata informazioni in rete.*

Considerazioni generali

Cercheremo di definire tutti i concetti/teoremi "ab initio" e fare esercizi su tutto.

- *Ricognizione indirizzi elettronici: mandare un messaggio a gregorio.dagostino@enea.it con nome, cognome, Subject: Enrollment e info:*
- *Iscritto a Ingegneria Medica?*
- *Disponibilità Portatile?*
- *OS: Linux (Debian, Ubuntu,..) Mac, Windows*
- *Linguaggi programmazione: Pyton, C (c++), Fortran (F95), Java, …*
- *Programmi di calcolo: Octave, Mathlab, etc*

Mathematica, Maxima etc

Autovalutazione

Faremo una autovalutazione/ valutazione (anonima) oltre quella della facoltà:

- *Quali temi abbiamo trattato? (10 parole)*
- *Quanta parte ho seguito/interiorizzato? (0-100%)*
- *Di quanta parte so fare gli esercizi? (0-100%)*
- *Si capisce la finalità verso l'obiettivo generale? (0-100%)*
- *Si intuiscono applicazioni pratiche? (0-100%)*

Motivazioni per la Sicurezza Informatica

- Ci sono Leggi Europee ed Italiane da rispettare
- Ci sono Pericoli economici ed anche fisici:
  - Perdite di dati (Clienti, forniture, etc)
  - Manipolazione di strumenti (e dati raccolti)
  - Perdita volume di affari
  - Responsabilità penali e civili: Carcere fino a 5 anni; Multe 100-200K€ Salvo reati o responsabilità civili maggiori.
  - Avvento dei registri distribuiti

Pericolo reale: Critto-Ricattatori

Hollywood hospital held to ransom by hackers

Dave Lee (http://www.bbc.com/news/technology-35584081)

***Ransomware** is a growing menace for computer users - but when a hospital is targeted, it makes the disruption far more serious.*

Computer systems at Hollywood Presbyterian Medical Center have been offline for more than a week following a ransomware attack.

*According to local news sources, hackers were said to have demanded **$3.4m** (£2.4m) to provide the codes to unlock the stolen data.*

The hospital has confirmed the attack took place, but has not commented on the ransom.

A voicemail message at the hospital reassures patients that medical records had not been accessed by the hackers.

Investigations into the source of the attack - which hospital officials said appeared to be random rather than targeted at the facility - are being conducted by the FBI, Los Angeles Police and computer forensics experts hired by the hospital.

The hospital insists that day-to-day operations have not been impacted, although many tasks normally carried out on computer are now being done on paper, much to the frustration of staff.

Patients are also being told they must travel to pick up medical test results in person rather than receive them electronically.

Critto-Ricattatori

(https://lifars.com/2016/02/hackers-encrypt-hollywood-hospital-systems-with-ransomware/

Fox News spoke to computer forensics veteran Eric Robi who gained knowledge of the hacking attack.

"The hackers have demanded, I think 9,000 ***bitcoin*** *or so that's a little over $3 Million," Robi revealed. "It's an unfortunate hack, a ransomware hack where they're asking for money in exchange for unlocking records at the hospital," Robi added.*

By today's rates, that figure is closer to $3.6 million, a significant ransom figure sought in exchange for the decryption key that will enable the hospital to regain access to key systems.

American Medical Association

http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/security-standards.page?

HIPAA: Health Insurance Portability and Accountability Act

September 23, 2013 was HIPAA privacy and security deadline

The U.S Department of Health & Human Services (HHS) recently adopted new rules which make changes to existing privacy, security and breach notification requirements in what is often referred to as the final "HIPAA Omnibus Rule.

AMA AMERICAN MEDICAL ASSOCIATION

Security Standards and Risk Analysis

The HIPAA Security Standards require physicians to protect the security of patients' electronic medical information through the use of procedures and mechanisms that protect the confidentiality, integrity, and availability of information. As of 2005, physicians must have in place administrative, physical, and technical safeguards that will protect electronic health information that the physician collects, maintains, uses, and transmits.

Access the AMA's toolkit to help your practice comply with the new HIPAA rules that were effective September 23, 2013, ”

HIPAA privacy and security toolkit: Helping your practice meet new compliance requirements." This toolkit provides step-by-step guidance to help your practice understand these rules and participate in a formal compliance plan designed to ensure all the requirements are met.

In Europa

General Data Protection Regulation (GDPR)

Entrato in vigore il **30 Maggio 2018** – Norme intepretative

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

*"Per **violazione dei dati**, personali o meno, generalmente si intende il risultato di azioni, accidentali o volutamente illecite, che compromettono la **sicurezza delle informazioni** che un'organizzazione, sia essa pubblica o privata, intende mantenere riservate, integre e disponibili esclusivamente per le proprie esigenze di business e nel rispetto della legge."*

Programma Orientativo I

- *Generalità **Sicurezza**, Sicurezza informatica, Sicurezza informatica in Medicina. Vulnerabilità, Rischio, resilienza, attacco, minaccia… Protezione e sicurezza. Protezione e difesa dei dati: **confidenzialità, disponibilità e integrità. Ingegneria Sociale***
- ***Criptografia antica**. Criptazione di Cesare, Scitale, Augusto, Atbash, affine, Vigenere, Alberti, Enigma. Scambio chiavi in antichità. Steganografia. Esercizi con Octave Cifratura, decifratura e decrittazione.*
- ***Complessità**: procedure, algoritmi, macchine di Touring, MonteCarlo, Las Vegas, scaling…*
- *Cenni di **Teoria della Probabilità**: Spazio di probabilità. Teoria dei linguaggi. Legge grandi numeri. Teoremi di Jansen e di Shennon. Entropia delle sorgenti Markoviane. Conseguenze in criptazione.*
- *Cenni di **Teoria dell'informazione**: entropia di Shennon, informazione reciproca, diseguaglianza di Jansen, cifrari ideali e cifrari perfetti.*
- *Cenni di **Teoria dei numeri** (anelli, gruppi, campi, classi, primalità, alg. Eulcide, th. Gauss, Th. Resti cinese, Piccolo Th. Di Fermat, Funzione di Eulero, Funzione di Charlmichael etc). Ricerca di numeri primi. Crivelli.*
- *Basi della **Criptazione moderna**. Generazione di numeri casuali e pseudo. Criptazione a chiave condivisa e criptazione asimmetrica. Scambio chiavi. RSA, DES, Certificazione…*

Programma Orientativo II

.

- *Cenni di **Teoria delle Reti**. Reti informatiche. I livelli OSI, Protocolli. TCP/IP Ridondanze. Integrità Hash functions. Servers, routers, hubs, DNS (darknet), Proxy, Cloud… - Disponibilità – Esercitazioni*

- *Cenni di **Sicurezza in Rete:** Integrità: CRC; Paradosso compleanno; Hash Functions. SHA; certificazione; SSH, TLS, etc.*
- ***Autenticazione.** Sistemi biometrici. Informazioni esclusive. Smart cards. Dispositivi OTP (password usa e getta). Firma digitale. Certificazioni. Kerberos.*

- *Principali **Attacchi** informatici. **DDOS**, **Man in the Middle**, Reply, Sniffing, Spooffing, Ingegneria sociale. Furto d'identità (Phishing). Stuxnet. Cryptlocker. Tubo di gomma (manganello).*

- ***Buone pratiche**. Backup; database; Pianificazione sicurezza. Classificazione informazione e Schemi di autorizzazione. Allocazione esterna: SLA.*
- *Cenni protezione operativa: Descrizioni malware (worm, virus), antivirus e OS patching.*

Testi

- W. Stalling & L. Brown *"Computer Security"*

(io ho 2° Ed Pearson **ISBN-13:** 978-0132775069 **ISBN-10:** 0132775069)

È uscita la 3. (**Sicurezza**)

- A Tanenbaum "*Computer Networks*" Pearson 2011 8-th Ed ISBN 978-81-7758-165-2 /S. Gai, P Montessori, P Nicoletti "*Dal Cablaggio all'internet Working*" Scuola Superiore G. reiss Romoli ISBN 88 85280 22 6 (**Reti** – Qualunque libro di reti va bene)
- G.M. Piacentini Cattaneo "*Algebra*" Zanichelli 2012 (**Th. dei numeri** anche qui va bene un qualunque libro base)
- Gnedenko "*Teoria della Probabilità*" Ed. Riuniti 1979 (**Probabilità**) [esiste anche della MIR]
- **Teoria dell'informazione** *Francesco Fabris "Teoria dell'informazione, codici, cifrari" Bollati Boringhieri*

General Data Protection Regulation

Il GDPR è la normativa Europea più recente sulla protezione dei dati.

La legge 20 novembre 2017, n. 167 Art 28: recepisce (insieme ad altre direttive Europee)

Il GDPR e

la Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015

Alcuni principi: “Persone fisiche” – “Consenso”

*“Le **persone fisiche** possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle. “*

*Il **consenso** dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.*

Alcuni principi: "**Dati relativi alla Salute**"

*(35) Nei **dati personali relativi alla salute** dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio (1); un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.*

Alcuni principi: “**Sicurezza**”

Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire ***la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi*** *che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di* ***emergenza*** *informatica (****CERT****), gruppi di intervento per la sicurezza informatica in caso di* ***incidente*** *(****CSIRT****), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «****blocco di servizio****» e ai danni ai sistemi informatici e di comunicazione elettronica.*

Alcuni principi: "**Finalità**"

*"Il trattamento dei dati personali per **finalità** diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti."*

Alcuni principi: **Interesse Pubblico**

(54) Il trattamento di categorie particolari di dati personali può essere necessario per motivi ***di interesse pubblico*** *nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. In tale contesto, la nozione di «****sanità pubblica****» dovrebbe essere interpretata secondo la definizione del regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio (1): tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito.*

Alcuni principi: “**diritto all'oblio**”

*(66) Per rafforzare il «**diritto all'oblio**» nell'ambiente online, è opportuno che il diritto di **cancellazione** sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi **link** verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti **misure ragionevoli** tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.*

General Data Protection Regulation

Alcuni principi: “Diritto di rettifica (art. 16)”

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Alcuni principi: "**Registri trattamenti - Tracciabilità**"

*(82) Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un **registro** delle **attività** di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.*

Alcuni principi: "**Registri trattamenti - Tracciabilità**"

*(82) Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un **registro** delle **attività** di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.*

General Data Protection Regulation

Alcune figure:

-“**Data Protection Officier**” (RPD responsabile protezione dati in italiano) è obbligatorio in alcuni casi della pubblica amministrazione, facoltativo in molti casi, ma spesso utile. Vigila sulla predispozizione ed attuazione di misure adeguate.

-**Titolare trattamento dei dati**: è, secondo l’art. 41f del (d.lgs. 196/2003), «la **persona fisica, giuridica**, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza

Leggi in Italia

- *Decreto Legislativo 30 giugno 2003, n. 196*

Art. 1

(Diritto alla **protezione** dei dati personali)

“Chiunque ha diritto alla protezione dei dati personali che lo riguardano.”

Art. 3

*(Principio di **necessita'** nel trattamento dei dati)*

“I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalita' perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalita' che permettano di identificare l'interessato solo in caso di necessita'.”

Art. 4 (Definizioni)

.....

b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

*c) "dati identificativi", i dati personali che permettono **l'identificazione** diretta dell'interessato;*

*d) "**dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonche' i dati personali idonei a **rivelare lo stato di salute e la vita sessuale;***

Art. 11

(Modalita' del trattamento e requisiti dei dati)

I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

*d) pertinenti, completi e **non eccedenti rispetto alle finalita'** per le quali sono raccolti o successivamente trattati;*

*e) **conservati** in una forma che consenta **l'identificazione dell'interessato** per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.*

Art. 20 cont

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

*e) **protezione degli strumenti elettronici** e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;*

*f) adozione di **procedure per la custodia** di **copie** di sicurezza, il ripristino della **disponibilita**' dei dati e dei sistemi;*

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitart.

Art. 20

(Principi applicabili al trattamento di dati sensibili)

Il trattamento dei dati sensibili da parte di soggetti pubblici e' consentito solo se ***autorizzato*** *da espressa disposizione di legge nella quale sono specificati i tipi di' dati che possono essere trattati e di operazioni eseguibili e le finalita' di rilevante interesse pubblico perseguite.*

Art. 34 (Trattamenti con strumenti elettronici)

1. *Il trattamento di dati personali effettuato con strumenti elettronici e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:*

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di ***autorizzazione****;*

Art. 91

(Dati trattati mediante carte)

1. Il trattamento in ogni forma di dati idonei a rivelare lo stato di salute o la vita sessuale eventualmente registrati su carte anche non elettroniche, compresa la carta nazionale dei servizi, o trattati mediante le medesime carte e' consentito se necessario ai sensi dell'articolo 3, nell'osservanza di misure ed accorgimenti prescritti dal Garante nei modi di cui all'articolo 17.

Art. 94

*(**Banche di dati**, registri e schedari in ambito sanitario)*

1. Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, e' effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri gia' istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso:

a) il **registro nazionale dei casi di mesotelioma** asbesto-correlati istituito presso l'Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), di cui all'articolo 1 del decreto del Presidente del Consiglio dei ministri 10 dicembre 2002, n. 308;

b) la banca di dati in materia di sorveglianza della **malattia di Creutzfeldt-Jakob** o delle varianti e sindromi ad essa correlate, di cui al decreto del Ministro della salute in data 21 dicembre 2001, pubblicato nella *Gazzetta Ufficiale* n. 8 del 10 gennaio 2002;

c) il registro nazionale delle **malattie rare** di cui all'articolo 3 del decreto del Ministro della sanita' in data 18 maggio 2001, n. 279;

d) i registri dei **donatori di midollo** osseo istituiti in applicazione della legge 6 marzo 2001, n. 52;

e) gli schedari dei **donatori di sangue** di cui all'articolo 15 del decreto del Ministro della sanita' in data 26 gennaio 2001, pubblicato nella *Gazzetta Ufficiale* n. 78 del 3 aprile 2001.

ALLEGATO B

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalita' tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

*1. Il trattamento di dati personali con strumenti elettronici e' consentito agli incaricati dotati di **credenziali** di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.*

ALLEGATO B (cont)

*2. **Le credenziali** di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.*

*3. Ad ogni incaricato sono assegnate o associate individualmente una o piu' credenziali per l'**autenticazione**.*

*4. Con le istruzioni impartite agli incaricati e' prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente **custodia dei dispositivi** in possesso ed uso esclusivo dell'incaricato.*

*5. **La parola chiave**, quando e' prevista dal sistema di autenticazione, e' composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed e' modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave e' modificata almeno ogni tre mesi.*

ALLEGATO B (cont)

*6. Il **codice per l'identificazione**, laddove utilizzato, non puo' essere assegnato ad altri incaricati, neppure in tempi diversi.*

*7. Le **credenziali di autenticazione** non utilizzate da almeno sei mesi sono **disattivate**, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.*

8. Le credenziali sono disattivate anche in caso di perdita della qualita' che consente all'incaricato l'accesso ai dati personali.

*9. Sono impartite istruzioni agli incaricati per **non lasciare incustodito e accessibile** lo strumento elettronico durante una sessione di trattamento.*

ALLEGATO B (cont)

*10. Quando l'accesso ai dati e agli strumenti elettronici e' consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalita' con le quali il titolare puo' assicurare la **disponibilita'** di **dati o strumenti** elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessita' di operativita' e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali e' organizzata garantendo la relativa **segretezza** e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.*

Sicurezza Informatica & Leggi

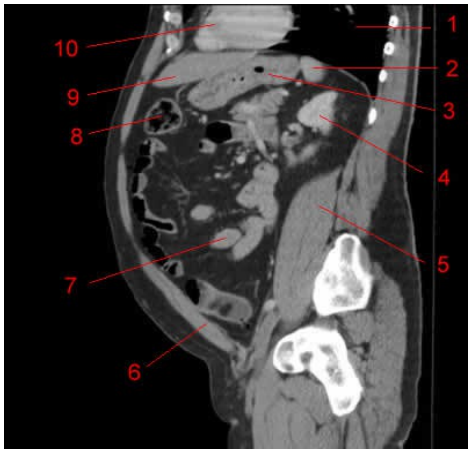
- ***Dove** avvengono i reati informatici?*
- *Chi ha la giurisdizione? Come procede?*
- *Si può utilizzare il diritto Nazionale?*
- *Diritto Comparato?*
- *Si può usare il diritto Internazionale?*
- *Si possono inibire i canali di comunicazione?*
- *Si può **contrattaccare**?*
- *SI possono imporre **Standard**? E' utile?*
- *Si possono imporre **Procedure Certificate**?*

Servizi Esistenti (Privato)

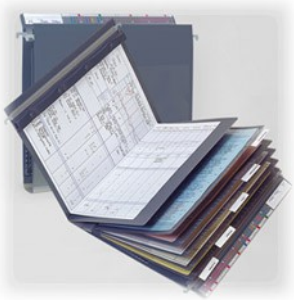
- *In molte cliniche esistono sistemi centralizzati che consento di accedere a molti dati riservati:*

- *Radiografie, TAC,*

Analisi per immagine



- *Cartelle cliniche (anamnesi – storia paziente)*
- *Analisi cliniche di laboratorio*



Pratiche telematiche (in fieri)

- *Teleconsulting (telefono, mail, skype, whatsapp etc)*
- *Telediagnostica (dispositivi automatizzati di monitoraggio sul paziente interfacciati con il computer del medico) IoT*
- *Prescrizioni Mediche: per adesso esiste solo per medico paziente e farmacie, ma va stampato. In futuro le unità sanitarie riceveranno per via telematica i dati.*
- *L'INPS riceve già adesso le diagnosi a fine giustificazione assenza per malattia.*

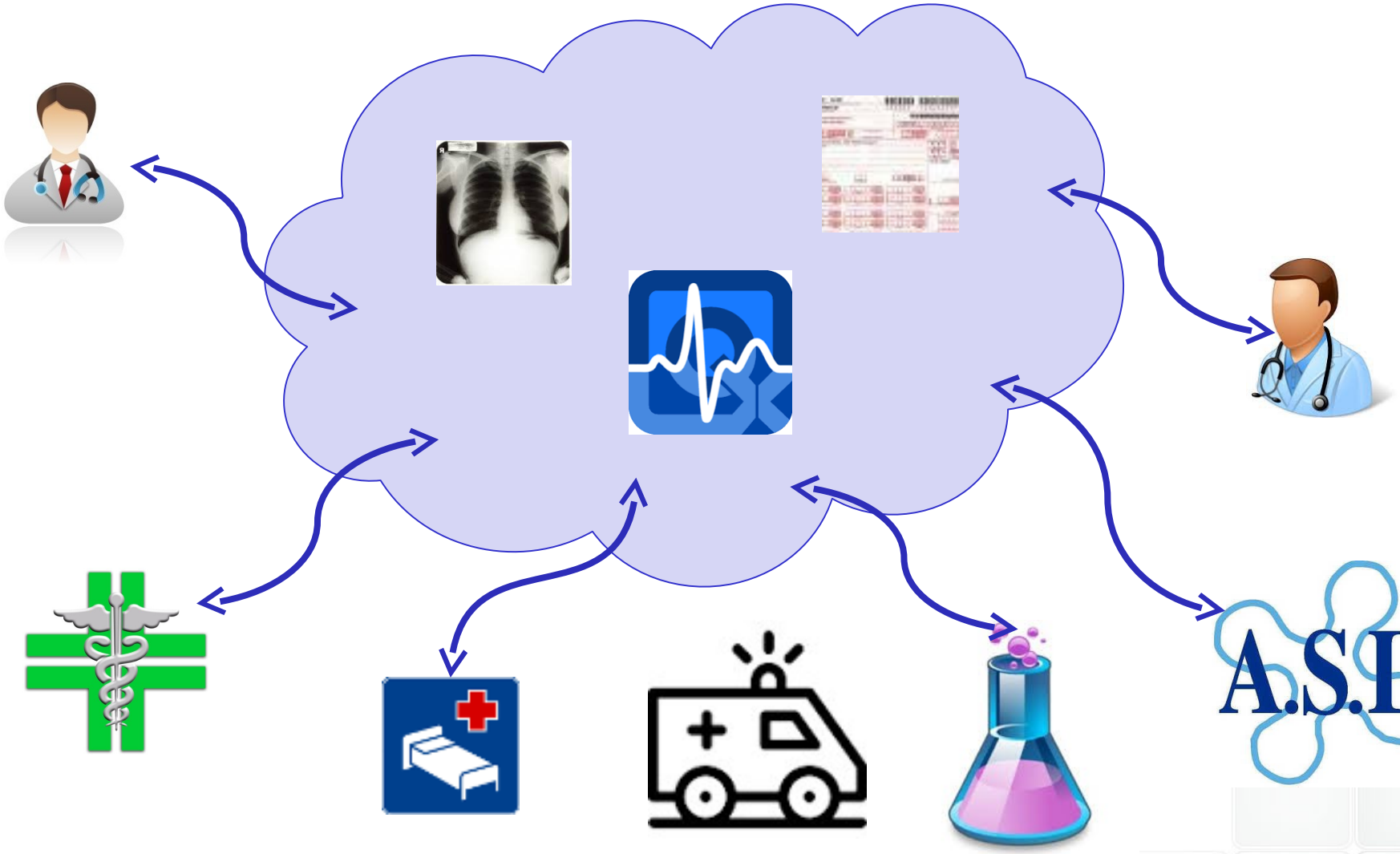
Sanità Digitale Sez IV Legge 294/2012

Art. 12 Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario

1. Il fascicolo sanitario elettronico (FSE) e' l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito.

2. Il FSE e' istituito dalle regioni e province autonome, conformemente a quanto disposto dai decreti di cui al comma 7, entro il 30 giugno 2015, nel rispetto della normativa vigente in materia di protezione dei dati personali, a fini di: a) prevenzione, diagnosi, cura e riabilitazione; b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; c) programmazione sanitaria, verifica delle qualita' delle cure e valutazione dell'assistenza sanitaria. Il FSE deve consentire anche l'accesso da parte del cittadino ai servizi sanitari on line secondo modalita' determinate nel decreto di cui al comma 7.

Sanità nel Cloud?



Info in tasca? Diagnosi continua?

E-Health

-Tessera sanitaria: Contiene informazioni

-Centro unificato di prenotazione (CUP) (Nel lazio al Tel.)

-Prescrizione elettronica, pagamento online delle prestazioni, consegna in modalità digitale del referto medico (Nel Lazio ancora in fieri)

-Cartella clinica digitale

-Il fascicolo sanitario elettronico (FSE Legge 179/2012)

-Sistemi di sorveglianza e registri in ambito sanitario

-Certificati di malattia online (INPS) Art 7 Legge 294/2012

Prime leggi: Legge 338 /2000

Art. 87. Il Nuovo Sistema Informativo Sanitario (NSIS)

*(Monitoraggio delle **prescrizioni mediche, farmaceutiche, specialistiche e ospedaliere**)*

1. Nel quadro delle competenze di governo della spesa da parte del Ministero del tesoro, del bilancio e della programmazione economica, di garanzia verso il cittadino di appropriatezza ed efficacia delle prestazioni di cura da parte del Ministero della sanità, e nel rispetto dei compiti attribuiti alle regioni in materia sanitaria, al fine di migliorare il monitoraggio della spesa sanitaria nelle sue componenti farmaceutica, diagnostica e specialistica, e di semplificare le transazioni tra il cittadino, gli operatori e le istituzioni preposte, è introdotta la gestione informatizzata delle prescrizioni relative alle prestazioni farmaceutiche, diagnostiche, specialistiche e ospedaliere, erogate da soggetti pubblici e privati accreditati. Tutte le procedure informatiche devono garantire l'assoluto anonimato del cittadino che usufruisce delle prestazioni, rispettando la normativa a tutela della riservatezza. Ai dati oggetto della gestione informatizzata possono avere accesso solo gli operatori da identificare secondo quanto disposto dal decreto legislativo 30 luglio 1999, n. 282.

2. Il sistema di monitoraggio interconnette i medici e gli altri operatori sanitari di cui al comma 1, il Ministero della sanità, il Ministero del tesoro, del bilancio e della programmazione economica, le regioni, la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, le aziende sanitarie locali e dispone, per la consultazione in linea e ai diversi livelli di competenza, delle informazioni relative:

a) ai farmaci del Servizio sanitario nazionale;

b) alle diverse prestazioni farmaceutiche, diagnostiche e specialistiche erogabili;

Prime leggi: Legge 338 /2000 (cont)

c) all'andamento dei consumi dei farmaci e delle prestazioni;

d) all'andamento della spesa relativa.

3. Entro novanta giorni dalla data di entrata in vigore della presente legge il **Ministero della sanità**, di concerto con il Ministero del tesoro, del bilancio e della programmazione economica, e sentita la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, emana i regolamenti e i decreti attuativi, individuando le risorse finanziarie nell'ambito di quelle indicate dall'articolo 103, definendo le modalità operative e i relativi adempimenti, le modalità di trasmissione dei dati ed il flusso delle informazioni tra i diversi organismi di cui al comma 2.

4. Le soluzioni adottate dovranno rispettare le norme sulla sicurezza e sulla riservatezza dei dati secondo le leggi vigenti e risultare coerenti con le linee generali del processo di evoluzione dell'utilizzo dell'informatica nell'amministrazione.

5. Entro il 1º gennaio 2002 o le diverse date stabilite con i decreti attuativi di cui al comma 3, tutte le prescrizioni citate dovranno essere trasmissibili e monitorabili per via telematica.

6. Per l'avvio del nuovo sistema informativo nazionale del Ministero della sanità, nonché per l'estensione dell'impiego sperimentale della carta sanitaria prevista dal **progetto europeo "NETLINK**" è autorizzata per l'anno 2001 la spesa, rispettivamente, di lire 10 miliardi e di lire 4 miliardi.

7. All'articolo 38, quarto comma, del regolamento per il servizio farmaceutico, approvato con regio decreto 30 settembre 1938, n. 1706, le parole: "I farmacisti debbono conservare per la durata di cinque anni copia di tutte le ricette spedite" sono sostituite dalle seguenti: "I farmacisti debbono conservare per sei mesi le ricette spedite concernenti preparazioni estemporanee".

Informazioni indirette
(“mondo di mezzo” **Data Analytics**)

*Alcuni **dati amministrativi** possono contenere indirettamente dati sensibili medici:*

*-Ricevuta di un intervento ad un **chirurgo oculistico***

*-Oppure **Oncologo***

*-Ricevuta acquisto **protesi mammaria***

*-Ricevuta **visita specialistica (**può bastare anche solo **il nome del medico)**.*

-Ricevuta analisi cliniche o diagnostiche

Dall’insieme si può risalire facilmente alle patologie del paziente.

Non solo conoscere

- *Come vedremo alcuni dispositivi sono controllati cibernetica mente e la loro manipolazione può portare a danni o perfino alla morte del paziente.*
- *La manomissione delle terapie può causare danni*
- *La gestione di impianti (antincendio, forniture di acqua, farmaci, energia etc) può essere oggetto di attacco. (SCADA)*
- *La manipolazione delle informazioni sulle presenze dei pazienti, dei mezzi, disponibilità ricoveri e del personale può essere un'arma formidabile etc*

Attaccanti

Chi ha interesse alle informazioni mediche:

- Compagnie assicurative

- Specialisti e studi consociati (Marketing)

- case farmaceutiche

- nemici personali

- datori di lavoro anche potenziali

- soci in affari

- parenti e amici curiosi o interessati

Messaggio Lezione

- *La **sicurezza informatica** è essenziale per una corretta gestione delle strutture Mediche operative ed informazionali.*
- *Esistono **pericoli reali** già attuati (es. critto-ricatti)*
- *Le **leggi** Italiane riguardano al momento solo la **Privacy** e il monitoraggio delle prestazioni, ma sono destinate ad aumentare.*
- *La domotica e l'internet of things (IoT), **Digital Society** in generale porteranno ad un aumento di richiesta di sicurezza.*
- *Essendo Internet abbastanza a-geografica è difficile applicare le leggi. **Giurisdizione***

Cognitiones ac Agenda (Info & ToDo)

Sito dove troverete le lezioni ed esercizi svolti:

gordion.casaccia.enea.it/SicurezzaInformatica/

Lectures

Exercises

Ricordatevi di:

-Registrarvi al corso tramite email (con info richieste) a gregorio.dagostino@enea.it

-Firmare il foglio presenze quando venite a lezione se le faremo