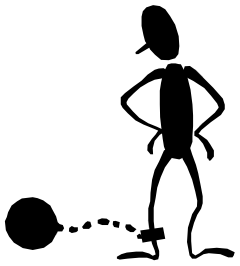
Università degli Studi di Padova
Scuola di Specializzazione in Biochimica Clinica (A.A. 2005-2006 2006-2007)
INDIRIZZI: DIAGNOSTICO E ANALITICO TECNOLOGICO

Biochimica Clinica e Biologia Molecolare Clinica:
automazione ed informatica in Biochimica Clinica
area D SSD BIO/12 ex E05C ore 20 anno IV
-OBIETTIVO FORMATIVO: Acquisire le conoscenze informatiche per la gestione del laboratorio

Comunicazioni elettroniche sicurezza dei dati e dei sistemi

Marco Pradella
Castelfranco Veneto

Sanzioni 196/03



- **Violazioni amministrative**
  - **161. 3-18000 €, 5-30000 € (aum. fino 3 volte)**
  - **162. 5-30000 € 500-3000 €**
  - **163 10-60000 € + diffusione media**
  - **164. 4-24000 €**
  - **165. 161 162 164 event. diffusione media**

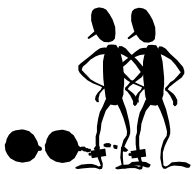
- **Illeciti penali**
  - **167. 6-18m / 6-24m / 1-3a**
  - **168. 6m-3a**
  - **169. 0-2a / 10-50000 €**
  - **170. 3m-2a**
  - **171. Legge 300/70 art. 38**
  - **172. + diffusione media**

Illeciti penali 196/03 Art. 167
Trattamento illecito di dati

- 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la **reclusione da sei a diciotto mesi** o, se il fatto consiste nella comunicazione o diffusione, con la **reclusione da sei a ventiquattro mesi**.
- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la **reclusione da uno a tre anni**.

Illeciti penali 196/03 articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129

- 18, trattamento solo fini istituzionali
- 19, comunicazione solo fini istituzionali
- 23, consenso espresso dell'interessato.
- 123, traffico elettronico
- 126, dati relativi all'ubicazione
- 130, comunicazioni indesiderate
- 129, elenchi



==> reclusione da sei a ventiquattro mesi

Illeciti penali 196/03 articoli 17, 20, 21, 22

- 17, rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato,
- 20, dati sensibili
- 21, dati giudiziari
- 22, dati sensibili e giudiziari
  - 8, diffusione
  - 11, test psico-attitudinali e diffusione
- 25, comunicazione e diffusione
- 26, consenso per dati sensibili
- 27, dati giudiziari
- 45, trasferimento altro Stato

==> reclusione da dodici a trentasei mesi

196/03 Art. 4 Definizioni

dati personali

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 e sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e. "**dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

Illeciti penali 196/03 Art.168 -Falsità nelle dichiarazioni e notificazioni al Garante

- Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la **reclusione da sei mesi a tre anni**

Illeciti penali **196/03** Art. 169 Misure di sicurezza

- 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 **diecimila euro a cinquantamila euro**
- **Art. 33 Misure minime**
  - 1. Nel quadro dei piu' 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.

196/03 Art. 34 Trattamenti con strumenti elettronici

- 1. Il trattamento di dati personali effettuato con strumenti elettronici è 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**;
  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 disponibilità 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 sanitari.

196/03
Art. 35 Trattamenti senza l'ausilio di strumenti elettronici

- Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
  a. **aggiornamento** periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
  b. previsione di procedure per un'idonea **custodia** di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
  c. previsione di procedure per la conservazione di determinati atti in archivi ad **accesso selezionato** e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

196/03 Art. 4 Definizioni

autenticazione informatica

c. "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d. "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e. "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f. "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g. "**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Illeciti penali 196/03
170 - 171 - 172

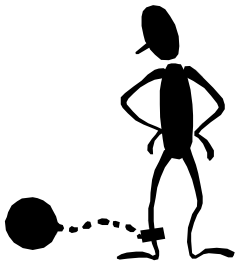
- Art. 170 Inosservanza di provvedimenti del Garante
  1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la **reclusione da tre mesi a due anni**.
- Art. 171 v. legge 20 maggio 1970, n. 300
  libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro
- *Art. 172 Pene accessorie*
  *1. La condanna per uno dei **delitti** previsti dal presente codice importa la pubblicazione della sentenza.*

reato e delitto

- Definizione formale di reato
  - Ogni fatto umano cui la legge ricollega una sanzione penale
- art. 39 del codice penale:
  - Sono **delitti** i reati al cui verificarsi l'ordinamento penale ricollega la pena dell'ergastolo, della reclusione e della multa.
  - Sono **contravvenzioni** i reati al cui verificarsi l'ordinamento penale ricollega la pena dell'arresto e dell'ammenda.

http://it.wikipedia.org/wiki/Reato

Sanzioni 196/03



- **Violazioni amministrative**
  - **161. 3-18000 €, 5-30000 € (aum. fino 3 volte)**
  - **162. 5-30000 € 500-3000 €**
  - **163 10-60000 € + diffusione media**
  - **164. 4-24000 €**
  - **165. 161 162 164 event. diffusione media**

- **Illeciti penali**
  - **167. 6-18m / 6-24m / 1-3a**
  - **168. 6m-3a**
  - **169. 0-2a / 10-50000 €**
  - **170. 3m-2a**
  - **171. Legge 300/70 art. 38**
  - **172. + diffusione media**

Violazioni amministrative **196/03**

Art. 161 Omessa o inidonea informativa all'interessato

- 1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da **tremila euro a diciottomila euro** o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da **cinquemila euro a trentamila euro**. La somma può essere aumentata sino al **triplo** quando risulta inefficace in ragione delle condizioni economiche del contravventore.

196/03 Art. 13 Informativa

- 1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
  a. le finalità e le modalità del trattamento cui sono destinati i dati;
  b. la natura obbligatoria o facoltativa del conferimento dei dati;
  c. le conseguenze di un eventuale rifiuto di rispondere;
  d. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
  e. i diritti di cui all'articolo 7;
  f. gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

196/03 Art. 7 Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a. dell'origine dei dati personali;
   b. delle finalità e modalità del trattamento;
   c. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d. degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a. l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a. per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b. al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

nformativa

Informativa: indicazioni per medici di base e pediatri - 19 luglio 2006
(G.U. n. 183 del 8 agosto 2006)
IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

INFORMAZIONE

Gentili signori,

desidero informarvi che i vostri dati sono utilizzati solo per svolgere attività necessarie per prevenzione, diagnosi, cura, riabilitazione o per altre prestazioni da voi richieste, farmaceutiche e specialistiche.

Si tratta dei dati forniti da voi stessi o che sono acquisiti altrove, ma con il vostro consenso, ad esempio in caso di ricovero o di risultati di esami clinici.

Anche in caso di uso di computer, adotto misure di protezione per garantire la conservazione e l'uso corretto dei dati anche da parte dei miei collaboratori, nel rispetto del segreto professionale. Sono tenuti a queste cautele anche i professionisti (il sostituto, il farmacista, lo specialista) e le strutture che possono conoscerli.

I dati non sono comunicati a terzi, tranne quando sia necessario o previsto dalla legge.

Si possono fornire informazioni sullo stato di salute a familiari e conoscenti solo su vostra indicazione.

In qualunque momento potrete conoscere i dati che vi riguardano, sapere come sono stati acquisiti, verificare se sono esatti, completi, aggiornati e ben custoditi, e far valere i vostri diritti al riguardo.

Per attività più delicate da svolgere nel vostro interesse, sarà mia cura informarvi in modo più preciso.

http://www.garanteprivacy.it/garante/doc.jsp?ID=1318699

196/03 Art. 4 Definizioni

- a. "**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- 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;

196/03 Art. 4 Definizioni

dati personali

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, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e. "**dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

196/03 Art. 4 Definizioni

persone

f. "**titolare**", la persona fisica, la persona 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 di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g. "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h. "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i. "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

196/03 Art. 4 Definizioni

dati

l. "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m. "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n. "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o. "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p. "**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

ISO TS 25237 - Pseudonimizzazione

- ISO TC 215 / WG4 - Security - NWIP **2005-05-11**
- **VOTE ON PROPOSED ISO/DTS** 25237
  - Closing date for voting 2007-03-20
- Pseudonymisation is recognized as an important method for privacy protection of personal health information. Such services may be used nationally as well as for trans-border communication.
  - A pseudonym is not about using a false name (as in the colloquial use of the word), but about deidentifying personal data. Pseudonymisation provides a means by which information may be linked to the same person across multiple data records or information system without revealing the identity of the person as a data subject. The primary risk mitigated by this technology is privacy as associated with de-identification, which may further influence legal, organizational, and financial risk factors.

geografia della normazione

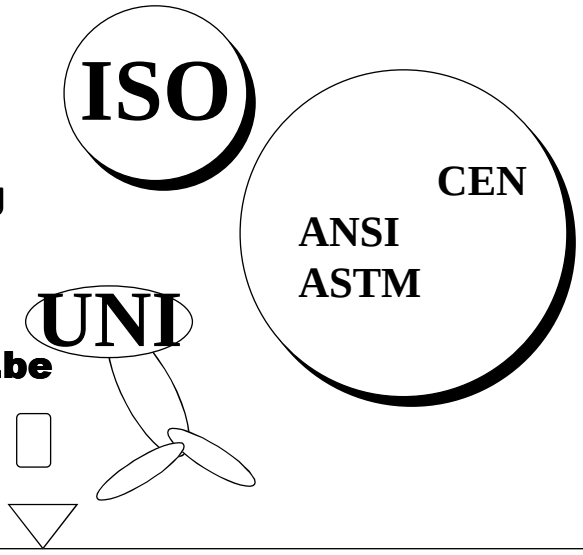
www.ANSI.org

www.ASTM.org

www.ISO.org

www.CENORM.be

www.UNI.com



ISO/TC 215
International Organization for Standardization's (ISO) Technical Committee (TC) on Health informatics.

several Working Groups (WG), each dealing with an aspect of Electronic Health Records (EHR).

* WG 1: Health Records and Modelling Coordination
* WG 2: Messaging and communications
* WG 3: Health Concept Representation
* WG 4: Security
* WG 5: Health Cards
* WG 6: Pharmacy and Medication

http://en.wikipedia.org/wiki/ISO_TC_215
last modified 01:28, 2 February 2007.

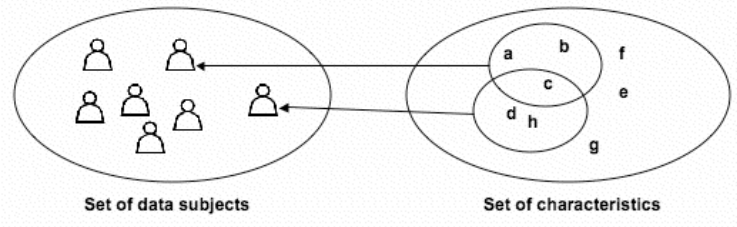
ISO TS 25237 - Pseudonimizzazione

80 pagine

ISO TS 25237 -
Annex A (informative) Healthcare pseudonymisation scenarios

- A.1 Introduction.
- A.2 Scenario explanation
- A.3 Healthcare scenarios
- Patient identification systems

ISO TS 25237 - Pseudonimizzazione
5.1.3.2 The idealized concept of identification

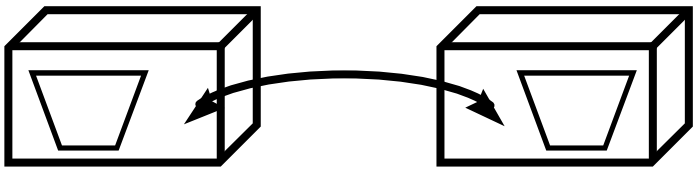


ISO TS 25237 5.1.3.3 The concept of anonymisation

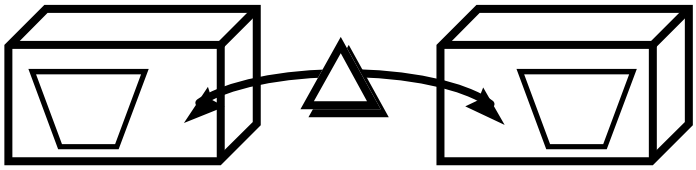
Anonymisation is the process that removes the association between the identifying data set and the data subject. This can be done in two different ways:

- by removing or transforming characteristics in the associated characteristics-data-set so that the association is not unique anymore and relates to more than one data subject
- by increasing the population in the data subjects set so that the association between the data set and the data subject is not unique anymore

ISO TS 25237 5.1.3.3 The concept of anonymisation



ISO TS 25237 5.1.3.3
Pseudonymisation



ISO TS 25237 5.1.3.3
Pseudonymisation

- Pseudonymisation is a particular type of anonymisation that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.
  - In **irreversible** pseudonymisation, the conceptual model does not contain a method to derive the association between the data-subject and the set of characteristics from the pseudonym.
  - In **reversible** pseudonymisation, the conceptual model includes a way of re-associating the data-set with the data subject.

ISO TS 25237 5.3 Re-Identification 5.3.1 Need for Re-identification of Pseudonymised Data

Pseudonymisation separates out personally identifying data from substantive data by assigning a coded value to the sensitive data before splitting the data out. This approach maintains a connection between substantive data (the payload data) and personal identifiers, but can allow for the reidentification under prescribed circumstances and protections. This approach serves researchers well in that it provides a means to cleanse research data while retaining the ability to reference source identifiers for the many (controlled) circumstances under which such information may be needed.

Such circumstances include the following coded values:

25237.1 verifiy/validate data integrity

25237.2 check for suspected duplicate records

25237.3 enable requests for additional data

25237.4 link to supplement research information variables

25237.5 compliance audit

25237.6 inform data subject or their care provider of significant findings

25237.7 facilitate follow-up research

ISO TS 25237 - A.3 Healthcare scenarios

1) Clinical pathology order (pseudonymous care)

Workflow/events/actions

- Submit order to HIS

- **The placer of the order authenticates towards the HIS**
- **The placer of the order submits the order with the hospital unique ID number of the data subject to the HIS**
- **HIS checks order against policies (e.g. recipient not allow to receive identifiable data, VIP,…) and decides on privacy protection measures.**

- pseudonymise

- **The hospital information system invokes the pseudonymisation service with as input the hospital unique ID number**
- **The PS processes the hosp ids**
- **The PS returns the pseudo-ID to the HIS**

- The HIS sends the order with the pseudo-id to the filler

- **Establish comm**
- **message sent,**
- **ack received**

- the order is processed by the filler of the order using the pseudo-id

- **(possible comparative analysis performed by specialist)**

The filler of the order submits the result to the HIS with the pseudo-id

- **Establish**
- **Message sent**
- **Ack received**

Re-identify results

- **The HIS submits the pseudo-id to the pseudonymisation services**
- **Authenticated user (HIS) is verified against reverse ID policy**
- **The PS processes the pseudo-id**
- **The PS sends the real ID to the HIS**

The HIS inserts the result with the hosp ID into the HCR

ISO TS 25237 - 8 Specification of interoperability of interfaces (methods and implementation)

... for instance, make use of an intermediary TTP to perform the de-identification and pseudonymisation, or may be an in-house module added to extraction software.

...

The common service of most pseudonymisation services consists of cryptographic transformations of indentifiable data.

TTP = Trusted Third Party = terzi di fiducia

ISO TS 25237 - 9 Policy framework for operation of pseudonymisation services (methods and implementation)

It is important to complement the technical measures with appropriate non-technical measures. Such non-technical measures are generally express through policies, agreements, and codes of conduct.

In order to satisfy these requirements, a trusted third party service:

• should be strictly independent of the organizations supplying source data

• must be able to guarantee security and trustworthiness of its methods by publishing to its subscribers its operating practices

...

• must be able to guarantee security and trustworthiness of its operating environment, platforms and infrastructure

o shall restrict network traffic to restrict all unnecessary traffic

o shall disable all unnecessary operating system services

o shall provide technical, physical, procedural, and personnel controls in accordance with ISO27799

...

196/03 Art. 4 Definizioni

elettronica

a. "**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
b. "**chiamata**", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
c. "**reti di comunicazione elettronica**", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
d. "**rete pubblica di comunicazioni**", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
e. "**servizio di comunicazione elettronica**", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

196/03 **Violazioni amministrative**

Art. 162 Altre fattispecie

Art. 163 Omessa o incompleta notificazione

1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da **cinque mila euro a trentamila euro**.
2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da **cinquecento euro a tremila euro**.

1. Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da **diecimila euro a sessantamila euro** e con la sanzione amministrativa accessoria della **pubblicazione** dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

196/03 Violazioni amministrative

Art. 164 Omessa informazione o esibizione al Garante
Art. 165 Pubblicazione del provvedimento del Garante

1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 15o, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da **quattromila euro a ventiquattro mila euro**.

1. Nei casi di cui agli articoli 161, 162 e 164 può essere applicata la sanzione amministrativa accessoria della **pubblicazione** dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.