FRONTESPIZIO DELIBERAZIONE

AOO: ASL_BO

REGISTRO: Deliberazione

NUMERO: 0000153

DATA: 26/03/2026 15:16

OGGETTO: Approvazione del Regolamento per l'utilizzo dei dati personali a fini didattici e di pubblicazione scientifica

SOTTOSCRITTO DIGITALMENTE DA:

Il presente provvedimento è stato firmato digitalmente da Petrini Anna Maria in qualità di Direttore Generale
Con il parere favorevole di Meschi Michele - Direttore Sanitario
Con il parere favorevole di Carlini Stefano - Direttore Amministrativo

Su proposta di Silvia Taglioli - UO Affari Generali e Legali (SC) che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [03-05]

DESTINATARI:

- Collegio sindacale
- Distretto Pianura Est
- Distretto dell'Appennino Bolognese
- UO Comunicazione (SS)
- UO Servizio Prevenzione e Protezione (SC)
- UO Medicina Legale e Risk Management (SC)
- UO Committenza e Governo dei Rapporti con il Privato Accreditato (SC)
- UO Governo Clinico, Ricerca, Formazione e Sistema Qualita' (SC)
- Uo Governo Dei Percorsi Di Screening E Specialistici(sc)
- Distretto Savena Idice
- Distretto Pianura Ovest
- Distretto Citta' di Bologna
- Distretto Reno, Lavino e Samoggia
- Dipartimento Oncologico
- Dipartimento Chirurgie Specialistiche
- Dipartimento Assistenziale, Tecnico e Riabilitativo - DATeR
- Dipartimento Farmaceutico Interaziendale - DFI

- Dipartimento Cure Primarie
- Dipartimento Emergenza Interaziendale - DEI
- Dipartimento Materno Infantile
- Dipartimento Chirurgie Generali
- Dipartimento Interaziendale per la Gestione Integrata del Rischio Infettivo - DIGIRI (IRCCS AOU)
- Dipartimento della Riabilitazione
- Dipartimento della Rete Ospedaliera
- Dipartimento Medico
- Dipartimento Tecnico-Patrimoniale
- Dipartimento della Rete Medico Specialistica Ospedaliera e Territoriale
- Dipartimento dell'Integrazione
- Dipartimento della Diagnostica e dei Servizi di Supporto
- Dipartimento Sanita' Pubblica
- Dipartimento Attivita' Amministrative Territoriali e Ospedaliere - DAATO
- Dipartimento Salute Mentale - Dipendenze Patologiche
- Dipartimento Interaziendale ad Attivita' Integrata di Anatomia Patologica - DIAP
- UO Anticorruzione e Trasparenza (SC)
- UO Libera Professione (SC)
- UO Sistemi Informativi Aziendali (SC)
- UO Programmazione e Controllo (SC)
- IRCCS Istituto delle Scienze Neurologiche - Direzione Scientifica
- UO Sviluppo Organizzativo e Gestione Operativa (SC)
- Servizio Unico Metropolitano Economato (SUME)
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)
- Servizio Unico Metropolitano Amministrazione Giuridica del Personale - SUMAGP (SC)
- Servizio Unico Metropolitano Amministrazione Economica del Personale - SUMAEP (SC)
- Servizio Acquisti di Area Vasta - SAAV (SC)

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000153_2026_delibera_firmata.pdf	Carlini Stefano; Meschi Michele; Petrini Anna Maria; Taglioli Silvia	CAE80F8E42A0EBDB45A13FAE2E0B15C14EB645223251CCCF6C399CF77EDAFC49
DELI0000153_2026_Allegato1.pdf:		C619E6BD437782B7DD0B0B3C9B7DC4A884E618BCC616CA7BD072231A69AF3F97

DELIBERAZIONE

OGGETTO: Approvazione del Regolamento per l'utilizzo dei dati personali a fini didattici e di pubblicazione scientifica

IL DIRETTORE GENERALE

Su proposta del Direttore f.f. della Unità Operativa Affari Generali e Legali, che esprime contestuale parere favorevole in ordine ai contenuti formali sostanziali e di legittimità del presente atto;

Visti

- il 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" ;*
- il D.lgs. 30 giugno 2003, n. 196 recante il " *Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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";*

Richiamato il Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 14 gennaio 2021 - Regione Veneto "Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica" mediante il quale l'Autorità Garante ha fornito specifiche indicazioni sul corretto trattamento di dati per finalità didattiche e di pubblicazione scientifica, con particolare riferimento alle misure di sicurezza tecniche ed organizzative che dovranno essere garantite;

Richiamata la deliberazione n.11 del 14/1/2019 " *Adeguamenti al Regolamento (UE) 2016/679.Definizione dell'organigramma delle responsabilità privacy aziendali e modalità di individuazione dei referenti privacy aziendali e dei soggetti autorizzati al trattamento dei dati personali"* così come modificata ed aggiornata dalla deliberazione n.464 del 2/12/2021;

Rilevato come in ambito sanitario il trattamento dei dati personali ed in particolare dei dati di salute, acquisiti originariamente per l'erogazione di prestazioni di prevenzione, diagnosi e cura, possa risultare, al contempo, di fondamentale importanza anche per lo sviluppo e l'accrescimento delle conoscenze e competenze scientifiche, oltre che per il costante miglioramento della qualità dei servizi offerti;

Considerato pertanto che i suddetti dati personali, inizialmente trattati per finalità di cura, potranno essere successivamente trattati da parte dei professionisti sanitari che operano in Azienda USL per la produzione

di elaborati/materiali destinati ad attività formative, didattiche, di aggiornamento professionale o di divulgazione scientifica, anche mediante tecniche di anonimizzazione e/o pseudonimizzazione, nel rispetto delle misure previste dal vigente quadro normativo sulla protezione dei dati personali;

Precisato che l'utilizzo dei dati personali per fini didattici e di pubblicazione scientifica da parte degli esercenti le professioni sanitarie che operano all'interno delle strutture del titolare del trattamento, alla luce del sopra richiamato Provvedimento dell'Autorità Garante, può avvenire solo previa adozione di specifiche misure di sicurezza di natura tecnica ed organizzativa;

Dato atto che al fine di disciplinare le operazioni di trattamento dei dati personali, ivi inclusi i dati appartenenti a categorie particolari ai sensi dell'articolo 9 del Regolamento 2016/679, svolte nell'ambito dell'Azienda USL di Bologna per finalità didattiche, formative e di pubblicazione scientifica, in coerenza alle indicazioni dell'Autorità Garante per la Protezione dei Dati Personali, è stato predisposto il regolamento allegato quale parte integrante e sostanziale alla presente deliberazione;

Precisato in particolare che rientrano nel campo di applicazione del Regolamento i trattamenti relativi a dati personali contenuti nella documentazione sanitaria e negli archivi clinico-assistenziali dell'Azienda USL, originariamente raccolti e trattati per finalità di diagnosi, cura e prevenzione, che siano successivamente elaborati, anche mediante tecniche di anonimizzazione e/o pseudonimizzazione, per la produzione di elaborati/materiali destinati ad attività formative, didattiche, di aggiornamento professionale o di divulgazione scientifica da parte dei professionisti sanitari;

Acquisito il parere favorevole del DPO Interaziendale;

Ritenuto pertanto di approvare il Regolamento per l'utilizzo di dati personali a fini didattici e di pubblicazione scientifica da parte degli operatori dell'Azienda USL di Bologna, allegato quale parte integrante e sostanziale al presente provvedimento;

Delibera

1) di approvare il Regolamento per l'utilizzo di dati personali a fini didattici e di pubblicazione scientifica da parte degli operatori dell'Azienda USL di Bologna, allegato quale parte integrante e sostanziale al presente provvedimento;

2) di dare atto che le modalità di trattamento dei dati personali per fini didattici e di pubblicazione scientifica, come disciplinate dal suddetto regolamento risultano coerenti rispetto alle indicazioni dell' Autorità Garante per la Protezione dei Dati Personali;

3) di dare altresì atto che il presente regolamento è stato presentato nella seduta del Collegio di Direzione del 20 marzo 2026;

4) di individuare quale responsabile del procedimento ai sensi della Legge n. 241/90 la Dott.ssa Rosa Preiti;

5) di trasmettere copia del presente provvedimento a:

- Collegio Sindacale
- Distretti
- Dipartimenti
- Servizi Centrali
- Uffici di Staff.

Letto, approvato e sottoscritto

Responsabile del procedimento ai sensi della L. 241/90:
Rosa Preiti

REGOLAMENTO PER L'UTILIZZO DI DATI PERSONALI A FINI DIDATTICI E DI PUBBLICAZIONE SCIENTIFICA

Sommario

Elenco allegati

Costituiscono parte integrante del Regolamento i seguenti allegati:

- *Allegato 1* Modello di Autorizzazione alla raccolta di dati personali dagli archivi sanitari per finalità didattiche e/o di pubblicazione scientifica;
- *Allegato 2* Allegato Tecnico (tecniche di pseudonimizzazione e anonimizzazione dei dati personali);
- *Allegato 3* Modello di informazioni da rendere agli interessati ai sensi degli artt. 13 e 14 del GDPR;
- *Allegato 4* Modello di consenso.

1. OBIETTIVI

Il presente Regolamento ha l'obiettivo di disciplinare le modalità di trattamento dei dati personali, già legittimamente raccolti e trattati dal Titolare nell'ambito delle attività cliniche e assistenziali, che siano successivamente utilizzati dai professionisti sanitari per finalità di didattica, formazione e pubblicazione scientifica.

2. AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a tutte le operazioni di trattamento dei dati personali, ivi inclusi i **dati rientranti in particolari categorie ex Art.** 9 del Regolamento (UE) 2016/679, svolte dall'Azienda in qualità di Titolare del trattamento per finalità didattiche, formative e di pubblicazione scientifica.

Rientrano nel campo di applicazione del presente Regolamento i trattamenti relativi a dati personali già contenuti negli archivi sanitari e nella ulteriore documentazione sanitaria in possesso dell'Azienda, originariamente raccolti e trattati per finalità di diagnosi, cura e prevenzione e successivamente elaborati, anche mediante tecniche di anonimizzazione e/o pseudonimizzazione, per la produzione di elaborati o materiali destinati ad attività formative, didattiche, di aggiornamento professionale o di divulgazione scientifica, tra i quali, a titolo

esemplificativo:
- redazione di relazioni, contributi scientifici e pubblicazioni, nonché partecipazione a convegni, seminari e iniziative analoghe;
- attività di formazione, approfondimento, discussione e dibattito scientifico relativi a casi clinici, anche nell'ambito esclusivamente aziendale e senza diffusione esterna;
- predisposizione di presentazioni o poster per convegni;
- attività didattiche nell'ambito di lezioni universitarie, corsi di perfezionamento o master extra-aziendali;
- elaborazione di tesi di laurea, master o specializzazione per studi esentati dal parere del Comitato Etico;
- project work relativi a master di II livello o a corsi di formazione manageriale.

Sono esclusi dal campo di applicazione del presente Regolamento **i trattamenti di dati personali effettuati per finalità di ricerca scientifica, medica, biomedica ed epidemiologica,** che restano disciplinati dalla normativa vigente e dalle specifiche disposizioni interne.

Il Regolamento si applica a tutti i professionisti sanitari, dipendenti, collaboratori, tirocinanti, specializzandi o altri soggetti comunque autorizzati al trattamento dei dati personali che operano nell'ambito dell'organizzazione aziendale e che intendano utilizzare tali dati per le finalità sopra indicate.

3. RIFERIMENTI NORMATIVI E DOCUMENTALI

- Regolamento (UE) 2016/679 (GDPR);
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. (Codice privacy);
- Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica, approvato ai sensi dell'articolo 40 del GDPR (Provvedimento del 14 gennaio 2021 Doc-Web 9535402);
- Codici di deontologia applicabili agli esercenti le professioni sanitarie.

Il Regolamento è altresì adottato nel rispetto delle disposizioni e procedure aziendali vigenti.

4. DEFINIZIONI E ABBREVIAZIONI

Termine	**Definizione**
Professionisti sanitari	I soggetti che effettuano prestazioni di prevenzione, diagnosi e cura sotto l'autorità del Titolare del trattamento e che sono vincolati al segreto professionale, così come previsto dal rispettivo Codice di deontologia.
DIP/UO	Dipartimento/Unità operativa
Tecniche di pseudonimizzazione e anonimizzazione	Le misure tecniche descritte nell'*Allegato 1* al presente Regolamento, finalizzate a ridurre o eliminare il rischio di identificazione degli interessati.
Archivio sanitario	L'insieme strutturato della documentazione sanitaria contenente dati personali degli assistiti, relativi alle attività di diagnosi e cura erogate dal Titolare del trattamento.

Termine	Definizione
Dati di natura particolare (ex art. 9 GDPR)	Dati c.d. *"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**.
Titolare del trattamento	L'Azienda sanitaria che, singolarmente o congiuntamente ad altri, determina le finalità e i mezzi del trattamento dei dati personali ai sensi dell'articolo 4, paragrafo 7, del Regolamento (UE) 2016/679.
Interessato	La persona fisica cui si riferiscono i dati personali oggetto di trattamento ai sensi del Regolamento (UE) 2016/679
Dataset	Insieme strutturato di dati personali estratti dall'archivio sanitario del Titolare e sottoposti a processi di anonimizzazione o pseudonimizzazione per le finalità disciplinate dal presente Regolamento.

5. PROCESSO DI TRATTAMENTO DEI DATI PERSONALI

5.1 CATEGORIE DI DATI PERSONALI TRATTATI

Per le finalità sopra indicate, il Titolare del trattamento può trattare dati personali di natura comune, quali dati identificativi, anagrafici (a titolo esemplificativo: codice fiscale, sesso, età, residenza, domicilio, professione, stato civile), nonché dati appartenenti a categorie particolari ai sensi dell'articolo 9 del Regolamento (UE) 2016/679, in particolare dati relativi alla salute.

Tali dati sono sottoposti, nei casi e secondo le modalità previste dal presente Regolamento, a tecniche di anonimizzazione o di pseudonimizzazione, volte rispettivamente a impedire l'identificazione dell'interessato o a ridurre il rischio di identificazione diretta mediante la separazione delle informazioni aggiuntive e l'adozione di adeguate misure tecniche e organizzative.

È in ogni caso vietata l'acquisizione, la duplicazione e/o l'archiviazione di dati personali degli interessati contenuti nella documentazione sanitaria mediante dispositivi personali o con modalità difformi da quelle previste dal presente Regolamento. La violazione di tali disposizioni comporta responsabilità, anche di natura disciplinare, in capo al Professionista sanitario.

5.2 MODALITÀ DI RACCOLTA

L'utilizzo dei dati per le finalità sopra indicate è consentito esclusivamente previo rilascio di **specifica autorizzazione**, a seguito di istanza presentata dal professionista sanitario interessato, preferibilmente mediante compilazione del modello di richiesta (*Allegato 1*).

In particolare:

- **qualora i dati siano contenuti negli archivi sanitari** come sopra descritti, l'autorizzazione è rilasciata dal Responsabile della struttura di afferenza (UO/Dipartimento) del

Professionista richiedente; ove l'autorizzazione sia rilasciata, il Professionista provvede autonomamente all'estrapolazione del dataset di interesse.

- **nel caso in cui i dati siano contenuti nei flussi amministrativi correnti aziendali**, l'accesso ai dati avviene previa presentazione di formale richiesta all'indirizzo istituzionale del Servizio Informativo Aziendale (SIA), secondo le modalità previste dal Regolamento aziendale n. 56 "*Regolamento per la richiesta di dati derivanti e correlati ad attività cliniche e assistenziali da flussi amministrativi correnti aziendali"* .

  In tal caso, a seguito della validazione della richiesta, il SIA provvede all'estrazione dei dati e, ove necessario, alla loro analisi, trasmettendo report, tabelle o database anonimizzati in formato Excel e/o PDF, in base alle necessità rappresentate. Eventuali dataset contenenti dati sensibili sono trasmessi in formato Excel protetto da password, mediante PEC o tramite sistemi di condivisione protetta (es. NEXTCLOUD).

5.3 MODALITA' DI UTILIZZO

A seguito dell'estrapolazione del dataset di interesse, effettuata mediante:

I. estrazione di dati da archivi sanitari, informatizzati o analogici;
II. trasmissione, da parte del SIA, di dataset non anonimizzati;

l'utilizzo di tali dati è consentito esclusivamente previa adozione, da parte del Professionista, delle misure di anonimizzazione o pseudonimizzazione previste nell*'Allegato 2.*

In particolare, il Professionista procede preliminarmente all'applicazione di **tecniche di anonimizzazione** dei dati, secondo quanto dettagliato nel citato *Allegato 2*.

Qualora, all'esito di tale processo, i dati non risultino effettivamente anonimizzati o permanga un rischio significativo di reidentificazione dell'interessato

N.B. *Tale rischio si considera sussistente, in particolare, quando all'interno di un dataset sia possibile:*
- *attribuire una combinazione di valori a una persona fisica identificata o identificabile, anche in ragione della dimensione del campione di riferimento;*
- *correlare almeno due dati riferibili alla medesima persona presenti nella banca dati gestita dal Titolare;*
- *desumere, con un elevato grado di probabilità, il valore di un attributo non noto relativo a un interessato identificabile.*

i dati sono comunque sottoposti a **pseudonimizzazione,** secondo le modalità descritte nell'*Allegato 2*, e il relativo trattamento è consentito esclusivamente **previa acquisizione del consenso dell'interessato**.

6. INFORMAZIONI DA RENDERE ALL'INTERESSATO ED EVENTUALE CONSENSO

Il Titolare del trattamento, in relazione alle attività di trattamento per le finalità sopra descritte, fornisce agli interessati le informazioni di cui agli articoli 13 e 14 del Regolamento (UE) 2016/679.

A tal fine, i professionisti sanitari coinvolti nel trattamento sono tenuti a mettere a disposizione degli interessati l'apposita informativa (*Allegato 3*), assicurandone la conoscibilità prima dell'avvio delle attività di trattamento.

L'informativa è altresì pubblicata e liberamente consultabile nella sezione dedicata "Privacy Policy" del sito istituzionale dell'Azienda.

Come indicato all'articolo 5.3, qualora, anche in considerazione della particolarità, rilevanza, singolarità o notorietà del caso preso in esame, le tecniche di anonimizzazione adottate non siano idonee a garantire la non identificabilità dell'interessato, il trattamento può essere effettuato esclusivamente **previo rilascio di apposito consenso** (*Allegato 4*) da parte dell'interessato.

Eventuali richieste di supporto in merito al modello di consenso e/o informativa possono essere rivolte all'Ufficio Privacy aziendale.

7. MISURE DI ACCOUNTABILITY

I dati personali oggetto di trattamento per le finalità sopra indicate non possono essere trattati al di fuori di quanto previsto dal presente Regolamento.

I Professionisti sanitari mettono in atto misure tecniche ed organizzative adeguate a garantire, che le attività di trattamento dei dati sono effettuate conformemente al GDPR e in particolare al principio di minimizzazione (art. 5, par. 1, lett. c) e par. 2 e 25 GDPR)).

I professionisti sanitari, autorizzati al trattamento come previsto dagli artt. 29 GDPR e 2-quaterdecies del Codice privacy, trattano i dati personali nel rispetto delle istruzioni fornite dal Titolare.

8. CONSERVAZIONE DEI DATI PERSONALI

I dati personali trattati per le finalità previste dal presente Regolamento sono conservati, unitamente all'elaborato didattico, alla richiesta di autorizzazione, alla relativa autorizzazione del responsabile e al modello di consenso sottoscritto dall'interessato, per un periodo di tre anni dalla presentazione; decorso tale termine, essi sono distrutti. La conservazione è a cura del professionista sanitario e potrà avvenire in modalità cartacea e/o analogica, nel rispetto delle misure di sicurezza previste in Azienda.

9. NOTIFICA DI UNA VIOLAZIONE DI DATI PERSONALI

Qualora i dati personali trattati nell'ambito delle attività disciplinate dal presente Regolamento siano oggetto di una violazione che possa comportarne, accidentalmente o in modo illecito, la perdita, la modifica o la divulgazione non autorizzata, il Professionista sanitario è tenuto a darne tempestiva comunicazione secondo le modalità previste dalla procedura per la gestione di violazione dei dati personali (Data Breach) di cui alla Delibera n. 5 dell'11/01/2023.

10. ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Qualora il Professionista sanitario riceva direttamente dall'interessato una richiesta di esercizio dei diritti previsti dalla normativa in materia di protezione dei dati personali, è tenuto a darne tempestiva comunicazione all'Ufficio Privacy aziendale o al Responsabile della Protezione dei Dati (DPO), al fine di agevolarne la corretta e tempestiva evasione, secondo le procedure interne vigenti.

Allegato 1

AUTORIZZAZIONE ALLA RACCOLTA DI DATI PERSONALI
DAGLI ARCHIVI SANITARI PER FINALITÀ DIDATTICHE E/O DI PUBBLICAZIONE SCIENTIFICA

Il/La sottoscritto/a .....
Codice Fiscale .....

in qualità di **Professionista Sanitario**:

☐ Medico / Infermiere / altro (specificare) .....
☐ Laureando
☐ Tirocinante
☐ Borsista
☐ Specializzando
☐ Altro (specificare) .....

operante presso la seguente struttura (*specificare)*.....

CHIEDE

al **Responsabile della struttura** *(specificare):*
.....

l'autorizzazione ad acquisire un **dataset di dati personali** avente le seguenti caratteristiche:

Tipologia di dati
☐ Dati personali appartenenti a categorie particolari (art. 9 GDPR – dati sensibili)
☐ Dati personali di natura comune (non rientranti nelle categorie particolari)

Categoria di interessati cui i dati sono riferiti .....

FINALITA'

(selezionare una o più opzioni)

☐ Tesi di laurea / master
☐ Convegno (specificare) .....
☐ Seminario
☐ Elaborazione di pubblicazione scientifica
☐ Position paper
☐ Poster scientifico
☐ Attività di formazione (specificare reparto/struttura) .....
☐ Approfondimento scientifico
☐ Discussione / dibattito scientifico
☐ Altro (specificare) .....

MISURE DI TUTELA DEI DATI

ANONIMIZZAZIONE	☐	**PSEUDONIMIZZAZIONE**	☐
Sostituzione degli attributi	☐	Crittografia con chiave segreta	☐
Aggiunta di rumore statistico	☐	Funzione hash	☐
Privacy differenziale	☐	Funzione hash cifrata con chiave memorizzata	☐
Permutazione	☐	Crittografia deterministica	☐
Generalizzazione degli attributi	☐	Funzione hash con cancellazione della chive	☐
Aggregazione / K-anonimato	☐	Tokenizzazione	☐
L-diversità	☐	Altre (specificare)	☐

T-vicinanza	☐
Altre (specificare)	☐

Il sottoscritto dichiara che i dati saranno trattati esclusivamente per le finalità sopra indicate, nel rispetto della normativa vigente in materia di protezione dei dati personali (Regolamento UE 2016/679 – GDPR e normativa nazionale applicabile).

Luogo e data.....
Firma del Richiedente.....

Firma del Responsabile che autorizza

.....

Allegato 2

Allegato Tecnico

Tecniche di anonimizzazione e pseudonimizzazione

Anonimizzazione dei dati personali raccolti dagli Enti del SSR

Sommario

Premessa

Si definiscono dati anonimi i dati che, a seguito di specifiche tecniche, risultano irreversibilmente privi degli elementi necessari per qualificarsi come dati personali e di conseguenza non sono assoggettati alla disciplina in materia di protezione dei dati personali dettata dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "Regolamento generale sulla protezione dei dati (GDPR) e dal D.lgs. n. 196/2003 (Codice Privacy).

A tal proposito il considerando 26 del GDPR afferma:

> *"i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca".*

Alla luce di ciò, l'art. 89 del GDPR, promuove l'anonimizzazione ove possibile affermando al par. 1:

> *"Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo".*

In letteratura prevale l'orientamento secondo il quale l'anonimizzazione dei dati non è una misura realizzabile. Secondo tale lettura sussiste sempre un rischio che gli interessati possano essere re-identificati, attraverso una serie di interconnessioni, incroci e combinazioni di dati resi anonimi. Infatti, attraverso l'incrocio di singoli data base in possesso dello stesso Titolare o di Titolari diversi, sarebbe possibile non solo individuare circostanziati target al fine di creare specifiche categorie sulla base dei differenti identikit emersi, ma addirittura risalire all'identità del soggetto.

Questa capacità di re-identificazione a partire da metadati anonimi deriva dal fatto che ogni individuo ha determinati modelli di comportamento. Secondo tali modelli, ad esempio, la frequentazione di determinati siti web e il rilascio di consensi all'uso di cookies analitici può rendere facilmente ricostruibile la propria identità, poiché ogni attività lascia le "impronte digitali" dell'interessato. La raccolta di queste informazioni, anche in possesso di più Titolari, è definita web scraping ed è una pratica molto diffusa, censurata dall'Autorità Garante.

Appare evidente, quindi, che l'anonimato non è mai assoluto e dipende in larga misura dalla varietà dei dati raccolti, dal periodo di tempo, dal progresso tecnologico e dalle modalità con cui vengono conservati.

Pertanto, si può affermare prudentemente che per garantire che i dati personali siano effettivamente anonimi, è fondamentale adottare un approccio sistematico che integri tecniche di anonimizzazione e applichi rigorose procedure di verifica e controllo.

Infine, si richiama l'attenzione sul fatto che i dati anonimi non devono essere confusi con i dati pseudonimizzati. Questi ultimi, infatti, a differenza degli anonimi possono ancora essere ricondotti a un individuo specifico mediante l'uso di informazioni aggiuntive. Ciò fa sì che i dati pseudonimizzati rimangano dati personali e siano soggetti alle disposizioni del GDPR.

L'utilizzo di dati per finalità ulteriori

Ciò detto, il titolare del trattamento, nel promuovere l'uso di dati anonimizzati per finalità ulteriori, rispetto alle finalità per le quali essi sono stati raccolti, dovrà implementare processi atti a raggiungere il grado di irreversibilità conosciuto allo stato dell'arte e dello sviluppo tecnologico.

A tal fine, rappresentano un riferimento:

a) La ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques, che definisce la terminologia e la classificazione delle tecniche di de-identificazione dei dati;
b) Il rapporto OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) che disciplina gli Standard internazionali riservati ai processi per la pseudonimizzazione e l'anonimizzazione;
c) I Principi sulla privacy che incoraggiano l'uso di tecniche di anonimizzazione per la protezione dei dati personali (Emerging privacy enhancing technologies: Maturity, opportunities and challenges);
d) Il Parere 5/2014 del Gruppo di Lavoro Articolo 29 (oggi European Data Protection Board EDPB) che, seppure particolarmente datato, con riferimento allo stato attuale dello sviluppo tecnologico, indica come applicare le tecniche di anonimizzazione (ivi incluse le tecniche ISO/IEC 20889:2018). Il Il Parere descrive, in relazione ai livelli di rischi residui di re-identificazione degli interessati, i seguenti elementi:

   - **Principi di base per l'anonimizzazione**

   Il processo dev'essere irreversibile, ovvero, occorre rendere impossibile risalire all'identità originaria della persona, ovvero non replicabile in senso contrario il processo disposto.

I metodi di anonimizzazione devono essere scelti in base alla natura e agli scopi dei dati trattati, cioè occorre valutare il processo di anonimizzazione in relazione alla finalità del trattamento.

È fondamentale considerare le capacità di attori esterni (ad esempio, hacker) nel tentativo di re-identificazione. È dunque, necessario disporre la valutazione del rischio.

- **Tecniche di anonimizzazione**

Tra le tecniche di anonimizzazione il Gruppo di Lavoro Articolo 29 ha previsto la randomizzazione e la generalizzazione. Nel dettaglio la:

- Randomizzazione prevede l'introduzione di elementi casuali nei dati per impedire correlazioni e include tecniche come Perturbazione e Aggiunta di rumore.
- Generalizzazione comporta la modifica dei dati riducendo il livello di dettaglio, ad esempio attraverso l'Aggregazione (sintesi di informazioni in gruppi più ampi) e la Soppressione (rimozione di dettagli specifici).

- **Criteri di valutazione dell'efficacia**

Ai fini della valutazione dell'efficacia dell'anonimizzazione è utile osservare la:

Resistenza alla re-identificazione, si tratta di una tecnica che deve essere valutata per la sua capacità di impedire tentativi di re-identificazione tramite attacchi di correlazione, combinazione o inferenza.

Perdita di informazioni, l'operazione attraverso la quale si effettua il bilanciamento dell'efficacia della protezione con l'utilità residua dei dati.

- **Analisi dei rischi residui**

È improbabile raggiungere una sicurezza assoluta che il processo di anonimizzazione sia stato pienamente efficace. Pertanto, è necessario valutare costantemente i rischi di re-identificazione in base all'evoluzione delle tecnologie. Una buona pratica è adottare approcci di anonimizzazione che siano proporzionati al rischio e al contesto del trattamento dei dati.

- **Implicazioni normative**

La scelta e l'applicazione delle tecniche di anonimizzazione devono essere sempre documentate e giustificate per dimostrare la conformità all'ordinamento.

Se i dati non sono sufficientemente anonimizzati e consentono la re-identificazione, continuano a rientrare nell'ambito di applicazione della normativa sulla protezione dei dati personali (ad esempio, GDPR).

e) Il Parere n. 28/2024 del European Data Protection Board (EDPB) ha precisato che l'anonimizzazione non rappresenta un processo "una tantum", ma deve essere valutata caso per caso rispetto al contesto, alla disponibilità di dati esterni e ai progressi tecnologici.

Nessuna tecnica è "sicura per definizione": occorre combinare più metodi e applicare valutazioni di rischio costanti. Deve esistere un equilibrio tra anonimato e utilità dei dati. Anche dopo l'anonimizzazione, l'organizzazione deve evitare tentativi di re-identificazione.

L'anonimizzazione dei dati personali di natura particolare

L'attività di anonimizzazione dei dati sanitari ha sue specificità e incontra due distinti profili di criticità.

Infatti, non è possibile adottare le stesse tecniche di anonimizzazione per tutte le categorie dei dati che vengono assoggettati a tale processo. Ogni qualvolta occorra anonimizzare dei dati personali è indispensabile creare procedure ad hoc, che variano in funzione delle categorie dei dati di partenza. Ad esempio: qualora occorra produrre un set di lettere di dimissione anonimizzato a partire da un set di lettere di dimissione nominative, utilizzando una o più tecniche (tra quelle, ad esempio, elencate in seguito) sarà possibile giungere al risultato

voluto. Mentre, per il caso dell'anonimizzazione di un set di referti ambulatoriali potrebbe accadere che la procedura predisposta per l'anonimizzazione delle lettere di dimissione non soddisfi appieno al compito, pur a fronte di set di dati di partenza non così dissimili per natura. Ciò si spiega non solo per la diversa destinazione d'uso che possono avere i due documenti (lettera dimissione e referto ambulatoriale), ma anche, e soprattutto, a causa della diversa struttura concettuale di essi. Tale struttura del documento può generare un rischio di re-identificazione. Quindi, è necessario progettare e realizzare strumenti di anonimizzazione tutte le volte diversi e progettati sempre *ad hoc* rispetto alle finalità.

In seconda battuta, vi è sempre una certa probabilità che un processo di anonimizzazione validato per una certa categoria di informazioni cada in difetto a causa di anomalie presenti nei dati originari.

Ciò rende spesso non percorribili percorsi di anonimizzazione apparentemente semplici, ma che per un numero limitato di casi (nei quali è presente qualche tipo di anomalia) mettono in dubbio l'intero processo.

Ad esempio: molte banche dati sanitarie prevedono la separazione fra dati personali e contenuto del documento. Appare quindi facile pensare che il percorso di anonimizzazione possa semplicemente consistere nel produrre documenti privi della parte nominativa. I referti ambulatoriali sono di questo tipo, ma talvolta il medico che redige il referto inserisce nel testo frasi del tipo: "A seguito delle evidenze diagnostiche riscontrate consigliamo al sig. XXXXXX la terapia XXXXX" o del tipo "Il sig. XXXXXX tornerà a visita il giorno XX/XX/XXXX"

Quindi in questo caso non basterà, come sarebbe sembrato ad una prima analisi, semplicemente eliminare il dato anagrafico dalla intestazione del referto, ma anche adottare delle tecniche di Natural Language Processing (NLP) per ripulire il testo.

Tecniche di anonimizzazione attualmente in uso

Esistono diverse tecniche di anonimizzazione che vengono utilizzate per proteggere i dati personali rendendoli non riconducibili a un individuo specifico.

Soppressione (o Redazione)

Consiste nel rimuovere completamente informazioni sensibili o identificative dai dataset, ad esempio: prevede l'eliminazione dei nomi, dei numeri di identificazione (come il codice fiscale) o degli indirizzi. Tuttavia, questa tecnica può ridurre l'utilità dei dati se vengono rimosse troppe informazioni.

Generalizzazione

Consiste nell'aggregare o ridurre il dettaglio dei dati per diminuire la specificità. Ad esempio:

- Convertire una data di nascita esatta in una fascia d'età (ad esempio, "15/07/1985" diventa "35-40 anni").
- Sostituire un codice di patologia specifico con uno che ne raggruppa una serie generica.

Questa tecnica preserva la struttura del dataset riducendo il rischio di identificazione.

Mascheramento

È la tecnica attraverso la quale i dati originali vengono nascosti utilizzando simboli o valori neutri. Ad esempio:

- Trasformare "Tizio" in "XXXX XXXX".
- Offuscare il codice nosologico lasciando solo le ultime cifre (es. 123-XXX-4567). Si

tratta di una tecnica molto usata durante gli audit.

Aggregazione

La tecnica dell'aggregazione è quella attraverso la quale i dati individuali sono combinati in insiemi o gruppi per rappresentare solo i valori collettivi. Ad esempio: Mostrare i sintomi di una patologia più frequenti rilevati su una corte di pazienti invece dei sintomi soggettivi.

Tuttavia, questa tecnica è utile solo per analisi di tipo aggregato, non per singoli record.

Differential Privacy (Privacy Differenziale)

Si tratta di una tecnica avanzata di anonimizzazione progettata per proteggere la privacy degli individui all'interno di un dataset, pur consentendo analisi statistiche utili. Consiste nell'aggiungere un "rumore" controllato (modifiche casuali) ai dati o ai risultati delle analisi per offuscare i dettagli individuali in modo che anche con accesso illimitato ai risultati, un utente malintenzionato non può determinare con certezza se un particolare individuo è incluso nel dataset. È una tecnica flessibile, può essere applicata sia a singoli dati che ai risultati di query su grandi dataset.

Questa tecnica ha alcuni vantaggi:

- Può essere applicata a diversi scenari, inclusi database, analisi statistiche e addestramento di modelli di machine learning;
- Garantisce protezione anche contro attacchi sofisticati;
- È robusta contro gli attacchi di reidentificazione, anche combinando il dataset con altre fonti di dati.

Tuttavia, essa:

- Introduce un compromesso tra utilità e privacy: un rumore eccessivo può ridurre l'utilità dei dati;
- Richiede competenze matematiche e tecniche per un'implementazione corretta;
- La selezione del valore di epsilon è critica e può essere difficile bilanciarla tra privacy e utilità.

Audit e Monitoraggio Continuo

I due strumenti in esame si basano sulla implementazione di un sistema di revisione periodica per assicurare che le procedure siano seguite e che l'anonimizzazione sia efficace. Alcuni strumenti finalizzati all'attività di audit e monitoraggio continuo sono:

- Il controllo a analisi dei log di accesso;
- L'adozione di Software di monitoraggio dei sistemi di gestione dei dati.

Esistono alcuni strumenti tecnologici utili per l'attività di audit e monitoraggio:

- ARX, Amnesia (software per l'anonimizzazione dei dati particolari);
- Sistemi di tracciamento anonimi basati su barcode (per l'anonimizzazione dei campioni biologici).

Crittografia

È uno dei metodi per rendere un messaggio non comprensibile/intelligibile a persone non autorizzate alla consultazione, garantendo così il requisito di confidenzialità o riservatezza tipico della sicurezza informatica. Esempi di crittografia sono:

- l'algoritmo di cifratura a blocchi a chiave simmetrica, denominato Advanced Encryption Standard (AES)
- La cifratura omomorfica (o homomorphic encryption) che consente di eseguire operazioni su dati cifrati senza doverli decifrare. Questo approccio permette di manipolare i dati cifrati, ad esempio mediante operazioni aritmetiche o booleane, garantendo la privacy delle informazioni stesse. La cifratura omomorfica rappresenta una rivoluzione nella sicurezza dei dati, consentendo l'analisi e l'elaborazione di informazioni sensibili in modo sicuro.

Un approccio innovativo: i dati sintetici

I dati sintetici rappresentano una forma di elaborazione dei dati personali, che può consentire di produrre data set anonimi o fortemente pseudonimizzati. Alla luce di ciò l'utilizzo delle tecniche di sintetizzazione del dato personale è da valutarsi quale tecnica di anonimizzazione esclusivamente quando non consente la re- identificazione.

I dati sintetici derivati da dati personali sono dati generati artificialmente attraverso algoritmi, progettati per replicare le caratteristiche statistiche e strutturali dei dati reali, senza contenere direttamente informazioni riconducibili agli individui, per poi generare nuovi dati che conservano:

- Distribuzione statistica: le correlazioni, i pattern, e i trend dei dati originali.
- Proprietà strutturali: come la gerarchia delle variabili e i tipi di dati.

Esempio: Se abbiamo un dataset con età, sesso, patologia e posizione geografica, i dati sintetici genereranno valori simili rispettando correlazioni come "prevalenza della patologia per sesso nella zona X".

I dati sintetici non contengono dati personali identificabili, poiché sono creati artificialmente, in estrema semplificazione i dati sintetici non includono direttamente le informazioni personali, ma imitano le caratteristiche generali dei dati reali e quindi possono astrattamente essere ricondotti all'identità dell'interessato.

Attualmente vengono impiegati nei:

- Test di software e algoritmi: per allenare sistemi di IA e simulare casi reali;
- Analisi predittiva: per allenare e per costruire modelli senza accedere a dati particolari.

Ottenere dati sintetici, derivati da dati personali, non è una operazione semplice ma richiede risorse tecniche quali grandi capacità computazionali e figure professionali altamente specializzate.

Il processo può essere distinto nelle seguenti fasi:

1. Analisi preliminare dei dati personali

- Qualità dei dati: vanno scelti dati esatti, aggiornati, attendibili, vanno rimossi i dati inconsistenti, e contestualmente sarà fondamentale assicurarsi che i dati reali siano rappresentativi.
- Classificazione: devono essere identificati i tipi di dati (es. personali, particolari, genetici).
- Rispetto delle norme: sarà necessario verificare la base giuridica che sta alla base del trattamento (conformità al GDPR e al D.lgs. 196/2003).

2. Scelta dell'algoritmo di generazione:

I metodi principali includono:

- Modelli statistici tradizionali;
- Modelli basati su Machine Learning (ML)GANs (Generative Adversarial Networks) - Reti neurali generative.

3. Implementazione di strumenti e piattaforme, allo stato attuale sono disponibili i seguenti framework open-source:

- SDV (Synthetic Data Vault): Piattaforma Python per generare dati sintetici basati su modelli probabilistici e GAN;
- CTGAN: Modello GAN ottimizzato per dati tabulariche vengono organizzati in tabelle formate da righe e colonne;
- Scikit-learn: Per la generazione manuale usando distribuzioni standard;
- Hazy, Mostly AI, Gretel.ai: Offrono interfacce user-friendly per generare dati sintetici;
- Altre soluzioni commerciali personalizzate.

4. Validazione dei dati sintetici

- Analisi statistica: verificare che i pattern e le distribuzioni siano coerenti con i dati reali;
- Valutazione sulla privacy: usare metriche come il Differential Privacy per assicurarsi che i dati sintetici non rivelino informazioni di natura particolare;
- Test funzionali: valutare l'usabilità dei dati sintetici rispetto agli obiettivi previsti (es. test software, modelli ML).

5. Accountability

In tale fase, si esegue il check finale prima dell'avvio del trattamento di anonimizzazione, nella quale le operazioni vanno accuratamente registrate al fine di poter dimostrare che durante tutto il processo di generazione dei dati sintetici ci si è attenuti alle tecniche sopra censite.

A tal fine, si rappresenta che esistono degli strumenti per assicurare riservatezza e sicurezza quali:

- Anonimizzazione iniziale: anche se i dati sintetici non contengono dati reali, è buona norma anonimizzare i dataset di input.
- Audit di sicurezza: coinvolgere esperti per verificare che i dati sintetici non siano "re-identificabili".
- Metriche di qualità: bilanciare il compromesso tra accuratezza statistica e privacy.

La sentenza della CJCE

In materia di anonimizzazione la Corte di Giustizia della Comunità Europea (CJCE) con la sentenza C-413/23 P (EDPS / SRB – Deloitte), pronunciata dalla Corte di giustizia il 4 settembre 2025, ha affermato che la pseudonimizzazione non mantiene automaticamente la natura dei dati come "personale" per chiunque: l'identificabilità è relativa al soggetto che tratta le informazioni e va valutata alla luce dei mezzi da lui ragionevolmente utilizzabili per la re-identificazione.

In termini generali, l'approdo giurisprudenziale rappresenta una conferma di principi già consolidati sia nella prassi che nella giurisprudenza UE, seppure sia stata valutata da molti studiosi quale rivoluzionaria.

A parere della CJCE:

> *"la pseudonimizzazione può, a seconda delle circostanze del caso di specie, effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato in modo tale che, per esse, quest'ultimo non sia o non sia più identificabile."*

Ne discende che talvolta il dato pseudonimo può assumere le caratteristiche del dato anonimo purché sia effettuata una valutazione puntuale delle "*circostanze del caso di specie".*

Ovvero, deve essere effettuata una valutazione che tenga conto delle finalità, delle operazioni di trattamento e dei mezzi o strumenti.

Anonimizzazione de facto

Alcuni dati sottoposti a pseudonimizzazione possono essere considerati anonimi. Si tratta di quei casi nei quali la re-identificazione degli interessati è possibile ma straordinariamente onerosa. Ovvero, accade allorquando lo sforzo necessario per giungere alla conoscibilità degli interessati è sproporzionato. Lo sforzo è quantificabile quale sproporzionato quando il carico di lavoro, discendente dall'attività di reidentificazione degli interessati, è tale da paralizzare in modo sostanziale il buon funzionamento dell'amministrazione. Il principio, validato da ANAC con la Deliberazione n. 1309 del 28 dicembre 2016, prevede che lo sforzo da applicare dovrebbe consistere nella individuazione di una o più unità di personale da dedicare esclusivamente all'attività di decodifica dei dati per giungere alla re-identificazione. Oppure, utilizzare strumenti tecnologici che hanno un costo elevato non sostenibile (in tal senso si sottolinea la possibilità di declinare detto costo con le risorse individuate per la pianificazione degli acquisti).

L'esperienza del codice di condotta della Regione Veneto

Con provvedimento n. 7 del 14/01/2021 l'Autorità Garante ha approvato il codice di condotta, proposto dalla Regione Veneto per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica.

Il codice, pur non applicandosi al trattamento di dati personali per finalità di ricerca scientifica, medica, biomedica ed epidemiologica, offre un quadro di riferimento sulle tecniche di anonimizzazione utili alla definizione e alla illustrazione della quale si tratta.

Inoltre, vengono definiti i requisiti e le categorie di dati personali trattati, le modalità di raccolta e uso, le informazioni da rendere all'interessato comprese le modalità di rilascio del consenso, le misure di accountability (tecniche ed organizzative), i tempi di conservazione dei dati personali, nonché le procedure per la notifica di una violazione di dati e l'esercizio dei diritti degli interessati.

In sintesi, oltre alle varie tecniche di anonimizzazione, il codice prende in esame i principi generali del trattamento e sottolinea l'importanza di bilanciare il progresso scientifico con la tutela della privacy e dei diritti degli interessati, proponendo, anche con carattere prescrittivo, misure pratiche e normative per un trattamento etico dei dati.

Considerazioni conclusive

Alla luce di quanto sopra esposto è possibile affermare che gli Enti del SSR necessitano di lavorare su un ampio ventaglio di dati attinenti alla salute e, se correttamente anonimizzati e trattati con adeguate misure di sicurezza, possono essere oggetto di trattamenti dei dati non lesivi per gli interessati.

Dal punto di vista giuridico si ottiene un equo bilanciamento tra la protezione dei dati e la protezione della salute, attraverso l'applicazione delle tecniche di anonimizzazione sopra descritte, tenendo conto:

- di un'adeguata analisi del rischio e valutazione dell'impatto sui diritti e le libertà fondamentali dell'interessato;
- dell'individuazione e applicazione di misure di protezione dei dati "by design" e "by default";
- dell'utilizzo di meccanismi idonei a rendere i dati personali anonimi;
- di una idonea attività di informazione nei confronti degli interessati, che li renda edotti della modalità di esercizio dei diritti, compreso il diritto di non essere sottoposti ad un processo decisionale automatizzato ex art. 22 GDPR.

Pertanto, per assicurare un efficace percorso di anonimizzazione occorre esercitare un approccio metodico e orientato al rischio. Nel dettaglio è raccomandabile:

- Combinare più tecniche per aumentare il livello di protezione;
- Adottare strumenti di anonimizzazione "personalizzati" rispetto alle finalità;
- Monitorare costantemente i progressi tecnologici e aggiornare i metodi utilizzati;
- Integrare l'anonimizzazione nel ciclo di vita del trattamento dei dati come parte della progettazione della privacy (privacy by design).

Bibliografia

- Autorità Garante per la Concorrenza ed il Mercato, Autorità per le Garanzie nelle Comunicazioni, Garante per la protezione dei dati personali, Indagine conoscitiva sui Big Data, 10 febbraio 2020, p.24, consultabile all'indirizzo: https://www.garanteprivacy.it/home/docweb/-/docweb- display/docweb/9264297.
- eHealth Network Towards a common approach for the use of anonymised and aggregatedmobility data for modelling the diffusion of COVID-19, and optimising the effectiveness of responsemeasures: Version 4.3, 30 giugno 2020, consultabile all'indirizzo: https://ec.europa.eu/health/sites/health/files/ehealth/docs/modelling_mobilitydata_en.pdf
- https://www.altalex.com/documents/news/2021/06/08/dati-personali-anonimizzazione-e- pseudonimizzazione
- https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

TECNICHE DI PSEUDONIMIZZAZIONE

Le tecniche di pseudonimizzazione consistono generalmente nella sostituzione di un attributo univoco con un altro, tale da rendere la re-identificazione di un individuo possibile solo per via indiretta. Di conseguenza, la pseudonimizzazione, se utilizzata da sola, pur rappresentando una misura di sicurezza utile, non consente di ottenere un insieme di dati anonimo.

A seguire, un elenco delle tecniche più usate:

- **Crittografia con chiave segreta**: applicando un sistema di crittografia avanzato, la decriptazione può avvenire solamente se si è a conoscenza della chiave;
- **Funzione hash**: corrisponde a una funzione che, a partire dall'immissione di un dataset di una certa dimensione, restituisce un'emissione di pari grandezza. Tale funzione di corrispondenza non è generalmente invertibile; tuttavia, se l'intervallo di valori di immissione relativi alla trasformazione è noto, essa stessa consente di riprodurli al fine di desumere il valore corretto associato a un dato specifico. Alla classica funzione hash viene aggiunto talvolta un valore casuale, il "salt", quale addendum aggiuntivo, rendendo di fatto più difficoltosa l'inversione della trasformazione;
- **Funzione hash cifrata con chiave memorizzata**: corrisponde a una funzione hash particolare che utilizza una chiave segreta quale immissione aggiuntiva, con caratteristiche e finalità simili all'addizione di un salt;
- **Crittografia deterministica o funzione hash cifrata con cancellazione della chiave**: tecnica equiparabile alla selezione di un numero casuale quale pseudonimo di ciascun attributo contenuto nell'insieme di dati, seguita dalla cancellazione della tabella delle corrispondenze;
- **Tokenizzazione**: tecnica derivata dalle precedenti basata tipicamente sull'applicazione di un meccanismo di criptografia univoca o sull'assegnazione, tramite una funzione indicizzata, di un numero sequenziale o di un numero generato casualmente che non deriva matematicamente dai dati originali.

PRINCIPALI CRITICITÀ APPLICATIVE	
Ritenere che un insieme di dati pseudonimizzati sia anonimizzato	La semplice modifica dell'identità non impedisce l'identificazione di una persona interessata se l'insieme di dati continua a contenere quasi-identificatori o se i valori di altri attributi consentono comunque di identificare una persona. Occorre adottare misure supplementari per poter considerare l'insieme di dati effettivamente anonimizzato
Utilizzare la stessa chiave in banche dati diverse	È importante evitare di utilizzare la stessa chiave in banche dati diverse per poter ridurre i rischi legati alla correlabilità
Utilizzare chiavi diverse ("chiavi a rotazione") per diversi utenti	Una rotazione della chiave secondo regole specifiche agevolerebbe la correlabilità delle informazioni corrispondenti a una determinata persona
Conservare la chiave	È assolutamente da evitare la conservazione della chiave segreta in mancanza di adeguate misure di sicurezza o del necessario isolamento dal dataset in chiaro

TABELLA DI ESPOSIZIONE A RISCHI PER METODOLOGIA

La seguente tabella ha lo scopo di illustrare le debolezze intrinseche di ciascuna delle tecniche analizzate rispetto alle tipologie di rischio ai quali i trattamenti di anonimizzazione e pseudonimizzazione sono soggetti. Dal prospetto riportato, risulta evidente come si renda necessario per ogni caso preso in esame, un'applicazione combinata specifica di queste metodologie tale da garantire la tutela degli interessati.

	RISCHIO DI INDIVIDUAZIONE	**RISCHIO DI CORRELABILITÀ**	**RISCHIO DI DEDUZIONE**
Sostituzione	Sì	Sì	Possibile
Rumore Statistico	Sì	Possibile	Possibile
Privacy differenziale	Possibile	Possibile	Possibile
Permutazione	Possibile	Possibile	Possibile
Aggregazione / K-Anonimato	No	Sì	Sì
L-Diversità / T-Vicinanza	No	Sì	Possibile
Pseudonimizzazione	Sì	Sì	Sì

Allegato 3

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 13 del Regolamento (UE) 2016/679

PER FINI DIDATTICI E DI PUBBLICAZIONE SCIENTIFICA

Gentile,

l'Azienda USL di Bologna, nella Sua qualità di Titolare del trattamento, La informa che tra le proprie finalità di trattamento dei dati personali è di estrema rilevanza anche lo sviluppo e l'accrescimento delle conoscenze e competenze e il costante miglioramento della qualità dei servizi offerti. A tal fine, previa adozione di tecniche di anonimizzazione, i suoi dati personali ed in particolare quelli di salute, già oggetto di trattamento per finalità di cura, potranno essere trattati per l'elaborazione di:

- tesi di laurea/master
- pubblicazioni scientifiche
- presentazione a convegni
- seminari
- position paper
- poster scientifici
- case-study

Il trattamento dei dati personali viene effettuato con modalità tali da garantire e assicurare la non identificabilità dell'interessato, mediante tecniche di:

- Anonimizzazione: Risultato di tecniche che vengono applicate ai dati personali con il fine di rendere la re identificazione ragionevolmente impossibile.
- Pseudonimizzazione: Elaborazione consistente nella sostituzione di un attributo di identificazione univoco legato ad una collezione di dati con uno pseudonimo, tale che il collegamento con l'Interessato non sia più immediatamente possibile senza l'uso di informazioni aggiuntive, tenute separate e messe in sicurezza con misure tecniche e organizzative adeguate.

Base giuridica del trattamento dei dati

Il trattamento dei dati personali viene effettuato previa anonimizzazione per esclusive finalità didattiche e per la produzione degli elaborati sopra descritti, con modalità tali da garantire e assicurare la non identificabilità dell'interessato. Nel caso in cui, in considerazione della particolarità, rilevanza, singolarità o notorietà del caso preso in esame, le tecniche di anonimizzazione applicate non siano in grado di garantire che Lei non possa essere identificato, Le sarà somministrata una specifica ed ulteriore nota di informazioni, prima di procedere al trattamento, e Le sarà richiesto l'apposito consenso (articolo 6, par. 1 lettera a) e nell'articolo 9 par. 2 lettera a) del GDPR), in mancanza del quale non si procederà ad alcun trattamento.

Categoria di dati e fonte da cui hanno origine

Per le finalità didattiche e di pubblicazione scientifica potranno essere raccolti ed elaborati dati personali e appartenenti a categorie particolari, tra cui: dati anagrafici e dati relativi allo stato di salute degli assistiti presenti negli archivi del Titolare.

Natura del conferimento dei dati

Il conferimento dei dati richiesti per l'espletamento delle suddette attività è facoltativo.

Un eventuale rifiuto di fornire i dati non avrà conseguenze negative sulla possibilità di usufruire delle prestazioni sanitarie richieste.

Il consenso, una volta manifestato, potrà essere modificato e/o revocato in qualsiasi momento.

Modalità di trattamento – utilizzo dei dati

Le attività di trattamento dei dati personali per finalità didattiche sono effettuate, previa adozione di misure adeguate di sicurezza tecnica ed organizzativa, con modalità elettroniche e/o analogiche da parte di soggetti appositamente autorizzati dal Titolare, in ottemperanza a quanto previsto dagli articoli 29 e 32 del Regolamento UE, rispettando i

principi di necessità, liceità, correttezza, trasparenza, esattezza, proporzionalità, pertinenza e non eccedenza nel trattamento.
I dati personali oggetto di trattamento sono sottoposti ad apposite modalità di anonimizzazione o di pseudonimizzazione allo scopo di non rendere identificabile gli Interessati.

Eventuali destinatari/categorie di destinatari dei dati personali
Le elaborazioni finalizzate alle pubblicazioni scientifiche avvengono in modalità anonimizzata e/o pseudonimizzata tramite personale interno autorizzato. I contenuti verranno condivisi con: gli utenti delle riviste medico/scientifiche, i partecipanti delle attività congressuali e tutti i possibili destinatari delle attività indicate nei punti precedenti. Con riferimento alle tesi, il trattamento dei dati avverrà tramite i tutor e gli studenti previamente autorizzati. I dati anonimizzati o pseudonimizzati, utilizzati per le tesi, possono entrare nella disponibilità degli Istituti/Università (Titolari del trattamento), per cui gli studenti ne rielaborano i contenuti. Le tesi possono essere oggetto di diffusione attraverso la loro pubblicazione.

Tempi di conservazione dei dati
I dati personali oggetto di trattamento per fini didattici, sottoposti a tecniche di anonimizzazione o di pseudonimizzazione sono conservati in copia conforme all'elaborato didattico per la durata di tre anni a seguito della sua presentazione e successivamente distrutti.

Trasferimento dei dati personali a paesi extra UE
I Suoi dati personali non saranno trasferiti a Paesi extra UE

Diritti dell'interessato
In qualità di interessato, in relazione ai dati personali oggetto della presente informativa, Lei ha facoltà di esercitare i diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679, e in particolare:

- diritto di accesso, ovvero la possibilità di essere informato sui trattamenti effettuati sui propri dati personali ed eventualmente riceverne copia (art. 15);
- diritto di rettifica dei propri dati personali inesatti (art. 16);
- diritto alla cancellazione dei propri dati personali senza ingiustificato ritardo, c.d. diritto all'oblio (art. 17);
- diritto di limitazione di trattamento dei propri dati personali nei casi e nei limiti di cui all'art. 18;
- diritto di opposizione al trattamento dei propri dati personali (art. 21);
- diritto di non essere sottoposto a processi decisionali automatizzati (art. 22).

Con riferimento alle finalità sopra richiamate, in qualità di interessato, Lei ha facoltà di procedere, in ogni momento, alla revoca del consenso al trattamento ai sensi dell'art. 7 del Regolamento (UE) 2016/679, ferma restando la liceità del trattamento effettuato sulla base del consenso successivamente revocato.

Le modalità di esercizio di tali diritti sono indicate nella pagina del sito internet aziendale.

Ricorrendone i presupposti, Lei ha, altresì, il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali ovvero all'autorità di controllo dello Stato membro UE in cui risiede abitualmente, lavora ovvero del luogo ove si è verificata la presunta violazione, secondo le procedure previste ai sensi dell'art. 77 del GDPR.

Titolare del trattamento
Il Titolare del trattamento è l'Azienda USL di Bologna con sede in Via Castiglione, 29 - 40124 Bologna - telefono 0516584910, PEC protocollo@pec.ausl.bologna.it

Data Protection Officer
Il Responsabile della Protezione dei Dati (DPO) può essere contattato all'indirizzo e-mail: dpo@aosp.bo.it – PEC: dpo@pec.aosp.bo.it

Ogni ulteriore informazione riguardante il trattamento dei Suoi dati, anche relativamente al trattamento dei dati per ulteriori attività, è reperibile sul sito istituzionale dell'Azienda USL di Bologna: https://www.ausl.bologna.it/privacy

Allegato 4

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Con la presente, il/la sottoscritto/a

Cognome: _____
Nome: _____
Data e luogo di nascita: _____

(Nel caso di soggetto diverso dall'interessato)
Il/la sottoscritto/a _____,
in qualità di rappresentante legale (*)
(specificare: esercente la responsabilità genitoriale / tutore / curatore / amministratore di sostegno)

di
Nome e Cognome: _____

dichiara

di aver ricevuto informazioni chiare, comprensibili ed esaurienti in merito al trattamento dei dati personali e di aver letto e compreso l'informativa fornita per iscritto.

e

☐ **presta il consenso** ☐ **nega il consenso**

affinché i propri dati personali, trattati mediante tecniche di pseudonimizzazione tali da non consentire la reidentificazione diretta dell'interessato, possano essere utilizzati per la produzione di elaborati e/o materiali destinati ad attività formative, didattiche, di aggiornamento professionale o di divulgazione scientifica.

Luogo e data: _____

Firma: _____