GDPR

La legge sulla privacy: “EU Regulation n. 2016/679” o “General Data Protection Regulation”, in Italia “DL 101/2018”.

La gestione dei dati sanitari è un’attività **pericolosa** dal momento che può causare un **danno**, sia in ambito discriminatorio che economico.

I dati elettronici aumentano il **rischio** che il danno si verifichi (aumenta la probabilità). I regolamenti danno strumenti normativi che consentono di ridurre i rischi. La tecnologia deve mettere in atto opportune strategie per la riduzione del rischio.

Sono **dati personali** le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc… sono dati sia che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. – che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa).

Ci sono dei dati c.d. "particolari/**sensibili**", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.

Trattamento dei dati personali: trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali. *Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).* I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Le parti in gioco attorno al DATO sono: l’interessato, il responsabile e il titolare:

- **Interessato** è la persona fisica alla quale si riferiscono i dati personali.
- **Titolare** è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento.
- **Responsabile** è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati.
- **Terse parti** sono gli altri attori indirizzati ai dati

Il **Data Protection Officer** è una figura interna o esterna all’organizzazione nominata dal titolare del trattamento e in possesso di un’adeguata conoscenza della normativa sul data protection. Guida il titolare e il responsabile del trattamento nell’adozione degli obblighi derivanti dal GDPR.

Alcuni principi:

- Minimizzazione dei dati: un titolare del trattamento deve trattare solo i dati di cui ha realmente bisogno per il perseguimento delle finalità del trattamento
- Adeguatezza dei dati
- Pertinenza alle finalità: Limitazione del trattamento al solo raggiungimento delle finalità
- Accuratezza e aggiornamento
- Limitazione alla memorizzazione: i dati non possono essere memorizzati all’infinito

- Territorialità: se i dati appartengono ad un soggetto della comunità europea sono soggetti al regolamento (es. cookie law)
- Integrità e confidenzialità.
- Sicurezza (tecnica e organizzativa

Gli interessati hanno sia diritti conoscitivi (all'informativa e all'accesso) e di controllo (dei propri dati).

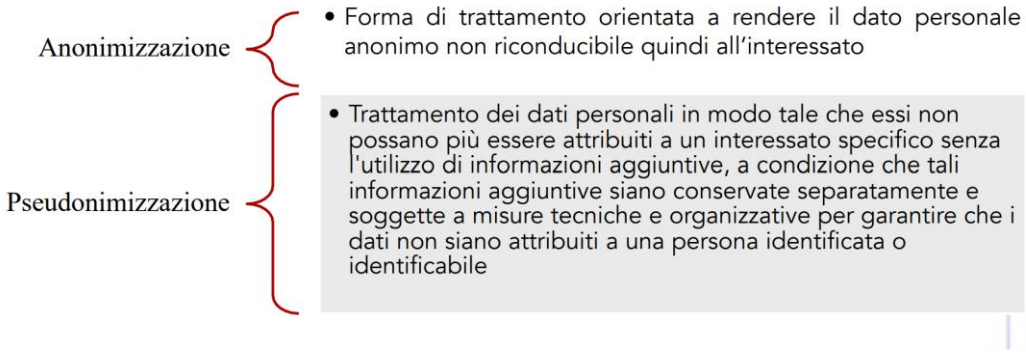
Il diritto all'oblio è il diritto dell'interessato ad ottenere la cancellazione dei dati personali dal titolare.

Articolo 9 GDPR: Trattamento di categorie particolari di dati personali: è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

- **consenso esplicito** per una o più finalità specifiche
- il trattamento riguarda dati personali resi pubblici dall'interessato
- interessino la salute pubblica
- trattamento necessario a fini di ricerca scientifica, i dati vengono deidentificati, anonimizzati.

Consenso informato: un valido consenso deve essere esplicitamente dato per la raccolta dei dati e per i propositi per i quali sono usati. Per i dati sensibili, invece, il consenso deve essere esplicito il che indica una modalità espressiva manifesta (dichiarazione scritta, procedura informatica con doppio passaggio di verifica, firma digitale, invio di firma autografa scansionata, compilazione modulo digitale …). È sempre accompagnato dall'**informativa** sul trattamento dei dati personali, con il consenso viene accettata.



D. Lgs. 196/2003: misure minime predefinite.

GDPR: obbligo di adottare misure tecniche ed organizzative adeguate alla valutazione dei rischi.

Il titolare ed il responsabile devono quindi adottare adeguate misure tecniche ed organizzative, per assicurare un livello di sicurezza adeguato ai rischi, sottoscrivendo un **documento di valutazione dell'impatto**, tenuto conto:

- dello stato dell'arte e costi di realizzazione
- della natura, contesto, oggetto e finalità del trattamento
- dei rischi per i diritti e la libertà degli individui e relativa probabilità e gravità

Le minacce possono essere sia legate all'inconsapevolezza del personale fino ai reati più gravi.

Trattamento con strumenti elettronici: sono consentiti ad incaricati dotati di **credenziali d'autenticazione** consistenti in un codice identificativo associato ad una password. Password di 8 caratteri, non facilmente intuibile, da sostituire al primo utilizzo e poi ogni 3 mesi (dati sensibili), non più riutilizzabile e da distruggere

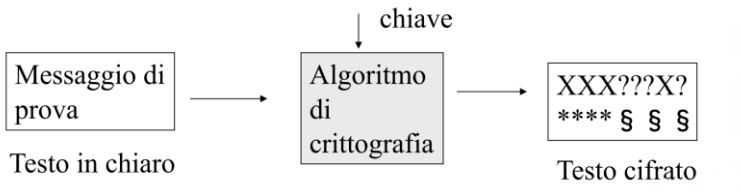
dopo 6 mesi di inutilizzazione. Profili d'autorizzazione (privilegi d'accesso) diversificati per ciascuno degli incaricati onde limitare l'accesso ai soli dati strettamente necessari. Adozione di idonei sistemi atti ad evitare l'accesso ai dati o l'introduzione di virus, trojani o worm che li possano danneggiare, tramite l'adozione di apposite apparecchiature hardware (firewall) o l'installazione di software (firewall, **antivirus**, ecc.) da aggiornare almeno ogni 6 mesi. Aggiornamento dei programmi applicativi e dei sistemi operativi, almeno ogni 6 mesi (dati sensibili). **Salvataggio dei dati** (copia di sicurezza) con cadenza almeno settimanale (dati sensibili) e verifica dell'effettivo ripristino. Adozione di idonee misure di sicurezza atte a prevenire il danneggiamento degli strumenti elettronici (gruppi di continuità, firewall, antivirus, ecc.). Trasferimento dei dati in formato elettronico solo in forma cifrata (**crittografata**).

Il titolare del trattamento è tenuto a custodire e controllare i dati personali oggetto del trattamento, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

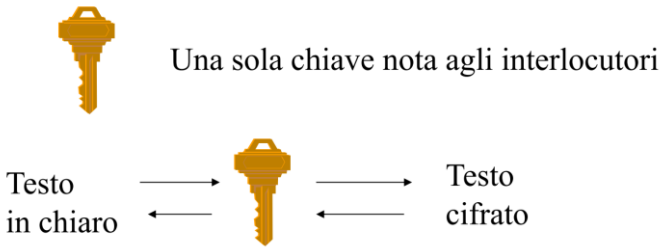
Requisiti di un sistema sicuro di scambio di documenti elettronici:

- Consenso: il mittente deve esprimere consenso sul contenuto
- Paternità: la paternità di un documento digitale deve essere garantita
- Integrità: il messaggio non deve essere contraffatto dagli altri utenti del canale, incluso il destinatario
- Autenticità: il destinatario deve poter verificare l'identità del mittente
- Segretezza: gli interlocutori siano in grado di scambiare documenti senza che nessuno all'infuori di loro due sia in grado di leggerli
- Non negazione: chi è legalmente autorizzato deve poter comunicare

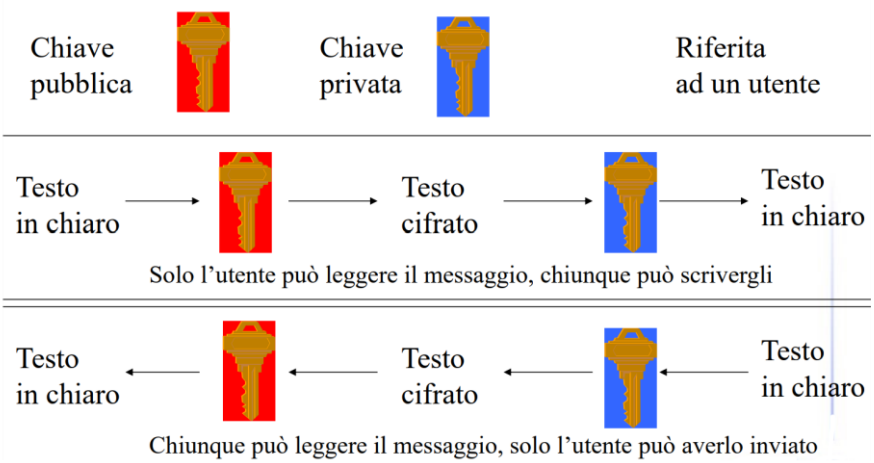
Segretezza: il metodo trae la sua origine nella crittografia, la disciplina che studia l'utilizzo e la creazione dei crittosistemi.



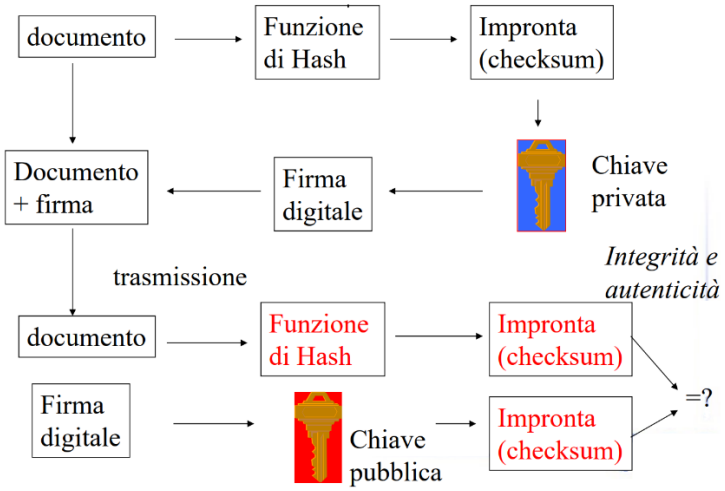
- Algoritmi a **chiave privata** (simmetrica, singola). La chiave viene scambiata in modo riservato. È necessaria una chiave diversa per ogni coppia di interlocutori Algoritmi "veloci" (e.g. IDEA).



- Algoritmi a **chiave pubblica** (asimmetrica, doppia). Bisogna mantenere le chiavi pubbliche, Algoritmi "lenti" (e.g. RSA, il più frequente).



[spesso la chiede]**Firma digitale:** Rif. Leg. Legge Bassanini (art. 15 n°59 15/03/97) e sue norme attuative (firma elettronica): deve rispettare i requisiti di consenso, paternità, integrità e autenticità.



Protocollo HTTPS (versione sicura del protocollo HTTP): assicura che il messaggio inviato sia crittografato. È con Secure Socket Layer (SSL). Utilizzato per transazioni commerciali via Web, utilizza i certificati ed entrambi i tipi di crittografia: si basa sull'identificazione del server (colui che fornisce un servizio su Internet).