

## **Elementi fondamentali di riservatezza e sicurezza dei dati clinici**

- **Terminologia di base**
  - Autenticazione
    - Autenticazione semplice
    - Mutua Autenticazione
  - Identificazione
  - Autorizzazione
  - Riservatezza (o segretezza)
  - Integrità
  - NON-ripudio
  - Crittografia
  - Message digest
  - Firma elettronica
  
- **La sicurezza dei dati: le possibili minacce e le tecniche per contrastarle**
  - Una Classificazione dei problemi e delle tecniche
  - La Sicurezza fisica
    - Controllo dell'accesso fisico
    - Protezione da sabotaggio
    - Protezione da intercettazione
    - Protezione da calamità e/o disastri
  - La Sicurezza logica
    - il controllo logico dell'accesso
    - l'accuratezza dell'elaborazione
  - La Sicurezza organizzativa
    - i problemi da affrontare
    - le tecniche per risolverli
  - La gestione del rischio
    - Selezione di misure di protezione per grandi sistemi e postazioni individuali

Elementi fondamentali di riservatezza e sicurezza dei dati clinici

- **La legislazione italiana vigente in materia di dati personali**
    - Il Codice della privacy: scheda informativa
      - Testo consolidato con la legge 26 febbraio 2004, n. 45, di conversione con modificazioni del d.l. 24 dicembre 2003, n. 354
      - Decreto legislativo 30 giugno 2003, n. 196 - Vigenza 31 luglio 2004 - Consolidato con la legge 27 luglio 2004, n. 188 di conversione con modifiche decreto legge 24 giugno 2004, n. 158
    - Il Codice della privacy: ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)
  
  - **Crittografia**
    - Definizione
    - Un esempio storico: Il Cifrario di Cesare
    - Algoritmi di crittografia a chiave privata (simmetrici)
      - L'algoritmo Data Encryption Standard (DES)
      - *L'algoritmo International Data Encryption Algorithm (IDEA)*
      - *L'algoritmo Advanced Encryption Standard (AES)*
  
    - Algoritmi a chiave pubblica (asimmetrici)
      - L'algoritmo RSA
      - *L'algoritmo DSA*
  
  - **Message Digest**
    - Definizione
    - Algoritmi di Message Digest
- Link interessanti a riguardo degli algoritmi di crittografia: RSA Security RSALABS  
<http://www.rsasecurity.com/rsalabs/>  
<http://www.rsasecurity.com/rsalabs/node.asp?id=2253>
- **Firma Elettronica**
    - Definizioni
    - Condizioni per l'uso
    - Scambio delle chiavi fuori linea (Out-Of-Band, OOB)
    - Certificati a chiave pubblica e Certification Authority (CA)  
CNIPA: Centro Nazionale per l'Informatica nella Pubblica Amministrazione  
([http://www.cnipa.gov.it/site/it-IT/In\\_primo\\_piano/Elenco\\_certificatori/Normativa/](http://www.cnipa.gov.it/site/it-IT/In_primo_piano/Elenco_certificatori/Normativa/))

Elementi fondamentali di riservatezza e sicurezza dei dati clinici

- **Sicurezza della posta elettronica**
  - Autenticazione del mittente
  - Integrità del messaggio
  - Non ripudio da parte del mittente
  - Riservatezza del messaggio
  
- *PEM (Privacy Enhanced Mail)*
- *PGP (Pretty Good Privacy)*
- *MOSS (Multimedia Object Security Services)*
- *S/MIME (Secure MIME)*
- *X.400, X.500, X.509 (Standard ISO-OSI per la realizzazione del servizio di posta elettronica testuale X.400, e multimediale X.421)*
  
- **Firewall**
  - Definizioni
  - Collegamento a rete sicura FIREWALL
  
- **File di LOG**
  - Definizioni
  - Come funzionano
  - Link
  - Common Log Format <http://www.bacslabs.com/WsvlCLF.html>
  - Extended Log File Format <http://www.w3.org/TR/WD-logfile.html>
  
- **Biometria**
  - Definizioni
  - Strumenti
  - SIK Something I Know
  - SIH Something I Have
  - SIA Something I Am
  - Un link interessante: <http://biometrics.cse.msu.edu>
  - Tutorial sulla Biometria: <http://biometrics.cse.msu.edu/icprareareviewtalk.pdf>