
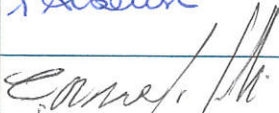
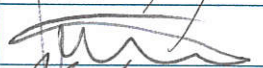
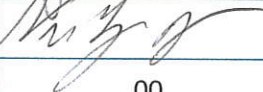


PROCEDURA AZIENDALE PER LA CORRETTA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento (UE) 2016/679

Redazione	Direttore U.O.C. Programmazione e Controllo di Gestione e Sistemi Informativi Aziendali		
Verifica	Responsabile Protezione Dati		
Approvazione	Direttore Medico di Presidio		
	Direttore Dipartimento Amministrativo		
	Rev.	00	01
	Data	Marzo 2020	

**PROCEDURA AZIENDALE PER LA CORRETTA
GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI**
ai sensi dell'art. 33 del Regolamento (UE) 2016/679

SOMMARIO

1. PREMESSA.....	3
2. SCOPO E AMBITO DI APPLICAZIONE	3
3. DEFINIZIONI.....	3
4. DESTINATARI.....	4
5. NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).....	4
6. MODALITÀ DI COMUNICAZIONE AGLI INTERESSATI.....	5
7. POSSIBILI SCENARI DATA BREACH	5
8. REGISTRO DELLE VIOLAZIONI.....	7
9. NORMATIVA DI RIFERIMENTO	7
ALLEGATO 1 - NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).....	8
ALLEGATO 2 – COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI ALL’INTERESSATO	9
ALLEGATO 3 – REGISTRO DELLE VIOLAZIONI (DATA BREACH).....	10

1. PREMESSA

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifrazione non autorizzata di informazioni criptate, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, perdita di riservatezza da parte di personale non attinente al ruolo e alla funzione, qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Il Regolamento Generale sulla Protezione dei Dati (GDPR) introduce l'obbligo di notificare una violazione dei dati personali (di seguito "violazione") all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

La mancata segnalazione di una violazione può comportare l'imposizione di una sanzione al Direttore della U.O.C./ Responsabile della U.O.S.D..

2. SCOPO E AMBITO DI APPLICAZIONE

Lo scopo della presente procedura è di definire, nel rispetto della normativa di riferimento, le modalità operative per una corretta e tempestiva gestione delle violazioni dei dati personali trattati dal Grande Ospedale Metropolitano "Bianchi Melacrino Morelli" di Reggio Calabria.

Pertanto, con il presente documento si definiscono e regolamentano:

- le modalità operative per la tempestiva segnalazione al Responsabile Protezione dati della violazione di dati personali;
- i processi da mettere in atto per essere in grado di rilevare e limitare tempestivamente gli effetti di una violazione di dati personali;
- le modalità e i criteri per la notifica della violazione all'autorità di controllo competente da parte del legale rappresentante del G.O.M. di Reggio Calabria;
- le modalità e i criteri per l'eventuale comunicazione alle persone fisiche interessate, ove necessario.

3. DEFINIZIONI

Dato personale: qualsiasi informazione che identifica o rende identificabile un persona fisica (quali per esempio nome, cognome, codice fiscale, numero di telefono); rientrano nella categoria "Dati personali" anche i dati che consentono di rilevare lo stato di salute (quali ad esempio (referti, esami diagnostici, dati genetici e biometrici, malattie in corso o avute, ecc.).

Trattamento: 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, come 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, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6)(ad es. archivio storico aziendale, archivio di reparto, armadi contenenti dati e informazioni sullo stato di salute).

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7). In questo contesto, è titolare del trattamento Grande Ospedale Metropolitano "Bianchi Melacrino Morelli" di Reggio Calabria.

Responsabile Protezione Dati o Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

Responsabile del trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno di ASP che determina specifiche modalità organizzative rispetto ad uno o più trattamenti. Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, punto 8)(quali ad es. fornitori, associazioni di volontariato, ecc.)

Violazione dei dati personali (data breach): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12)

4. DESTINATARI

La presente procedura è rivolta a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del G.O.M. quali:

- i Direttori/Responsabili di U.O., gli incaricati al trattamento, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare (di seguito "destinatari interni");
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dai destinatari interni che, in ragione del rapporto contrattuale in essere con il Titolare abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 del GDPR o di autonomo Titolare del trattamento (di seguito "destinatari esterni"), di seguito genericamente denominati "destinatari".

Tutti i destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione. Tale procedura viene, pertanto, pubblicata sul sito istituzionale nonché nell'area riservata del portale del dipendente.

5. NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

La notifica deve essere trasmessa utilizzando il modello allegato alla presente procedura (Allegato 1) attraverso il protocollo informatico "Lapis web", anticipandola telefonicamente:

- al Responsabile dei Sistemi Informativi Aziendali in caso di violazione di dati gestiti su sistemi informatici o analogici;
- alla U.O.C. Direzione Medica di Presidio in caso di violazione di documenti cartacei di tipo sanitario,
- alla U.O.C. Affari Generali, Legali e Assicurativi in caso di violazione di atti amministrativi.

La stessa notifica deve essere trasmessa, per conoscenza, anche al Responsabile Protezione Dati.

Il Legale Rappresentante pro tempore, in qualità di titolare del trattamento, a quel punto, per il tramite del Responsabile Protezione Dati, dovrà notificare l'evento all'autorità di controllo, tranne che nel caso in cui "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*" (es. perdita di una chiavetta usb con dati cifrati).

La notifica all'autorità di controllo deve avvenire **senza ingiustificato ritardo** e, ove possibile, *entro 72 ore* dal momento in cui ne è venuto a conoscenza il Titolare. Qualora la notifica non avvenga nelle 72 ore, il titolare dovrà precisare anche i motivi del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).

6. MODALITÀ DI COMUNICAZIONE AGLI INTERESSATI

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate, senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'eventuale comunicazione all'interessato/agli interessati (Allegato 2), a firma del titolare, deve inviarsi nei tempi e nei modi che lo stesso individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

7. POSSIBILI SCENARI DATA BREACH

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui dati personali dei pazienti, dei lavoratori, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti (es. dati idonei a rilevare lo stato di salute), una perdita, un danno alla vita privata dei pazienti e qualsiasi altro significativo svantaggio economico o sociale.

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella valutazione in merito alla necessità di effettuare o meno la notifica di *data breach* all'Autorità Garante.

Tipi di violazioni dei dati personali:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

TIPO DI BREACH	DEFINIZIONE	CRITERI PER LA SEGNALEAZIONE	ESEMPI DI CASI DA SEGNALEARE	ESEMPI DI CASI DA NON SEGNALEARE
DISTRUZIONE	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Dati non recuperabili o provenienti da procedure non ripetibili.	Guasto non riparabile dell'hard disk contenente dati attinenti lo stato di salute uno o più referti che, in violazione al regolamento, erano salvati localmente. Incendio di archivio cartaceo delle cartelle cliniche. Distruzione di campioni biologici.	Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia). Rottura di un PC che non contiene dati personali originali. Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura. Rottura server.
PERDITA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo ed è possibile che terzi possano avere impropriamente accesso al dato.	Dati non recuperabili o provenienti da procedure non ripetibili. Dati la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato.	Smarrimento di chiavetta USB contenente dati originali. Smarrimento di fascicolo cartaceo personale dipendente.	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa.
MODIFICA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Modifiche sistematiche su più casi.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup. Azione involontaria, o fraudolenta, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery. Azione involontaria di un utente che porta all'alterazione di dati tracciata e reversibile. Modifica di un documento non ancora validato dal proprio autore.
DIVULGAZIONE NON AUTORIZZATA	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione. Diffusione dati personali mediante pubblicazione su sito aziendale. Diffusione immagini dei pazienti su social network.	Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet. Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
ACCESSO NON AUTORIZZATO	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolari ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi. Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico.	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi. Accesso non autorizzata di un documento non ancora validato dal proprio autore.
INDISPONIBILITÀ TEMPORANEA DEL DATO	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup. Cancellazione accidentale dei dati da parte di una persona non autorizzata. Perdita della chiave di decrittografia di dati crittografati in modo sicuro.	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso.

Un *data breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).

I casi di *data breach* per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach*, ma è considerato un normale errore procedurale. Questo poiché chi riceve non può sapere a quale paziente fisico è riferito il testo o il paziente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

8. REGISTRO DELLE VIOLAZIONI

Il Titolare del trattamento, con il supporto del Responsabile Protezione Dati (RPD), cura l'aggiornamento del registro delle violazioni (Allegato 3), ai sensi dell'art. 33 comma 5 del GDPR.

9. NORMATIVA DI RIFERIMENTO

- Regolamento UE n. 2016/679 (GDPR).
- Decreto Legislativo 18 maggio 2018, n. 51 *“Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”*.
- Linee guida in materia di notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 - WP250rev.01.
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019.

ALLEGATO 1 - NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

(art. 33 del Regolamento (UE) 2016/679 e art. 26 del d.lgs. n. 51/2018)

Sezione A - Dati del soggetto che effettua la notifica

Cognome e nome _____

E-mail _____

Recapito telefonico _____

Funzione rivestita _____

Sezione B – Ulteriori soggetti coinvolti nel trattamento

Denominazione _____

Riferimenti _____

Denominazione _____

Riferimenti _____

Sezione C - Informazioni in sintesi

Quando si è venuti a conoscenza della violazione _____

Come si è venuti a conoscenza della violazione _____

Breve descrizione _____

Natura della violazione

Perdita di confidenzialità

Perdita di integrità

Perdita di disponibilità

Causa della violazione

Azione intenzionale interna

Azione accidentale interna

Azione intenzionale esterna

Azione accidentale esterna

Sconosciuta

Note _____

Sezione D - Comunicazioni agli interessati

Comunicazioni effettuate agli interessati _____

Comunicazione effettuate a soggetti interni _____

Comunicazione effettuate a soggetti esterni _____

Sezione E - Altre informazioni

ALLEGATO 2 – COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali (Regolamento (UE) 679/2016), il Grande Ospedale Metropolitano "Bianchi Melacrino Morelli" di Reggio Calabria, titolare del trattamento, con la presente Le comunica l'intervenuta violazione dei Suoi dati personali (data breach), che si è verificata in data _____ alle ore _____ e/o di cui si è avuta conoscenza in data _____ alle ore _____.

A) Descrizione della natura della violazione

Modalità della violazione dei dati: _____.

Tipo di violazione:

- Lettura,
- Copia (i dati sono ancora presenti sui sistemi del titolare),
- Alterazione (i dati sono stati alterati),
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione),
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione).

Dispositivo oggetto di violazione:

- Computer, Rete, Dispositivo mobile, Strumento di backup, Documento cartaceo.

Tipo di dati oggetto di violazione:

- Dati anagrafici,
- Dati di accesso e di identificazione (user name, password, altro),
- Dati personali idonei a rivelare l'origine razziale ed etnica,
- Dati personali idonei a rivelare lo stato di salute,
- Dati personali idonei a rivelare la vita sessuale,
- Dati giudiziari,
- Dati genetici,
- Dati biometrici,
- Dati _____
- Ancora sconosciuti.

B) Descrizione delle probabili conseguenze della violazione di dati personali:

C) Descrizione delle misure tecnologiche e organizzative assunte per porre rimedio alla violazione e se del caso per contenere la violazione dei dati o per attenuarne i possibili effetti negativi:

Per maggiori informazioni relativamente alla violazione in oggetto, si forniscono i seguenti recapiti:

posta elettronica:

pec: protocollo@pec.ospedalerc.it

indirizzo:

