OSPEDALE POLICLINICO SAN MARTINO
Sistema Sanitario Regione Liguria
Istituto di Ricovero e Cura a Carattere Scientifico

PROCEDURA AZIENDALE

GESTIONE DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DI DATI PERSONALI

Redazione:

- Data Protection Officer
- Ufficio Privacy (U.O. Affari Generali e Legali)
- Referente Privacy dell'U.O. Affari Generali e Legali

Controllo e validazione:

- Direttore Sanitario
- Direttore Amministrativo
- Direttore dell'U.O. Information & Communication Technologies

Approvazione per la pubblicazione:

- Direttore Generale

Acronimi

D.A. Direttore Amministrativo
DPO Data Protection Officer
D.S. Direttore Sanitario
EDPB Comitato europeo per la protezione dei dati (organismo europeo indipendente sotto la cui egida si riuniscono le Autorità nazionali per la protezione dei dati personali dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati)
GDPR General Data Protection Regulation (ovvero il Regolamento UE 2016/679 "Regolamento Generale sulla Protezione dei Dati)
ICT Information & Communication Technologies
I.O. Istruzione Operativa
MOD Modulo
PQAZ Procedura Aziendale
S.S.D. Struttura Semplice Dipartimentale
U.O. Unità operativa
WP29 Gruppo di lavoro "Articolo 29" (istituito dalla direttiva 95/46/CE, si è occupato delle questioni relative alla tutela della privacy e dei dati personali fino al 25 maggio 2018 - entrata in vigore del GDPR - e successivamente è stato sostituito dal EDPB).

Modifiche effettuate alla revisione precedente

Num. Rev.	Capitolo/Pag modificate	Descrizione tipo/natura della modifica
Rev. 0	-------	Nuovo documento

1. GENERALITÀ

Il Regolamento (UE) 2016/679 (di seguito GDPR) prevede che l'IRCCS Ospedale Policlinico San Martino (di seguito Policlinico) in quanto Titolare del trattamento, debba garantire la protezione dei dati personali adottando tutte le misure tecniche e organizzative adeguate a prevenire eventuali violazioni, tenuto conto anche del rischio presentato dal trattamento.

L'art. 32 del GDPR prevede che il Policlinico tratti i dati personali degli Interessati garantendo, in particolare, un'adeguata protezione da trattamenti non autorizzati, illeciti o da perdite e distruzioni dei dati personali nonché, in generale, da ogni altra ipotesi di violazione.

Il considerando 87 del GDPR stabilisce che sia opportuno *"verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'Autorità di controllo e l'Interessato […]".*

Ai sensi degli articoli 33 e 34 GDPR, nel caso in cui venga a determinarsi un incidente o una violazione dei dati personali trattati, compete al Policlinico, Titolare del Trattamento:

a) valutare e qualificare l'evento;
b) procedere, in presenza dei relativi presupposti, a notificare all'Autorità Garante e a comunicare l'accaduto agli Interessati;
c) implementare, alla luce delle criticità rivelate dalla violazione, le proprie misure tecniche e organizzative di sicurezza.

Pertanto, in ragione della normativa ora richiamata, il Policlinico adotta misure tecniche e organizzative adeguate al rischio di violazione, che dovranno essere determinate secondo i parametri fissati dalla presente Procedura.

Il presente documento, pertanto, si prefigge lo scopo di indicare agli operatori del Policlinico le opportune modalità di gestione dell'incidente sulla sicurezza o della violazione dei dati personali nel rispetto della normativa in materia di trattamento dei dati personali.

2. RESPONSABILITÀ

- Direttore Generale
- Direttore Sanitario
- Direttore Amministrativo
- Direttore U.O. ICT
- Ufficio Privacy (U.O. Affari Generali e Legali)

3. CONTENUTI

3. 1 BREVI CENNI SULLA GESTIONE DELLE MISURE DI SICUREZZA NELLE STRUTTURE SANITARIE

Le strutture sanitarie sono tenute ad adottare tutte le misure tecniche ed organizzative necessarie per evitare che i dati dei loro pazienti siano comunicati per errore ad altre persone.
Sin da subito appare indispensabile assumere un comportamento proattivo volto a mitigare il margine di errore; indispensabile è dunque dimostrare un elevato grado di cooperazione con l'Autorità Garante e fare in modo che gli episodi abbiano caratteristiche di sporadicità.

L'adozione di una procedura interna è considerata anch'essa un elemento di prova utile a dimostrare il rispetto del principio cardine del GDPR, l'accountability, volto ad assicurare un assetto di piena responsabilizzazione nella corretta gestione del flusso delle informazioni che governano i processi aziendali.
Si ricorda che le informazioni sullo stato di salute possono essere comunicate a terzi solo sulla base di un presupposto giuridico o su indicazione della persona interessata, previa delega scritta.
Il Policlinico è pertanto tenuto al pieno rispetto dei principi di correttezza e trasparenza, adottando misure tecniche ed organizzative utili non solo a proteggersi da attacchi informatici, ma anche ad evitare violazioni di dati personali, in particolari quelli più delicati, come quelli sulla salute, troppo spesso causate da inadeguate procedure gestionali.

3.2 INDICAZIONI OPERATIVE RIVOLTE AL TITOLARE

Il Policlinico, così come previsto dal GDPR, ha adottato misure di prevenzione delle violazioni di dati personali e dispone che:

tutte le segnalazioni relative a notizia di furto o smarrimento di documentazione che riporta dati personali e particolari oppure di dispositivi di memoria che comportino la eventuale possibilità che terzi possano aver avuto accesso non autorizzato a tali dati vengano inoltrate al seguente indirizzo e-mail:
- ufficio.privacy@hsanmartino.it

Analoga attività deve essere assicurata in caso di:

- eventuali comunicazioni di dati, anche via e-mail, a soggetti diversi dagli autorizzati di specifico riferimento o nel caso in cui i dati personali non siano più disponibili a causa di distruzione, cancellazione o di altri problemi di natura anche automatizzata, come ad esempio un virus;

- ricezione di notizia di una possibile violazione di dati personali (cfr. par. 3.4 "Definizioni"), ad esempio nel caso in cui un terzo informi di aver ricevuto dall'azienda una comunicazione non destinata a lui contenente dati personali.

Nel caso di segnalazioni provenienti da soggetti esterni all'organizzazione del Policlinico le stesse dovranno essere inoltrate al predetto indirizzo di posta elettronica e, in caso di protocollazione, assegnate all'U.O Affari Generali e Legali – Ufficio Privacy.

L'Ufficio Privacy, valutata la rilevanza dell'episodio segnalato, condivide la comunicazione pervenuta con il Gruppo di Gestione Incidenti di Sicurezza (cfr. par. 3.5, lett. b per la composizione del Gruppo): laddove a seguito di esame congiunto si ravvisi la sussistenza di effettivo *data breach*, il Titolare avvia la procedura di segnalazione al Garante.
In alternativa l'episodio viene annotato nel registro degli incidenti di sicurezza.

3.3 LINK AUTORITÀ GARANTE

- servizio telematico dedicato alla notifica del data breach: HTTPS://WWW.GARANTEPRIVACY.IT/REGOLAMENTOUE/DATABREACH

3.4 DEFINIZIONI

NOZIONE DI "INCIDENTE DI SICUREZZA" E "VIOLAZIONE DEI DATI PERSONALI"

Per **"incidente di sicurezza"** si intende qualsiasi evento critico che interessa il sistema di protezione dei dati personali e che può ricomprendere la "violazione dei dati personali".

Tutte le violazioni di dati personali sono anche incidenti di sicurezza, mentre non è vero l'inverso: alcuni incidenti di sicurezza non comportano violazione dei dati personali.

La "**violazione dei dati personali"** o "***data breach***" è definita dall'articolo 4, punto 12, del GDPR come *"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".*

Il **criterio di distinzione** tra incidente di sicurezza e violazione dei dati risiede nelle conseguenze dannose dell'evento critico: l'evento deve essere considerato una violazione dei dati (*data breach*) nell'ipotesi in cui il Policlinico, a seguito dell'incidente, non dovesse essere più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR, con conseguente pericolo o danno ai diritti, libertà e dignità degli Interessati.

TIPOLOGIE DI INCIDENTE DI SICUREZZA

Preliminarmente devono essere individuate due diverse categorie di incidenti di sicurezza, a seconda della causa che ha determinato l'incidente (natura dell'incidente):

NATURA DELL'INCIDENTE	
INFORMATICA	Causato da eventi che interessano applicativi o dispositivi informatici, ad esempio attacchi hacker, cancellazione di database, accessi abusivi alle reti aziendali, furto o diffusione illecita dei dati durante la trasmissione fra software ecc…
ANALOGICA	Causato da eventi che non interessano applicativi o dispositivi informatici, come ad esempio, smarrimento di documenti, distruzione di archivi cartacei, perdita di dispositivi rimovibili di archiviazione dati ecc...

Il GDPR, all'articolo 32 par. 2, individua specifiche tipologie di rischio del trattamento che, anche alla luce delle *"Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679",* adottate dal WP29 (di seguito "Linee guida"), sono di seguito dettagliate.

TIPOLOGIE DI RISCHIO	
DISTRUZIONE	Ipotesi in cui a seguito dell'evento i dati non esistono più o non esistono più in una forma che sia di qualche utilità per il TITOLARE poiché danneggiati o corrotti
PERDITA DEFINITIVA	Ipotesi in cui i dati potrebbero comunque esistere, ma il TITOLARE potrebbe averne perso il controllo, l'accesso o il possesso. Qualora i dati non siano più recuperabili la perdita è definitiva ed equivale ad una distruzione. Un esempio di perdita definitiva può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware*. Si ha perdita dei dati anche nel caso in cui il TITOLARE abbia adottato come misura di sicurezza la crittografazione dei dati mediante una chiave non più in suo possesso.
PERDITA NON DEFINITIVA	Ipotesi in cui i dati non sono più nel possesso del Policlinico ma l'accesso o il controllo può essere recuperato. Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati in cui sono contenuti dati personali degli Interessati. Un altro esempio può essere la cancellazione accidentale dei dati comunque conservati in copia.
ACCESSO NON AUTORIZZATO	Ipotesi in cui un soggetto non autorizzato ha accesso al sistema dei dati personali nella titolarità del Policlinico, che comporta la visualizzazione non consentita dei dati con l'ulteriore rischio di un'appropriazione.
MODIFICA NON AUTORIZZATA	Ipotesi in cui si ha una modifica dei dati personali diversa dalla cancellazione eseguita da un soggetto che non sia autorizzato a tale operazione, che può derivare da un accesso completamente illegittimo o dall'accesso di un soggetto autorizzato alla modifica di una parte del database che però, data la mancanza di adeguate

	misure di sicurezza, modifica dati di cui non dovrebbe avere la disponibilità.
DIVULGAZIONE NON AUTORIZZATA	Ipotesi in cui si ha la trasmissione dei dati personali, da parte di un soggetto non autorizzato, a soggetti terzi o la divulgazione di dati personali da parte di un soggetto autorizzato verso terzi che non sono abilitati alla ricezione degli stessi.

TIPI DI VIOLAZIONI DI DATI PERSONALI

Una violazione di dati personali (*data breach*) può essere di tre diverse tipologie, anche combinate tra di loro:

VIOLAZIONE DELLA RISERVATEZZA	Ipotesi in cui si ha divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali
VIOLAZIONE DELL'INTEGRITÀ	Ipotesi in cui si ha modifica non autorizzata o accidentale dei dati personali
VIOLAZIONE DELLA DISPONIBILITÀ	Ipotesi in cui si ha perdita o distruzione accidentale o non autorizzata di dati personali

A seguito di un incidente di sicurezza può generarsi un danno significativo ai diritti delle persone fisiche, quali ad esempio danni fisici, perdita del controllo da parte degli Interessati sui dati personali, limitazione della libertà o pregiudizio per l'esercizio dei diritti, discriminazione, furto d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto d'ufficio.

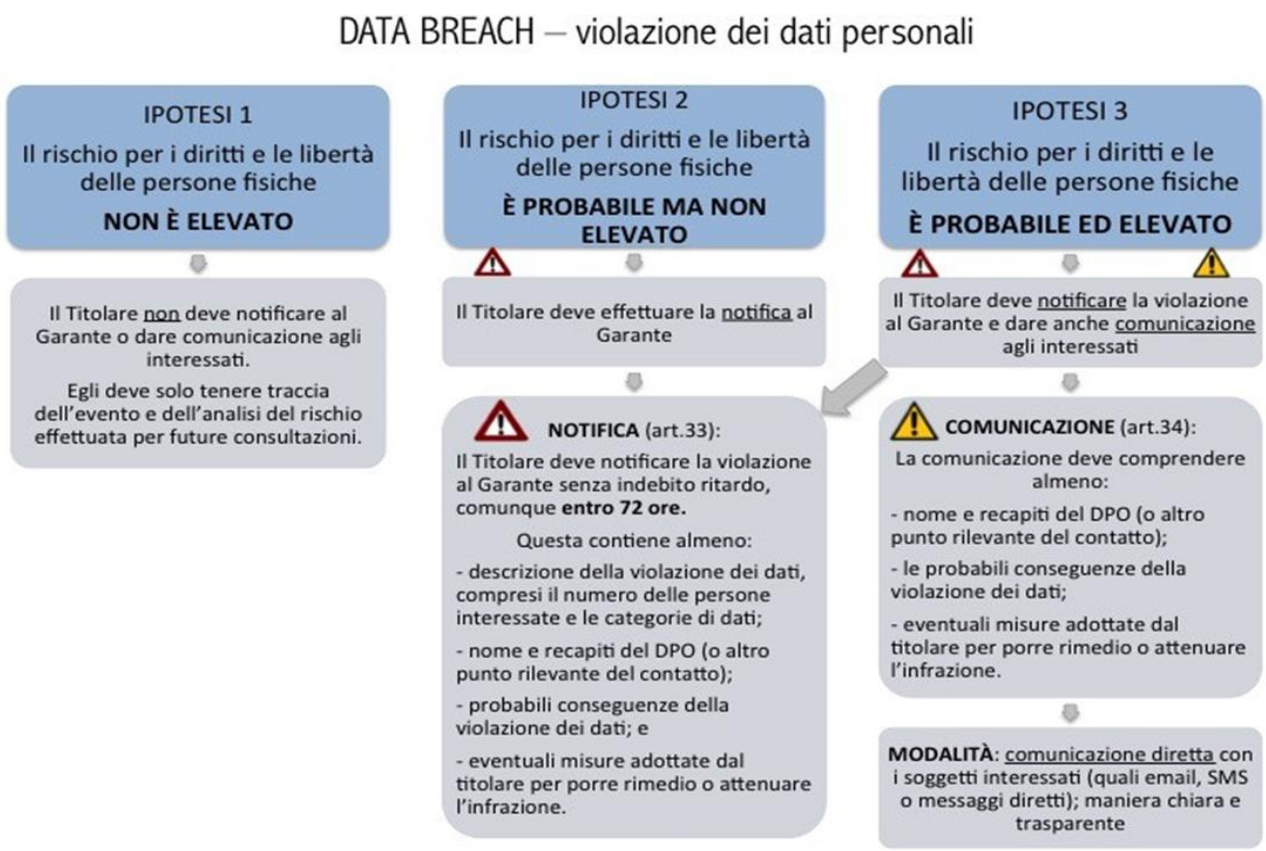
La violazione può potenzialmente avere una serie di effetti negativi significativi sulle persone, che possono provocare danni fisici, materiali o immateriali. Tali accadimenti possono comportare una perdita di controllo sui propri dati personali, una limitazione dei propri diritti, discriminazione, furto di identità o frode, perdita finanziaria, annullamento non autorizzato della pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro svantaggio economico o sociale significativo per gli individui.

Il Policlinico ha dunque l'obbligo di valutare i rischi e le libertà degli interessati ed adottare misure tecniche ed organizzative adeguate ad affrontarli.

3.5 PROCEDURA DI GESTIONE DELL'INCIDENTE DI SICUREZZA

Il presente documento individua i soggetti coinvolti, i criteri con cui effettuare le valutazioni e la procedura da seguire per la gestione degli incidenti di sicurezza e delle violazioni di dati (*data breach)*, al fine di assicurare il rispetto del principio di *accountability*.
Il Policlinico, mediante l'adozione della presente procedura, si propone di adempiere agli obblighi legali e di minimizzare il rischio di eventuali danni ai diritti, alle libertà o alla dignità degli Interessati.

La procedura prevista e regolata nel presente atto può essere graficamente rappresentata come segue:



a- SEGNALAZIONE DELL'INCIDENTE DI SICUREZZA

La segnalazione dell'incidente di sicurezza può arrivare al Policlinico in due distinti casi:

Segnalazione interna, che può essere effettuata da:

Dipendenti / Collaboratori del Policlinico / ogni altro soggetto "Delegato" o "Autorizzato" al Trattamento dei dati personali	Qualora un dipendente, collaboratore del Policlinico, o altro soggetto "Autorizzato al trattamento dei dati personali", abbia causato un possibile incidente di sicurezza oppure ne venga a conoscenza, dovrà comunicarlo immediatamente al Delegato al trattamento dei dati personali di riferimento (ossia al Direttore di U.O. / Responsabile di S.S.D.) che, laddove ritenga la sussistenza di un incidente di sicurezza, effettuerà la comunicazione dello stesso al seguente indirizzo: ufficio.privacy@hsanmartino.it. La comunicazione del Delegato al trattamento dovrà avere forma scritta e contenere la descrizione dell'evento così da rendere possibile la valutazione preliminare del rischio da parte del Gruppo di Gestione Incidenti di Sicurezza.
Ufficio Privacy / Direttore U.O. ICT / Data Protection Officer	Qualora uno di questi soggetti venga diversamente a conoscenza di un possibile incidente di sicurezza, previa eventuale acquisizione dei necessari elementi istruttori presso le strutture interessate, avrà cura di informare gli altri membri del Gruppo di Gestione Incidenti di Sicurezza per l'esame del caso.

Segnalazione esterna, che può essere effettuata da:

Responsabili del trattamento	Il Responsabile del trattamento è obbligato ad informare il Policlinico, di regola, entro 24 ore dall'avvenuta conoscenza di ogni ipotesi di incidente di sicurezza da lui causato o di cui venga direttamente a conoscenza. Questo obbligo viene attribuito al Responsabile ed agli eventuali sub

	responsabili con l'atto di nomina previsto dall'art. 28 del GDPR. La comunicazione dovrà essere scritta e riportare la descrizione dettagliata di quanto avvenuto mediante invio a: ufficio.privacy@hsanmartino.it.
Interessati o soggetti terzi	L'Interessato o un soggetto terzo possono segnalare un possibile incidente di sicurezza al Policlinico all'indirizzo: ufficio.privacy@hsanmartino.it.

b- VALUTAZIONE DELL'INCIDENTE DI SICUREZZA

Valutazione preliminare dell'evento e sua qualificazione.
Il Gruppo di Gestione Incidenti di Sicurezza è formato da:

- Ufficio Privacy
- Direttore U.O. ICT (in caso di incidenti di sicurezza aventi carattere informatico)
- D.A. / D.S. (per quanto di rispettiva competenza)

Il Gruppo, una volta ricevuta la segnalazione, esegue una **valutazione preliminare** del rischio per stabilire se l'evento sia da considerarsi irrilevante, un mero incidente di sicurezza o una vera e propria violazione dei dati personali.

Ai fini di tale valutazione dovranno essere considerate:

Natura dei dati personali oggetto di incidente	I dati appartenenti alle categorie di cui all'art. 9 presentano un rischio più alto per i diritti e le libertà degli interessati e nella valutazione devono essere presi in considerazione anche altri dati personali che potrebbero già essere disponibili dell'interessato.
Facilità di identificazione degli Interessati	La facilità con cui possono essere identificati gli interessati, in particolare se sono violati dati personali anagrafici collegati a dati particolari in chiaro
Categorie e numero di Interessati a cui si riferiscono i dati personali	Il caso in cui la violazione riguardi dati personali relativi a minori o altre persone particolarmente vulnerabili, che potrebbero essere a rischio di pericolo.
Tipologie di violazione e numero approssimativo di registrazioni dei dati personali	Una violazione può comportare la semplice conoscenza del dato, la sua alterazione o distruzione e può essere anche reiterata più volte nel tempo.
Tipologia e conseguenze negative della violazione dei dati personali	Il caso in cui la violazione potrebbe comportare furto di identità o frode, danni fisici, disagio psicologico, umiliazione o danno alla reputazione.
Portata dell'incidente di sicurezza	La probabilità che la violazione incida sui diritti e libertà degli Interessati
Data e luogo dell'incidente di sicurezza	La data e il luogo influiscono nella valutazione dell'evento in quanto l'accessibilità del luogo e il momento possono diminuire o aumentare sensibilmente la probabilità che i dispositivi o supporti vengano trovati da soggetti non autorizzati.
Misure preliminari di gestione del rischio	L'efficacia delle misure adottate dopo l'evento idonee a ridurre la probabilità che si verifichi un danno ai diritti, libertà o dignità dell'Interessato.

Una volta completato l'esame sommario dell'evento, e comunque non oltre le 24 ore dalla ricezione della segnalazione, il gruppo di lavoro dovrà stabilire se l'evento segnalato sia da qualificarsi come evento irrilevante, incidente di sicurezza o violazione dei dati personali, compilando l'apposita scheda di rilevazione dell'evento critico (cfr. par. 5).

Nel caso in cui l'evento sia ritenuto irrilevante verrà immediatamente annotato dall'Ufficio Privacy nel registro degli incidenti di sicurezza all'interno dell'apposita sezione falsi positivi, senza ulteriori comunicazioni o notifiche ma indicando l'ora, la data e il numero identificativo della scheda di valutazione del rischio**.**

Viceversa, ove l'evento sia valutato come incidente di sicurezza oppure come violazione dei dati personali, dovrà essere portato tempestivamente a conoscenza del Titolare del trattamento secondo le modalità di cui alla successiva lettera c.

Analisi delle possibili conseguenze lesive di una violazione di dati personali.
Le conseguenze negative che possono derivare da una violazione dei dati personali possono consistere, a norma dell'articolo 4 del GDPR, in danni ai diritti, alle libertà e alla dignità dell'Interessato.

A titolo meramente esemplificativo, da una violazione di dati personali può conseguire:

Lesione di diritti o libertà personali	Perdita della riservatezza, furto o usurpazione dell'identità, perdita di dati personali non riproducibili quali quelli genetici o biometrici, commissione di reati contro l'integrità fisica, divulgazione di dati coperti da segreto professionale e in generale danni fisici, morali o all'immagine professionale
Lesione di diritti patrimoniali	Reati contro il patrimonio dell'Interessato resi possibili dall'illecito utilizzo dei dati personali come per esempio furti o estorsioni anche tramite sistemi informatici, danneggiamento o perdita della possibilità di uso di dispositivi software di uso personale
Lesione della dignità	Discriminazione o pregiudizio alla reputazione personale o patrimoniale

Il Gruppo di Gestione Incidenti di Sicurezza, valutando il rischio, dovrà innanzitutto identificare di che tipo sono i diritti o le libertà messi in pericolo dalla violazione.

Analisi della probabilità del verificarsi della conseguenza lesiva.
Una volta valutata la tipologia di evento e la sua gravità, dovrà essere valutata la probabilità che la conseguenza dannosa si verifichi; questa ultima valutazione dovrà tener conto di:

Luogo e circostanze dell'evento	Luogo accessibile / inaccessibile, numero di persone a conoscenza della condizione di vulnerabilità dei dati
Data e orario dell'evento	Per accertare e valutare fatti verificatisi tra il momento della violazione e quello della valutazione di probabilità che possono influenzare la probabilità che si verifichino conseguenze negative (es. distruzione del supporto di cancellazione dei dati con sistemi di sicurezza a distanza o inseriti nel dispositivo ecc.)
Efficacia delle misure tese a contenere il danno nell'immediato	Per verificare se esiste la possibilità di eliminare la visibilità di dati diffusi in web, attivazione immediata di sistemi di recupero dei dati perduti o cancellati ecc.

In caso di dubbio nella valutazione dell'evento il Gruppo di Gestione può richiedere parere al DPO.

c- COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO

Nel caso in cui il Gruppo di Gestione Incidenti di Sicurezza valuti l'evento segnalato come incidente sulla sicurezza o violazione dei dati personali, l'Ufficio Privacy dovrà comunicare per iscritto al Titolare l'accaduto riportandone una sintesi, il risultato della valutazione, la menzione dei pareri espressi dal Gruppo di Gestione Incidenti di Sicurezza, allegando la scheda di rilevazione dell'evento critico (compilata a cura dell'Ufficio Privacy con il supporto del Gruppo di Gestione Incidenti di Sicurezza).

Alla comunicazione dovrà quindi essere allegata la predetta scheda per rendere edotto il Titolare di tutti gli elementi utili alla descrizione e alla portata dell'evento; la predetta scheda dovrà infine essere sottoscritta dal Titolare.
Quest'ultimo ha comunque facoltà di chiedere ulteriori pareri e valutazioni al DPO.

Dal momento in cui il Titolare è messo a conoscenza della violazione di dati / *data breach*, inizia a decorrere il termine di 72 h previsto dall'art. 33 del GDPR entro cui effettuare le notifiche all'Autorità Garante Privacy.

3.6 ADOZIONE DELLE MISURE PRELIMINARI DI CONTENIMENTO DEL RISCHIO

La conoscenza dell'evento di incidente di sicurezza o violazione dei dati personali comporta la necessità per il Policlinico di adottare qualsiasi misura idonea a ridurre la probabilità che dall'evento derivi una conseguenza lesiva dannosa per gli Interessati o, comunque a ridurre il più possibile l'aggravarsi di tali conseguenze.
Le misure suddette, da determinare di volta in volta in base alle concrete esigenze di protezione, dovranno essere **attuate** e **coordinate** da:

Violazione che coinvolge le risorse software e hardware	Direttore ICT (con supporto Ufficio Privacy)
Violazione non informatica	D.A. / D.S. (con supporto Ufficio Privacy)

3.7 NOTIFICA ALL'AUTORITA' GARANTE PRIVACY

Obblighi di notifica
Il Titolare è tenuto, ricevuta la comunicazione con la scheda di rilevazione dell'evento, a decidere, entro 72 ore dal momento della conoscenza della violazione o dell'incidente di sicurezza se, in base all'art. 33 del GDPR, notificare l'evento all'Autorità Garante Privacy ed eventualmente comunicarlo agli Interessati.
Per effettuare la notifica all'Autorità Garante Privacy il Titolare si avvale della collaborazione del DPO e del Gruppo di Gestione Incidenti di Sicurezza.

Casi di esclusione della notifica all'Autorità Garante Privacy
La notifica all'Autorità Garante Privacy è obbligatoria nel caso in cui l'evento integri una violazione dei dati personali ai sensi dell'articolo 33, paragrafo 1 del GDPR.
La stessa non è necessaria qualora l'evento, ancorché possa astrattamente configurare un danno all'Interessato, abbia generato un rischio talmente basso da risultare irrilevante oppure integri solo un'ipotesi di incidente di sicurezza.

Notifica tardiva, cumulativa e per fasi
L'articolo 33, par. 1, chiarisce che, qualora la notifica all'Autorità Garante Privacy non sia effettuata entro 72 ore dall'avvenuta conoscenza dell'evento, questa deve essere corredata dei motivi del ritardo.
Tale caso si può avere, ad esempio, nel caso delle cosiddette violazioni "cumulative", violazioni multiple riconducibili alla stessa tipologia (ad esempio molteplici attacchi informatici provenienti da un'unica fonte che colpiscono gli stessi applicativi) e che riguardano lo stesso tipo di dati personali di numerosi Interessati. In tali casi la scelta più opportuna in termini di tempo e di efficacia è quella di eseguire una sola notifica nella quale si segnalano tutte le violazioni.
Un secondo esempio si ha quando si rende necessaria una notifica per fasi, come nel caso in cui la stessa derivi da un evento di cui risulta complessa la valutazione e sia difficile stabilire precisamente i tipi e la portata delle possibili conseguenze negative, nel cui caso si potrebbe rendere necessario un supplemento di analisi. In tale ipotesi le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Nel caso di notifica per fasi, il Policlinico dovrà inizialmente procedere ad una prima notifica all'Autorità Garante nella quale verranno indicati i motivi del ritardo, illustrando le ragioni per cui non dispone ancora di tutte le informazioni richieste, le azioni di indagine che intende adottare e l'impegno a fornire nel minor tempo possibile gli ulteriori dettagli.

3.8 COMUNICAZIONE ALL'INTERESSATO

Scopo e presupposti della comunicazione all'Interessato

Lo scopo principale della comunicazione agli Interessati ai sensi dell'art. 34 GDPR consiste nel fornire loro una tempestiva conoscenza della violazione e le informazioni sulle misure che possono prendere per proteggere i propri dati evitando le conseguenze negative della violazione.

La comunicazione all'Interessato può essere effettuata utilizzando l'apposito modulo di comunicazione (cfr. par. 5):

- senza ingiustificato ritardo, quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- in un momento successivo, qualora vi siano i presupposti per una notifica tardiva oppure cumulativa;
- successivamente alla notifica della violazione all'Autorità Garante Privacy nel caso in cui quest'ultima ne ravvisi la necessità e imponga al Policlinico di adempiervi.

Contenuto della comunicazione all'Interessato

La comunicazione all'Interessato deve contenere almeno le seguenti informazioni descritte con un linguaggio semplice e chiaro:

A	La descrizione della natura della violazione
B	Il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto
C	La descrizione delle probabili conseguenze della violazione
D	La descrizione delle misure adottate o di cui si propone l'adozione da parte del Policlinico per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi; a tal proposito, il Policlinico può anche riportare all'Interessato le indicazioni che ha ricevuto dal Garante in merito alla gestione della violazione.

Criteri per predisporre la comunicazione all'Interessato

Nel valutare le modalità più opportune per effettuare la comunicazione agli interessati il Policlinico, avvalendosi della collaborazione del DPO, si attiene ai seguenti criteri:

- scegliere la forma più adatta: la comunicazione di violazione dei dati personali deve consistere in un messaggio dedicato, (no messaggi standard o contenuti in newsletter periodiche, ecc…). L'oggetto della notifica deve riportare in modo chiaro e immediato che la comunicazione riguarda una violazione dei dati personali, con l'indicazione della norma di riferimento (art. 34 del GDPR).
  Nel caso in cui la violazione dei dati personali riguardi un grande numero di interessati e richieda uno sforzo o dei costi non sostenibili, il Policlinico procederà ad una comunicazione pubblica o comunque una comunicazione in grado di raggiungere in modo efficace i destinatari.
- predisporre con chiarezza il testo della comunicazione: la comunicazione deve essere eseguita nella lingua comprensibile dall'Interessato a prescindere da quella ufficiale nello Stato dove questi risiede.
  La comunicazione elettronica e gli eventuali allegati devono essere trasmessi in un formato facilmente leggibile (es. PDF, PDF compilabile) indicando inoltre all'Interessato di segnalare tempestivamente l'impossibilità di visualizzare o compilare il file.
- indicare le possibili precauzioni che l'interessato può adottare, informandolo della possibilità di ottenere dallo stesso Policlinico chiarimenti specifici in merito alla violazione occorsa.

Circostanze nelle quali non è richiesta la comunicazione all'Interessato

La comunicazione agli Interessati non sarà effettuata qualora la valutazione dell'evento compiuta dal Gruppo di Gestione Incidenti di Sicurezza evidenzi l'esistenza di fattori che ne diminuiscono la pericolosità al punto tale che risulterebbe superfluo comunicare l'evento agli Interessati.

Le cause di esclusione del dovere di comunicazione all'Interessato previste dalle Linee Guida europee sono:

A	Applicazione ai dati personali oggetto della violazione di preventive misure tecniche e organizzative adeguate a proteggere i dati che li rendono incomprensibili a chiunque non sia

	autorizzato ad accedervi, ad esempio qualora i dati personali siano sottoposti a cifratura rispetto alla quale la riservatezza della chiave rimane intatta in quanto è stata generata in maniera tale da non poter essere individuata con i mezzi tecnici disponibili da qualcuno che non è autorizzato ad accedervi.
B	Immediata adozione, a seguito della violazione, di misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche, ad esempio se il Policlinico individua il soggetto che ha avuto accesso ai dati personali e intraprende un'azione idonea a impedire qualsiasi tipo di utilizzazione.
C	Sforzo sproporzionato per effettuare la comunicazione *ad personam*: ciò può accadere ad esempio nel caso in cui i dati con cui contattare l'Interessato siano stati persi a causa della violazione stessa oppure non siano mai stati noti. In tali circostanze il Policlinico deve invece effettuare una comunicazione pubblica o una misura analoga, tramite la quale gli Interessati vengano informati in maniera altrettanto efficace.

Nel caso in cui il Policlinico ritenga sussistente una delle suddette clausole di esclusione e conseguentemente non effettui la comunicazione agli Interessati, dovrà comunque comunicarla all'Autorità Garante, fatta salva la ricorrenza di una delle relative cause di esclusione.

Nel caso in cui la situazione relativa all'evento evolva nel corso del tempo, si procederà ad una rivalutazione del rischio per i diritti e le libertà delle persone fisiche con possibilità di riconsiderare la decisione adottata relativamente alle modalità di comunicazione ai soggetti interessati.

3.9 ANNOTAZIONE NEL REGISTRO DEGLI INCIDENTI DI SICUREZZA

Nel rispetto del principio di *accountability,* il Policlinico ha predisposto un apposito Registro di tutti gli incidenti di sicurezza, sul quale annotare ogni singolo evento che possa comportare anche in ipotesi una violazione di dati personali, che sarà tenuto costantemente aggiornato, compresi gli eventi che, successivamente alla valutazione preliminare, sono qualificati come irrilevanti oppure come incidenti di sicurezza a basso rischio che non obbligano ad eseguire nessun tipo di notifica o comunicazione.

Il Registro degli Incidenti di Sicurezza, la cui tenuta e aggiornamento è affidata all'Ufficio Privacy, può raccogliere le seguenti informazioni:

A	Data e ora dell'evento
B	Tipo di evento
C	Sistemi fisici o informatici eventualmente coinvolti che hanno presentato criticità
D	Data, ora, mezzo della segnalazione e soggetto che la esegue
E	Data ora ed esito della valutazione preliminare
F	Qualificazione dell'evento come falso positivo, incidente di sicurezza o violazione dei dati personali
G	Misure preventive di contenimento o esclusione della pericolosità
H	Data, ora in cui viene effettuata la notificazione all'autorità Garante Privacy
I	Specificazione della natura della notifica all'autorità Garante Privacy (completa, per fasi o cumulativa)
L	Eventuale comunicazione agli Interessati e modalità con cui viene effettuata
M	Misure adottate per prevenire ulteriori violazioni dello stesso tipo (misure disciplinari o implementazione delle misure tecniche e organizzative)

3.10 IMPLEMENTAZIONE DELLE MISURE DI SICUREZZA

A seguito della gestione di un incidente di sicurezza, il Policlinico è tenuto a migliorare il proprio sistema di protezione dei dati personali - anche avvalendosi del Registro degli Incidenti di Sicurezza e considerando la tipologia di incidente o violazione, l'efficacia delle azioni di prevenzione e gestione, le indicazioni fornite o le misure correttive imposte dall'Autorità Garante Privacy - secondo la seguente traccia:

1	Adozione di misure tecniche informatiche dirette al miglioramento degli applicativi utilizzati dal Policlinico tramite aggiornamento di quelli già in uso, sostituzione di sistemi obsoleti rafforzamento delle modalità di accesso
2	Adozione di misure tecniche analogiche che aumentino la sicurezza dei dati inseriti in supporti cartacei come l'utilizzo di schedari dotati di chiavi, eliminazione dei riferimenti personali dalle cartelle o dai fascicoli cartacei o misure che impediscano l'accesso agli archivi
3	Miglioramento della valutazione, in fase di acquisto, degli applicativi e più generale di tutti i dispositivi informatici che trattano dati personali così da ottenere beni e servizi più adeguati a proteggere i dati personali degli Interessati
4	Formazione periodica e specifica degli operatori del Policlinico
5	Predisposizione di istruzioni operative per dipendenti e collaboratori del Policlinico
6	Responsabilizzazione dei Delegati al trattamento affinché sorveglino con maggiore attenzione l'osservanza delle misure tecniche e organizzative per la protezione dei dati personali all'interno della Struttura di competenza
7	Adozione di sanzioni disciplinari a dipendenti e collaboratori che non hanno rispettato le indicazioni operative fornite dal Policlinico rendendosi responsabili del verificarsi l'evento critico.

4 ESEMPI DI VIOLAZIONE CON RELATIVI OBBLIGHI DI NOTIFICA E COMUNICAZIONE

(estratto da Linee Guida "WP250rev.01" elaborate dal WP29).

Al fine di chiarire quanto finora detto può essere utile illustrare una casistica di eventi che integrano una violazione dei dati personali e fornire indicazioni circa la necessità di notificare l'evento all'Autorità Garante Privacy oppure comunicarlo all'Interessato.
È bene chiarire comunque che i seguenti esempi, data la molteplicità di casi che nel concreto possono verificarsi, non devono ritenersi né esaustivi né da seguire rigidamente in quanto la valutazione dell'evento, della gravità delle sue conseguenze e della probabilità che queste si verifichino deve sempre essere fatta alla luce degli elementi e delle circostanze verificatisi in concreto.

ESEMPIO	NOTIFICA ALL'AUTORITÀ GARANTE PRIVACY	COMUNICAZIONE ALL'INTERESSATO	RACCOMANDAZIONI
A - Il Titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati contenuti in una chiave USB, successivamente dispersa o rubata.	**No**	**No**	Finché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
B- Il Titolare del trattamento gestisce un servizio online oggetto di un attacco informatico a seguito del quale, i dati	**Sì**. Segnalare l'evento all'Autorità di controllo se vi sono probabili conseguenze per le	**Si**. Segnalare l'evento alle persone fisiche qualora si tratti di dati di natura sensibile. In altri casi	

personali vengono prelevati illecitamente	persone fisiche	valutare se il data breach comporta comunque pericolo di grave pregiudizio per l'Interessato.	
C- Una breve interruzione di corrente di alcuni minuti impedisce agli utenti di contattare il Titolare del trattamento ed esercitare il diritto di accesso ai propri dati personali.	**No**.	**No**.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il Titolare del trattamento deve conservare adeguate registrazioni in merito.
D- Un Titolare del trattamento subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati.	**Sì.** Effettuare la segnalazione all'Autorità Garante Privacy, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità dei dati personali.	**Sì.** Effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario notificare o comunicare la violazione in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'Autorità Garante Privacy fosse comunque venuta a conoscenza dell'incidente, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
E- Una persona segnala al Titolare di aver ricevuto documentazione relativa a un soggetto diverso. Il Titolare del trattamento intraprende una breve indagine da cui risulta che la violazione dipende da una potenziale carenza	**Sì.**	**Si**. Ma la comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'Autorità Garante Privacy, e il Titolare del trattamento deve informare le altre

sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.			persone fisiche interessate se sussiste un rischio elevato per loro.
F- una *software house* che fornisce servizi al Titolare subisce un attacco informatico a seguito del quale vengono pubblicati online le credenziali degli utenti per l'accesso ad aree riservate del sito web del TITOLARE contenenti dati personali, gestite da tale ditta fornitrice.	**Si**. In veste di Responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che dalla comunicazione del Responsabile emerga con certezza che sussiste violazione dei dati personali il Titolare sarà considerato a conoscenza del data breach nel momento in cui riceve la comunicazione. Il Titolare del trattamento deve quindi effettuare la notifica all'Autorità Garante Privacy entro 72 ore da quel momento.	**Sì**. Poiché la violazione potrebbe comportare un rischio elevato.	Il Titolare del trattamento dovrebbe adottare delle misure di protezione come ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio quali la cancellazione o quanto meno l'individuazione dei dati eventualmente diffusi online.
G – La documentazione relativa alle ispezioni è indisponibile per un periodo di 30 ore a causa di un attacco informatico.	**Sì.** Il Titolare è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la tutela della vita privata degli interessati.	**Sì**. Il Titolare è tenuto a informare le persone fisiche coinvolte.	
H- I dati personali di un gran numero di utenti o dipendenti/collaboratori del Titolare vengono inviati per errore a una mailing list sbagliata con più di mille destinatari, oppure vengono inseriti per errore indirizzi mail personali nei campi "a:" oppure "cc." Così che ogni destinatario può vedere l'indirizzo mail degli altri.	**Sì**. Segnalare l'evento all'Autorità Garante Privacy se è interessato un numero elevato di persone se vengono rivelati dati sensibili (ad esempio una mailing list) o se altri fattori presentano rischi elevati (ad esempio, il messaggio contiene password oppure dati bancari).	**Sì**. Segnalare l'evento alle persone fisiche coinvolte, in particolare qualora nella comunicazione siano presenti dati giudiziari o di salute.	

5 MODULISTICA AZIENDALE CORRELATA ALLA PROCEDURA

- SCHEDA DI RILEVAZIONE EVENTO CRITICO DI SICUREZZA (MODAZHAG_0005PRIVACY)

- SCHEMA DI COMUNICAZIONE ALL'INTERESSATO DI UNA VIOLAZIONE DI DATI PERSONALI (MODAZHAG_0006PRIVACY)

6 NORMATIVA E DOCUMENTI DI RIFERIMENTO

- Regolamento UE 2016/679 "Regolamento Generale sulla Protezione dei Dati" (GDPR);
- D. Lgs. n. 196/2003 "Codice per la protezione dei dati personali";
- Linee Guida adottate dal "Gruppo di lavoro Art. 29 (WP29)**"** in materia di notifica delle violazioni di dati personali (*data breach notification*) – WP250;
- Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione di dati, adottate il 14 dicembre 2021;
- D. Lgs. 82/2005 "Codice dell'Amministrazione Digitale" (CAD).