



**Dott. Tarcisio Niglio, M.D.**

Servizio Informatico  
Istituto Superiore di Sanità  
Roma

**Sicurezza & Privacy  
nella gestione di un Registro Nazionale:  
l'esperienza ISS con il CNMR**

Prevenzione Italia - CLUSIT - Roma 29 ottobre 2004



**Dott. Tarcisio Niglio, M.D.**

Servizio Informatico  
Istituto Superiore di Sanità  
Roma

**Sicurezza & Privacy  
nella gestione di un Registro Nazionale:  
l'esperienza dell'ISS**

Prevenzione Italia - CLUSIT - Roma 8 aprile 2005



**Dott. Tarcisio Niglio, M.D.**

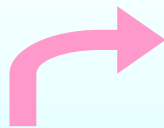
Servizio Informatico  
Istituto Superiore di Sanità  
Roma

**Sicurezza & Privacy  
di alcuni Archivi Sanitari dell'ISS:  
stato dell'arte**

Prevenzione Italia - CLUSIT - Roma venerdì 17 giugno 2005

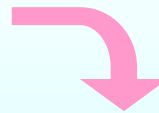


**Archivio Sanitario Nazionale**



**Sig. Xyz**  
**Cartella  
clinica**  
**Risultati  
Laboratorio**

**TRASMISSIONE**  
cartacea  
email  
online

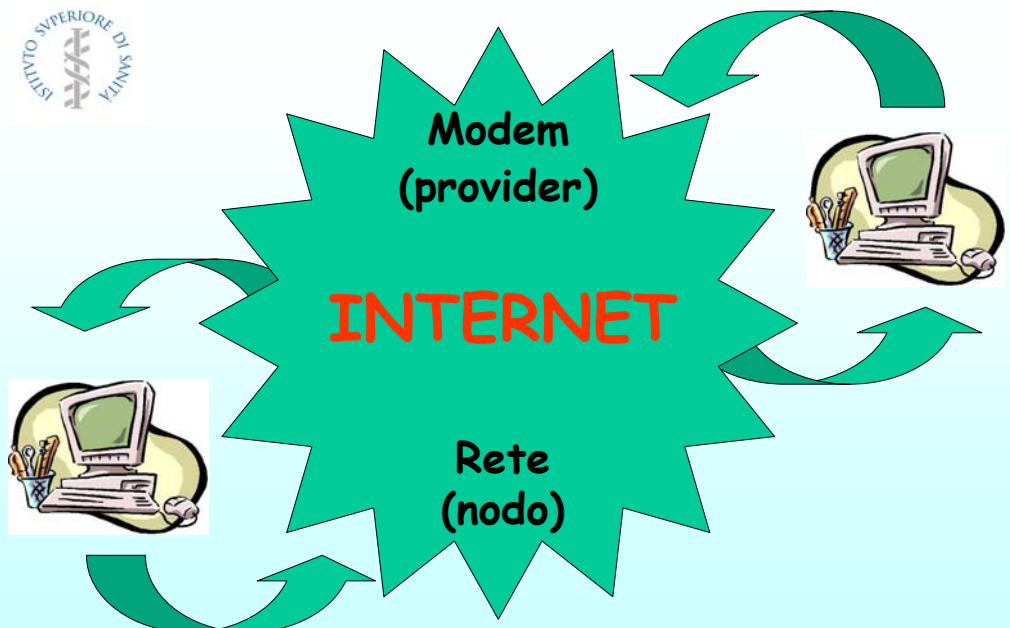




# TELEMATICA

Tecnologie  
Informatiche  
di Telecomunicazione:

- Hardware
- Software





# Norme sulla riservatezza del contenuto dei dati scambiati



## Art. n.622 del Codice Penale

### Rivelazione di segreto professionale:

**Chiunque**, avendo notizia, per ragione del proprio stato o ufficio, o della propria **professione** o arte, di un segreto, lo rivela senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocimento, con la **reclusione fino a un anno** o con la multa da L. 60.000 a 1 milione (c.p.326).



### **Art. n.9 del Codice di Deontologia Medica della FNOMCeO**

**Il medico deve mantenere il segreto** su tutto ciò che gli è confidato o che può conoscere in ragione della sua professione; ... omissis ...

Costituiscono **giusta causa di rivelazione**, oltre alle inderogabili ottemperanze a specifiche norme legislative (referti, denunce, notifiche e certificazioni **obbligatorie**):

a) - **la richiesta o l'autorizzazione da parte della persona assistita** o del suo legale rappresentante, previa specifica informazione sulle conseguenze o sull'opportunità o meno della rivelazione stessa;

b) - l'urgenza di **salvaguardare la vita** o la salute dell'interessato o di terzi, nel caso in cui **l'interessato stesso non sia in grado** di prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere e di volere;

c) - l'urgenza di **salvaguardare la vita** o la salute di terzi, anche **nel caso di diniego** dell'interessato, ma **previa autorizzazione del Garante** per la protezione dei dati personali

**La morte del paziente non esime il medico dall'obbligo del segreto.**

**Il medico non deve rendere al Giudice testimonianza** su ciò che gli è stato confidato o è pervenuto a sua conoscenza nell'esercizio della professione.

**La cancellazione dall'albo non esime moralmente** il medico dagli obblighi del presente articolo.



### **Art. n.33 e 169 del DECRETO LEGISLATIVO 30 giugno 2003, n. 196**

Nel quadro dei più generali **obblighi di sicurezza** di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di **protezione** dei dati personali.

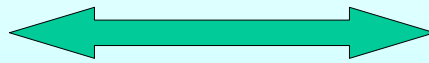
Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'**arresto** sino a **due anni** o con l'ammenda da **10.000** euro a **50.000** euro.

## LIVELLI DI SICUREZZA



**SERVER**

TRASFERIMENTO



**CLIENT**

## Collegamento modem diretto



**modem**



**modem**



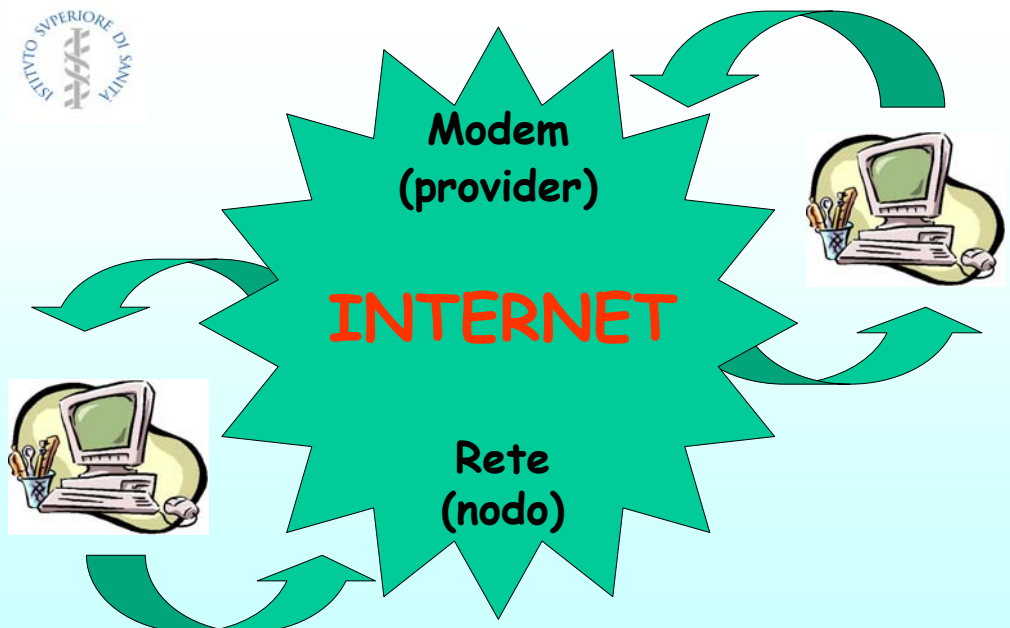
**Collegamento "lento" tra PC "uguali"**





## Velocità di connessione

Modem	56 KB
ISDN	64 KB
Doppia ISDN	128 KB
ADSL	1.280 KB
ADSL "fast"	4.096 KB
WAN "high speed"	50.000 KB





## Indirizzo IP (Internet Protocol)

**172.16.1.131**

Equivale al mnemonico

**www.iss.it**



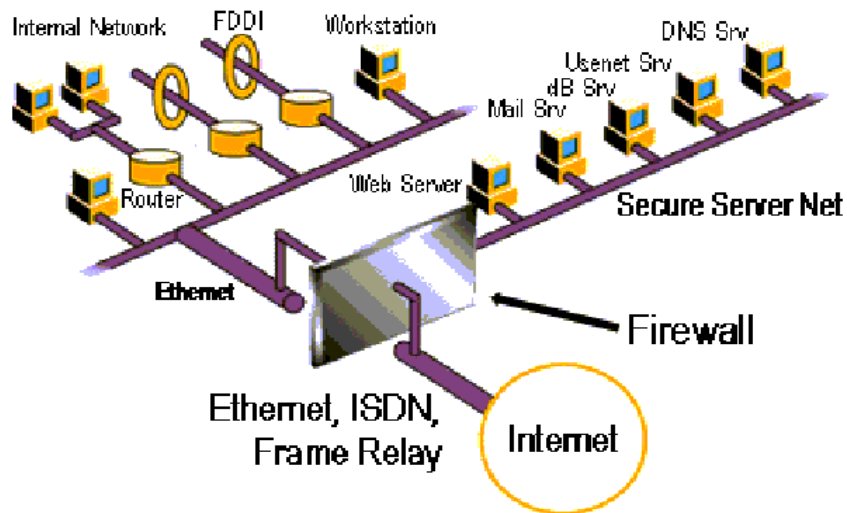
## Indirizzo IP del gateway intranet

**10.200.0.1**

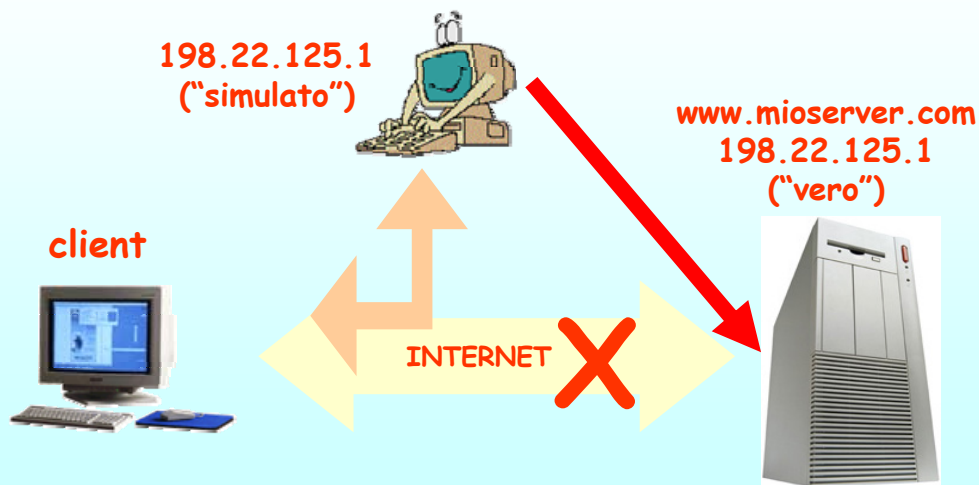
Molteplici sottoindirizzi

**10.200.xxx.xxx**

## Struttura di un nodo



## IP spoofing



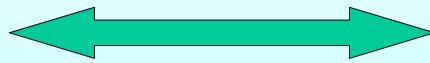


## LIVELLI DI SICUREZZA



**SERVER**

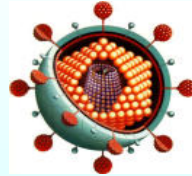
TRASFERIMENTO



**CLIENT**



**Virus**  
**Worm**  
**Malware**  
**Spyware**  
**Network worm**



**X5O!P%#@AP[4\PZX54(P^)^7CC)7}\$  
 EICAR-STANDARD-ANTIVIRUS-  
 TEST-FILE!\$H+H\***



**Inizio del listato  
 esadecimale del  
 codice binario del**

**Virus  
 JS\_CBASE.EXP1**

**Aliases:  
 Troj/Mimail-A  
 W32.Mimail.A@mm**

```
000000 4b50 0403 000a 0000 0000 43f3 2f56 45a3
000001 490a 5a55 0000 5a55 0000 000c 0000 656d
000002 7373 6761 2e65 7468 6c6d 494d 454d 562d
000003 7265 6973 6e6f 203a 2e31 0a30 6f43 746e
000004 6e65 2d74 6f4c 6163 6974 6e6f 463a 6c69
000005 3a65 2f2f 6f66 2e6f 7865 0a65 6f43 746e
000006 6e65 2d74 7254 6e61 6673 7265 452d 636e
000007 646f 6e69 3a67 6220 6e69 7261 0a79 4d0a
000008 905a 0300 0000 0400 0000 ff00 00ff b800
000009 0000 0000 0000 4000 0000 0000 0000 0000
00000a 0000 0000 0000 0000 0000 0000 0000 0000
00000b 0000 0000 0000 0000 0000 8000 0000 0e00
00000c ba1f 000e 09b4 21cd 01b8 cd4c 5421 6968
00000d 2073 7270 676f 6172 206d 6163 6e6e 746f
00000e 6220 2065 7572 206e 6e69 4420 534f 6d20
00000f 646f 2e65 0d0d 240a 0000 0000 0000 5000
000010 0045 4c00 0301 a800 a39d 003f 0000 0000
```



**Riassumendo  
il versante hardware:**

**L'unico PC "sicuro" al 100%  
è quello spento  
e ... possibilmente  
NON in rete.**

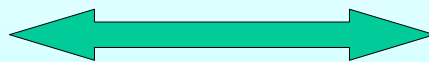


**LIVELLI DI  
SICUREZZA**



**SERVER**

**TRASFERIMENTO**



**CLIENT**

# Metodi di crittografia



Lisandro  
(400 a.C.)

Metodo della  
striscia di cuoio  
su bastone



## Cifrario di Giulio Cesare (100-40 a.C.)

Chiario a b c d e f g h i j k l m n o p q r s t u v w x y z  
Cifrato D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

### Messaggio segreto

Chiario e s e m p i o d i c i f r a t u r a s e m p l i c e  
Cifrato H V H J M L R G L F L I U D W X U D V H P S O L F H



## Enigma (1918)

La macchina presenta una meccanica a tre rotori D, C, S forniti di 26 contatti elettrici su ogni faccia che in modo segreto connettono ogni contatto sulla faccia destra con un contatto sulla faccia sinistra; e all'estrema sinistra un riflettore con 26 contatti elettrici solo sulla faccia destra, accoppiati a due a due secondo uno schema segreto.





## Phil R Zimmermann (1991)

Crittografia a  
doppia chiave  
(?!?)

e Pretty  
Good  
Privacy



Chiave  
**pubblica**  
(su Server remoto)



Chiave  
**privata**  
(sul PC locale)



**internet**

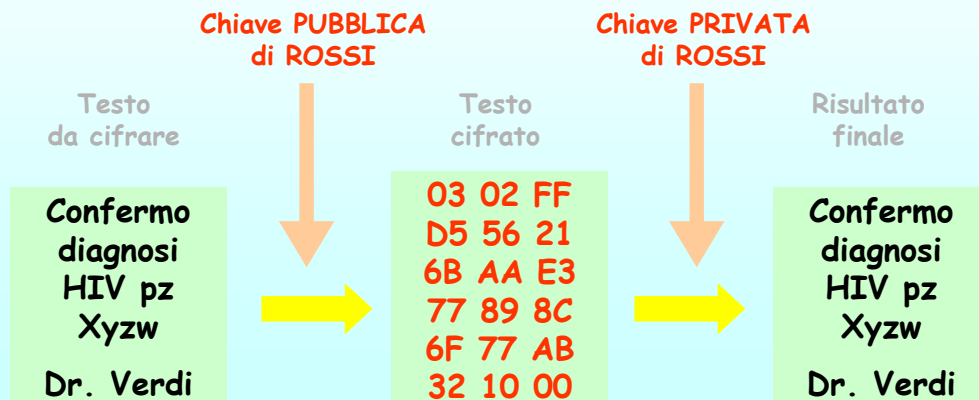


## Sicurezza delle chiavi del PGP

384 bit	bassa
512 bit	commerciale
1024 bit	militare
2048 bit	proibita in USA



## Messaggio dal dottor Verdi al dottor Rossi





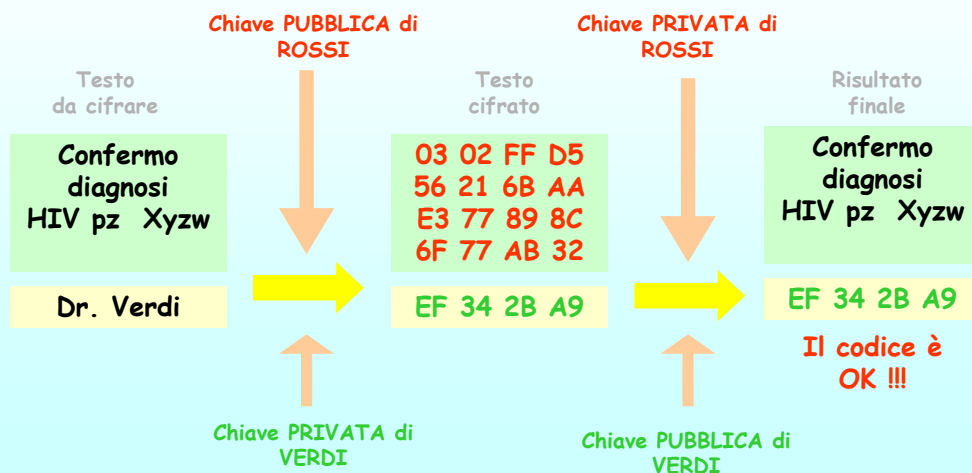
Nell'esempio riportato:

Verdi è sicuro  
che solo Rossi  
leggerà il suo messaggio.

Ma chi assicura Rossi  
che il messaggio viene  
proprio da Verdi ?!?



Messaggio  
dal dottor Verdi  
al dottor Rossi



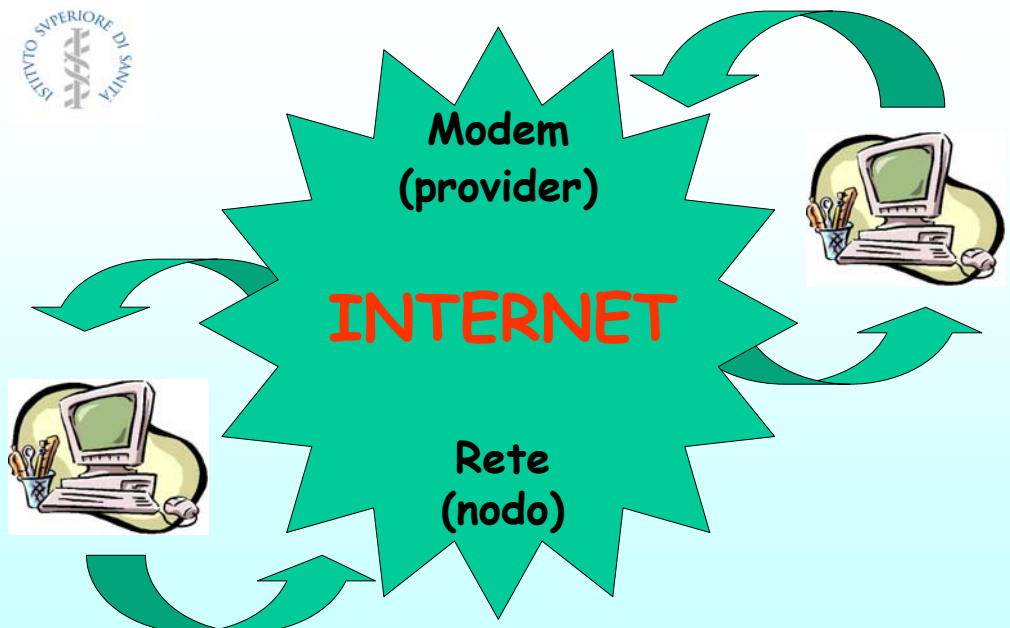


## Con la firma digitale:

Verdi è sicuro che solo Rossi leggerà il suo messaggio.

Rossi è sicuro che solo Verdi può aver scritto il messaggio.

Ma chi ci assicura che Rossi è Rossi e che Verdi è Verdi ?!?





## Archivio Sanitario Nazionale Flusso dei dati e relativa gestione



Sig. Xyz  
Cartella  
clinica  
Risultati  
Laboratorio

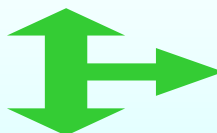
TRASMISSIONE  
cartacea  
email  
online



## Archivio Sanitario Nazionale

Sig. Xyz  
Cartella  
clinica  
Risultati  
Laboratorio

Sig. Xyz  
CODICE



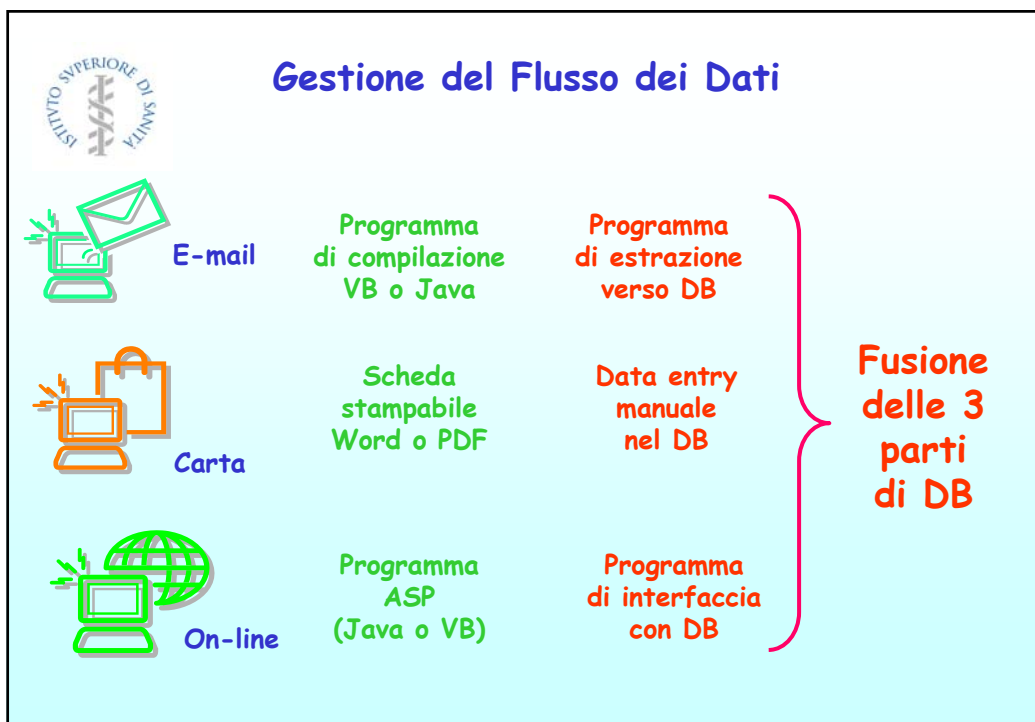
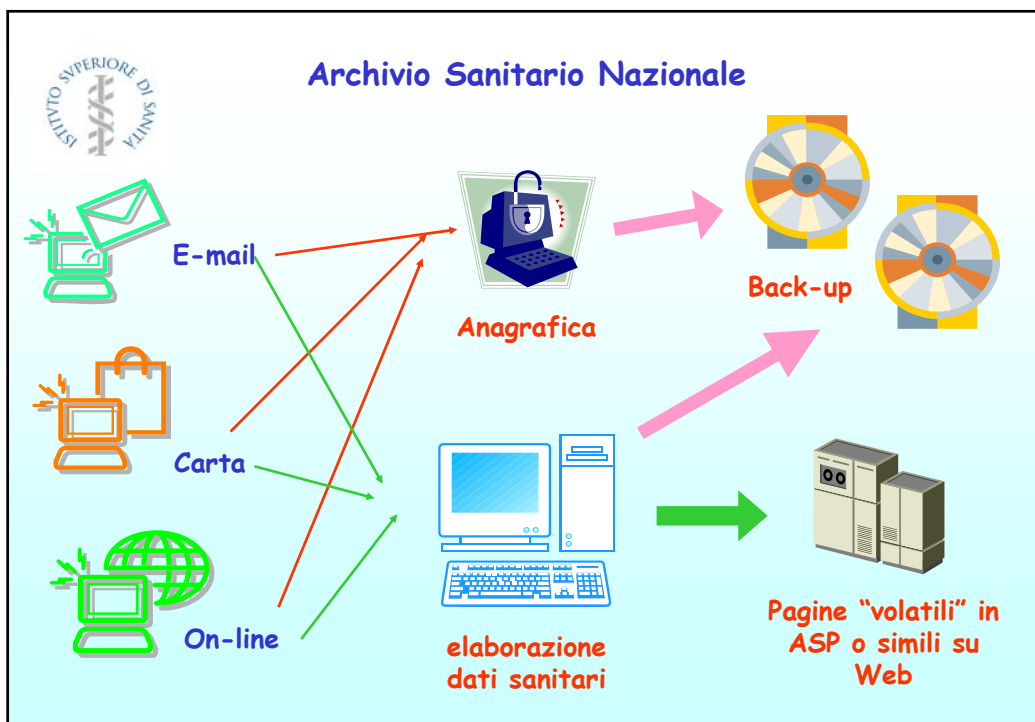
CODICE  
Cartella  
clinica  
Risultati  
Laboratorio

Firma digitale

Crittografia  
1024 bit

https 128 bit

Archivi separati  
fisicamente  
e logicamente







## Studio di coorte sulla ipercolesterolemia in età pediatrica nelle Comunità delle Serre Calabre (Vibo Valentia)

Catella Clinica Studio VV2004 v.2.0.0

### SCHEDA RACCOLTA DATI STUDIO DELLA COMUNITA' MONTANA DELLE SERRE

A001	Cognome			
A002	Nome			
A003	Luogo di Nascita (specificare la provincia)			
A004	Data di Nascita (gg/mm/aaaa)			
A005	Sesso (M/F)	non noto		
A006	Altezza (cm)			
A007	Peso (kg)			
A008	Circonferenza vita (cm)			
A009	Circonferenza fianchi (cm)			
A010	Circonferenza braccio (cm)			
A011	Pressione arteriosa (max/min in mmHg)			
A012	Pulsazioni cardiache (rpm su 60 sec)			
A013	Colesterolemia totale (mg/dL, se nota)			
B001	Data prelievo (gg/mm/aaaa)			
B002	Colesterolemia totale (mg/dL)			
B003	Colesterolemia HDL (mg/dL)			
B004	Colesterolemia LDL (mg/dL)			
B005	Triglicerolemia (mg/dL)			
B006	Glicemia (mg/dL)			
C001	Tipo di parto	<input checked="" type="checkbox"/> eutocico	<input type="checkbox"/> distocico	<input type="checkbox"/> non noto
C002	Allattamento	<input checked="" type="checkbox"/> seno materno	<input type="checkbox"/> artificiale	<input type="checkbox"/> misto
C003	Svezamento	<input checked="" type="checkbox"/> < 4 mesi	<input type="checkbox"/> 4 - 6 mesi	<input type="checkbox"/> > 6 mesi

Pag. 1 di 4



## Rischi nella Gestione Elettronica dell'Informazione

## Sindrome di Star Trek





## **?!?** Conclusioni **?!?**

**Sicurezza all'interno**  
(privacy dei contenuti)

**Sicurezza dall'esterno**  
(cracker & hacker)

**Aggiornamento continuo**  
(hardware & software)



**Potrete trovare  
una copia  
di queste diapositive  
all'indirizzo internet:**

**<http://www.tarcisio.net/20050617/niglio.pdf>**

**per contatti con  
Dott. Tarcisio Niglio  
Tel.: 06.4990.3141  
Fax.: 06.6227.6150  
Email: [etrusco@iss.it](mailto:etrusco@iss.it)**