TITOLO

Procedura di Gestione delle Violazioni di dati Personali (Data Breach)

Stesura		
Struttura	Nome Cognome	Qualifica
S.S. S.A.A.S.	Patrizia Melchionne	Collaboratore Amministrativo Professionale Esperto

Validazione		**Emissione**	
Struttura	S.A.A.S.	Struttura	Direzione Generale
Dott.ssa Donatella Baravalle	*Firmato in originale* Data 22/12/2020	Dr. Claudio Baccon	*Firmato in originale* Data: 23/12/2020
Struttura	Tecnico- Ingegneria Clinica - Sistemi Informativi Informatici Responsabile per la transizione al digitale	Struttura	Direzione Sanitaria
Dott. ssa Marina Marzuoli	*Firmato in originale* Data: 18/12/2020	Dr. Roberto Arione	*Firmato in originale* Data: 23/12/2020
Struttura	Risk Management-Qualità	Struttura	Direzione Amministrativa
Dott.ssa Caterina Mineccia	*Firmato in originale* Data: 18/12/2020	Dott.ssa Rita Benedetta Venezia	*Firmato in originale* Data: 23/12/2020

Stato Aggiornamento

Revisione	Data	Paragrafi modificati / Note	Modificatori / Struttura

Lista di distribuzione

Struttura	Destinatario
Tutte le Strutture	Tutto il personale
Contitolari del Trattamento	
Responsabili del Trattamento	

In accordo con il principio di responsabilizzazione, di cui all'art. 5 e 24 del GDPR, la diffusione della presente procedura viene assicurata attraverso:
- la pubblicazione sulla Intranet Aziendale nella sezione Privacy;
- trasmissione ai Direttori/Dirigenti della Strutture Aziendali e, e per il loro tramite al personale in esse operante per informarlo es istruirlo in merito alle azioni da porre in essere nel caso di violazioni;
- trasmissione ai Contitolari/Responsabili del trattamento.

INDICE DEL DOCUMENTO

1. PREMESSA

Una violazione dei dati personali (di seguito *"data breach"*) può scaturire sia dall'interno che dall'esterno dell'Azienda e, qualora non affrontata tempestivamente e in maniera adeguata, può comportare pericoli significativi per la privacy degli interessati cui i dati si riferiscono (es. discriminazioni, furti di identità, perdite economiche, pregiudizi alla reputazione, etc).

Le violazioni della privacy più comuni sono quelle derivanti dall'errore umano. Basti pensare alla consegna o alla comunicazione di documenti contenenti dati particolari alla persona sbagliata (es. referto del paziente Caio nella cartella del paziente Tizio; invio documentazione sanitaria a persona sbagliata, furto/smarrimento di agende, documentazione clinica, etc.).

I possibili scenari di violazione dei dati sono sicuramente aumentati con l'avvento della società digitale. Gli operatori devono, pertanto, **sviluppare la capacità di riconoscere ed affrontare le potenziali conseguenze** -ad esempio sulle cure di un paziente- di eventi pregiudizievoli quali un accesso non autorizzato (hackeraggio o cessione di credenziali, furto di agende/fogli contenenti password), una modifica erronea di un database, un malfunzionamento di uno strumento informatico o il furto o perdita di un dispositivo (smartphone o chiavetta USB, telefonino aziendale) contenente dati di estrema delicatezza (dati sullo stato di salute), o la comunicazione di dati attraverso strumenti a larga diffusione (invio massivo di email o pubblicazione dati sul web).

2. SCOPO

La predisposizione della presente procedura consente di:

- definire i ruoli e le responsabilità organizzative per la gestione di un data breach;
- fornire **indicazioni pratiche e modalità operative per riconoscere e gestire situazioni relative a violazioni di dati al fine di minimizzarne l'impatto e prevenirne la reiterazione** a chi a diverso titolo tratta dati all'interno dell'Azienda Ospedaliera Universitaria San Luigi Gonzaga di Orbassano (di seguito ber brevità "Azienda"), nonché a chi tratta dati per conto dell'Azienda (Responsabili del Trattamento)**;**
- fornire l'opportuna modulistica.

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata osservanza di quanto in essa previsto potrà comportare, rispettivamente a carico dei dipendenti, collaboratori a

vario titolo (specializzandi, tirocinanti, sumaisti, borsisti, ect) e fornitori l'adozione di provvedimenti disciplinari- ovvero giusta causa di risoluzione dei contratti in essere.

3.CAMPO DI APPLICAZIONE

La presente procedura deve essere applicata in tutti i casi in cui si verifichi un potenziale, ma attuale, rischio di **perdita, distruzione o diffusione indebita** di dati personali (ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi che possono determinare pericoli significativi per la protezione dei dati degli interessati).

4. DESTINATARI E RESPONSABILITA'

La presente procedura si applica a tutto il personale delle Strutture dell'Azienda che, a qualsiasi titolo (dipendenti, universitari, borsisti, tirocinanti,..) e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea), trattanodati all'interno dell'Azienda, nonché ai Responsabili che trattano i dati per conto dell'Azienda.

5. GLOSSARIO E ABBREVIAZIONI

Terminologia, Abbreviazione	Definizione
G.D.P.R.	Regolamento (UE) 2016/679 del Parlamento Europeo 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), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento)
AGID	Agenzia per l'Italia Digitale
NIS	Network and Information Security
WP29	Working Party Art. 29 - Gruppo di lavoro Art. 29 - dal 25/05/2018 EDPB (European Data Protection Board – Comitato Europeo per la Protezione dei Dati)
TITOLARE DEL TRATTAMENTO	L'Autorità Pubblica (AOU San Luigi Gonzaga di Orbassano) che singolarmente o insieme ad altri, determina la finalità e i mezzi del trattamento dei dati personali
CONTITOLARE	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali;

RPD (o DPO)	Responsabile della Protezione dei Dati (o Data Protection Officer):la persona individuata dal Titolare del Trattamento dei dati quale responsabile della protezione dei dati all'interno dell'Azienda che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.
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
SUB RESPONSABILE	La persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento
TRATTAMENTO DEI DATI	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);
INTERESSATO	Persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
SOGGETTO DESIGNATO	I Direttori di Struttura Complessa, i dirigenti responsabili.
AUTORIZZATO	Per 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. 4.10 GDPR
REFERENTE PRIVACY	Persona individuata all'interno delle Strutture con il compito di collaborare con il Gruppo Aziendale Privacy nel processo di analisi dei trattamenti e valutazione dei rischi.
COMMISSIONE AZIENDALE PRIVACY	Gruppo di lavoro multidisciplinare istituto con deliberazione n.555 del 9.11.2017 e successive modifiche ....
GRUPPO DI GESTIONE DATA BREACH	Gruppo di lavoro muldisciplinare per la gestione degli incidenti di sicurezza che possano comportare la violazione dei diritti e delle libertà fondamentali delle persone fisiche
INCIDENTE DI SICUREZZA	Evento singolo o una serie di eventi di sicurezza non voluti o inaspettati che hanno una significativa probabilità di compromettere il funzionamento di processi aziendali e di minacciare la sicurezza informativa (ISO 27000)

6. RIFERIMENTI NORMATIVI

- Regolamento (UE) 2016/679 del Parlamento Europeo 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), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento);
- D.Lgs. 196/2003 Codice per la protezione dei dati personali;
- Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679;
- Decreto Legislativo 10 agosto 2018 n, 101 "*Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del 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)*";
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015, come modificata Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951];
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951];
- D.Lgs. 82/2005 Codice dell'Amministrazione Digitale (CAD);
- Artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale);
- Decreto 9 gennaio 2008 del ministero degli interni in attuazione della Legge 155/2005 sulle infrastrutture critiche;
- Direttiva (UE) 2016/1148 (Direttiva NIS) del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea;
- Prescrizione del WP29 "Guidelines on Personal data breach notification under Regolation 2016/679, adottate il 03.10.2017 (ultima revision 06/02/2018);
- D. Lgs. 65/2018, "Attuazione delle Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informatici nell'Unione";
- Circolare 18.04.2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le Pubblice Amministrazioni (Direttiva del PCM 01.08.2015, pubblicata in G.U. Serie Generale n. 103 del 05.05.2017).

7. MODALITA' OPERATIVE

7.1. Definizione Data Breach

Un data breach è, secondo la definizione fornita dall'art. 4 par. 12 del Regolamento Generale sulla Protezione dei Dati (di seguito "GDPR"), **un incidente di sicurezza** che comporta a**ccidentalmente** 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.

Le violazioni, secondo le indicazioni fornite dal Gruppo di Lavoro art. 29, possono manifestarsi in diversi modi ed essere classificate in tre tipologie:

Tipologia di violazione	Evento/Minaccia
Violazione della riservatezza	Accesso o trattamento non autorizzato o illecito
	Divulgazione non autorizzata
Violazione dell'integrità	Modifica non autorizzata o accidentale
Violazione della disponibilità	Perdita o distruzione accidentale o illegale
	Indisponibilità temporanea o prolungata

A seconda dei casi, una violazione può riguardare contemporaneamente la **riservatezza, l'integrità e la disponibilità dei dati personali**, nonché qualsiasi combinazione delle stesse.

L'articolo 32 del "GDPR" dispone che il Titolare del trattamento, nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, deve tenere conto, tra le altre cose*, "della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".*

In caso di violazione dei dati personali, il Titolare del Trattamento deve, ex art. 33 del GDPR, notificare all'autorità di controllo (Garante) la violazione senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Ne deriva che la notifica dell'avvenuta violazione al Garante non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati. Se la probabilità del rischio è elevata, dovranno essere informati anche gli interessati.

Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è pertanto **la probabilità che l'incidente di sicurezza possa porre a rischio** (per la notifica all'Autorità), o ad **elevato rischio** (per la comunicazione agli interessati) le libertà e i diritti degli individui.

Di conseguenza un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione da notificare al Garante e comunicare agli interessati **solo qualora la mancanza di accesso alle informazioni può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche**. Non configura invece una "violazione della sicurezza" l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata se accompagnata da opportune misure organizzative tese a salvaguardare i diritti e le libertà fondamentali.
Il Titolare ha il dovere di notificare al Garante nei seguenti casi:

a. l'organizzazione è Titolare del/i trattamento/i dei dati coinvolti nell'incidente
b. l'organizzazione è Contitolare del trattamento con delega alla notifica
c. l'organizzazione è Responsabile del trattamento con delega alla notifica.

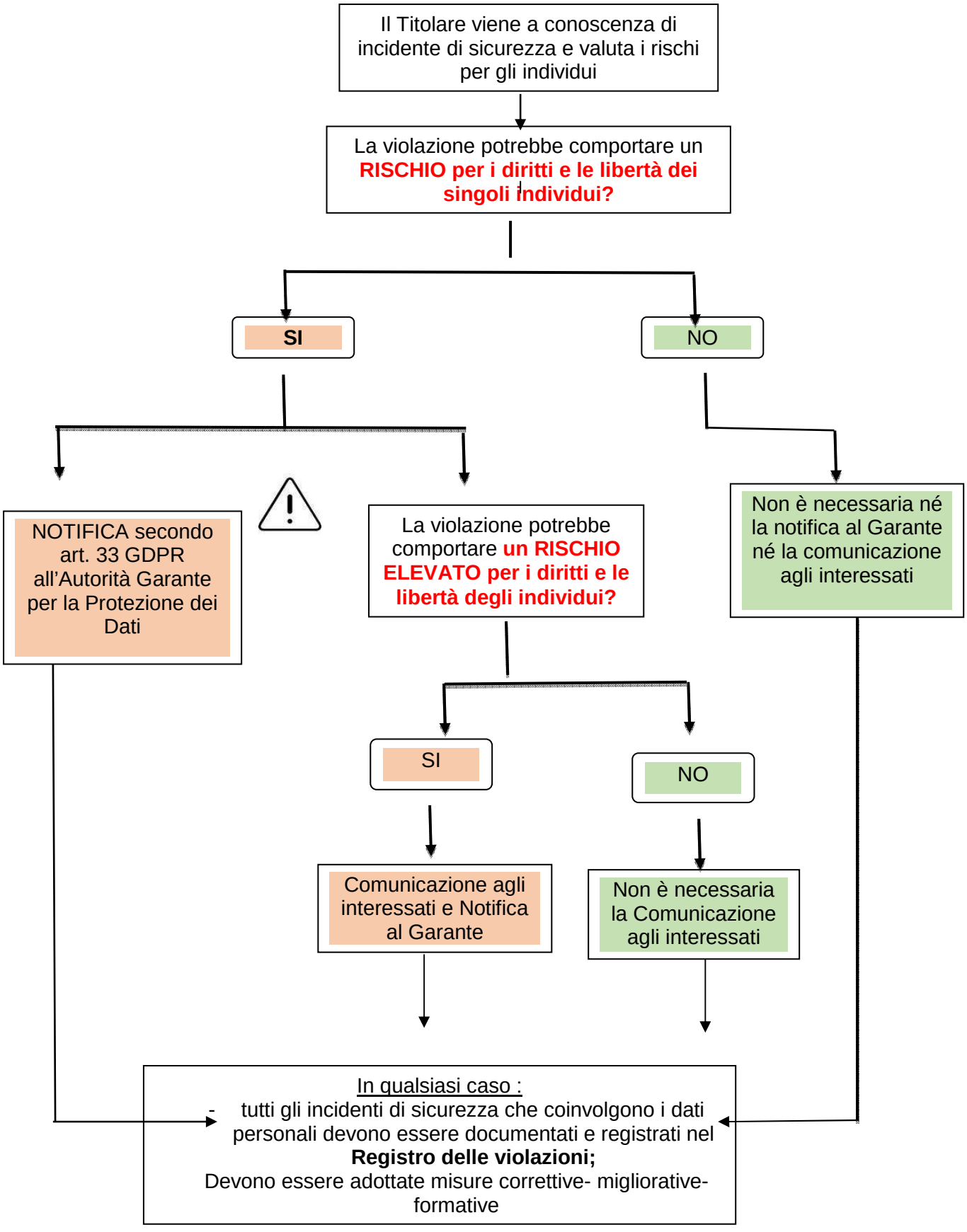
Gli incidenti di sicurezza occorsi, anche se non notificati al Garante e non comunicati agli interessati, nonché l'indicazione delle circostanze e conseguenze in cui la violazione si è verificata ed i provvedimenti adottati in merito, dovranno essere comunque **sempre annotati e documentati sul registro delle violazioni.**

7.2. Fasi del Processo di Gestione del Data Breach

Il processo di gestione di una violazione concreta, potenziale o sospetta dei dati si articola nelle seguenti fasi:

0	Predisposizione strumenti
1	Rilevazione dell'Evento- Acquisizione Notizia dell'avvenuto incidente.
2	Analisi preliminare e invio segnalazione.
3	Gestione (contenimento del danno) e valutazione gravità dell'evento.
4	Notifica al Garante Privacy
5	Altre segnalazioni dovute: es. agli organi di Polizia e, nel caso di incidente informatico, a CERT-PA, all'autorità NIS competente
6	Comunicazione agli interessati, ove necessario, e raccolta riscontro dell'avvenuta comunicazione.
7	Inserimento dell'evento nel Registro delle Violazioni (Comprese le violazioni che non richiedono la notifica).
8	Azioni correttive specifiche e per analogia.

Allo scopo di supportare i soggetti coinvolti nel caso di *"Incidente di* Sicurezza", sono state esplicitate schematicamente sopra le fasi del processo di gestione del rischio e di seguito il flusso delle azioni da adottare per discriminare le violazioni da notificare al Garante e da comunicare agli interessati dagli altri incidenti.



7.3 Predisposizione degli strumenti

Questa fase può essere definita come **"Fase 0"** in quanto diretta a garantire la sicurezza dei dati attraverso l'adozione di comportamenti e di misure tecniche per **prevenire e/o ridurre il rischio di incidenti di sicurezza e/o gli effetti degli stessi**.

In primo luogo la sicurezza del dato è garantita dalla rigorosa applicazione dei principi previsti all'art. 5 del GDPR (principi applicabili al trattamento dei dati) ed in particolare , esemplificando, da:

- principio di minimizzazione: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- periodo di conservazione dei dati: es. conservare i dati per il periodo strettamente necessario per il conseguimento delle finalità per cui sono stati raccolti;
- pertinenza delle informazioni gestite rispetto alle finalità;
- numero di soggetti autorizzati al trattamento;
- autorizzazione dei singoli al trattamento al trattamento e alle relative procedure.;
- l'applicazione dei principi di Privacy by design.

Tra le misure tecniche ed organizzative da predisporre rientrano:

- le azioni di sensibilizzazione e formazione del personale;
- i sensori tecnici per individuare intrusioni di rete (SIEM, SOC);
- gli strumenti di supporto alla procedura in oggetto (es. gestione con canali di comunicazione in caso di blocco informatico);
- la predisposizione di questa procedura;
- la predisposizione di procedure sulla continuità operativa;
- la corretta allocazione di risorse umane anche in regime di reperibilità;
- gli audit periodici sui trattamenti e sul sistema informativo;
- gli interventi di digitalizzazione dei processi previsto dal CAD nel quadro delle misure tecniche previste.

7.4 Rilevazione dell'evento- Acquisizione Notizia dell'avvenuto incidente

Il verificarsi di un evento anomalo relativo alla sicurezza delle informazioni può essere rilevato da qualsiasi soggetto interno (es. personale dipendente, personale convenzionato, stagisti, tirocinanti, borsisti, specializzandi etc.), o da soggetti esterni (cittadini, pazienti, utenti) nonché da Responsabile/Contitolare, Titolare (nel caso in cui l'Azienda agisca in qualità di Responsabile con delega alla notifica).

Il segnalante, dopo aver messo in atto le più semplici ed immediate misure di contenimento provvede a dare comunicazione dell'incidente di sicurezza come segue:

- i soggetti interni devono segnalare immediatamente quanto rilevato al Direttore/Dirigente della Struttura di afferenza, o a suo delegato/sostituto, verbalmente, tramite contatto telefonico, e via e-mail o altro mezzo scritto in caso di indisponibilità della posta elettronica;
- i soggetti esterni quali cittadini, pazienti, utenti tramite segnalazione all'URP;
- i soggetti esterni quali I Responsabili e altre figure Privacy quali Titolari/Contitolari, verbalmente, tramite contatto telefonico ed invio di una PEC indirizzata al relativo DEC.

E' ammessa, in casi eccezionali e se giustificata, la comunicazione da parte del Responsabile esterno entro le 48 ore. Il Responsabile Esterno deve garantire la collaborazione e il supporto necessari a ricostruire l'incidente e a ripristinare la situazione.

In considerazione dell'importanza della tempestività delle azioni, nel caso di incidente di sicurezza in orario notturno o in giornata festiva, l'evento deve essere segnalato al Dirigente Medico reperibile della S.C. Direzione Medica di Presidio, al reperibile dei Sistemi informativi nel caso di incidente informatico, i quali svolgeranno l'analisi preliminare e metteranno in atto e prime azioni per il contenimento delle possibili conseguenze.

Chiunque riceva notizia di incidenti di sicurezza da soggetti esterni, ad es. utenti, è tenuto alla segnalazione con le suddette modalità.

7.5 Analisi preliminare e invio segnalazione

L'Analisi Preliminare dell'evento è una fase importante volta **ad accertare, attraverso la raccolta delle informazioni e la definizione dei soggetti coinvolti, l'effettiva sussistenza del "data breach** e **l'adozione tempestiva delle prime azioni per contenere/annullare il danno**.

Il Direttore della Struttura, o suo delegato, il Medico reperibile della S.C. Direzione Medica di Presidio e/o il reperibile dei Sistemi informativi (nel caso di evento occorso nelle ore notturne o in giornate festive) venuti a conoscenza dell'incidente di sicurezza, valutano la situazione nel più breve tempo possibile, e se ritengono che vi sia stata una violazione o presunta violazione attivano il processo di gestione dell'evento:

- mettendo in atto le prime azioni per il contenimento/annullamento del danno

- dandone prima comunicazione telefonica dell'evento e poi fornendo i dettagli attraverso la compilazione del modulo per la segnalazione "All. A"
- inviando il modulo per la segnalazione al Gruppo di Gestione Data Breach,.

A titolo esemplificativo si riportano nella sezione "Allegati" la tabella contenente tabella contenente alcuni esempi tratti dalle Linee Guida adottate il 03.10.2017 dal Gruppo di Lavoro Art. 29 (Tab. 1) e la tabella contenente alcuni possibili scenari di violazione (Tab. 2).

7.6 Gestione (contenimento del danno) e valutazione gravità dell'evento

La segnalazione dell'incidente è presa in carico dal Gruppo di Gestione Data Breach, composta, a seconda della tipologia della violazione, dalle seguenti figure professionali:

- Coordinatore del Gruppo Aziendale Privacy;
- Componente del Gruppo Aziendale Privacy che svolge attività di supporto giuridico al Coordinatore aziendale Privacy;
- Referente Sistemi Informativi/Informatici o suo delegato;
- Direttore S.C: Tecnico-Ingegneria Clinica- Sistemi Informativi Informatici o suo delegato;
- Il DPO dell'Azienda. La presenza del DPO può essere garantita anche con contatto telefonico o a distanza.

Nel caso in cui si accerti che la violazione abbia compromesso dati contenuti in un sistema informatico, spetta ai Sistemi Informativi/Informatici procedere all'analisi tecnica dell'evento e all'individuazione delle azione da porre in essere per il contenimento degli eventuali danni e il ripristino dei dati.

Il Gruppo di Gestione data breach, esamina il caso e svolge una breve indagine sulla base di quanto indicato nel modulo di segnalazione 'allegato "A", documentandone gli esiti per valutare la necessità di attivare la procedura di notifica al Garante e di comunicazione agli interessati.

In tale fase, sulla base delle informazioni raccolte si procede alla valutazione del rischio sulla base dei parametri e criteri indicati nel modulo "Allegato B", verificando, il tipo di violazione, la natura e il volume dei dati personali coinvolti, la facilità di identificazione delle persone fisiche, la gravità delle conseguenze per le persone fisiche, le caratteristiche particolari dell'interessato e il numero delle persone fisiche coinvolte.

A titolo esemplificativo nella sezione Allegati si riporta la tabella (Tab.3) contenente per ogni tipologia di violazione cosa verificare e alcuni esempi.

Si ricorda che in base all'art. 82 del GDPR Titolari e Responsabili rispondono in solido dei danni arrecati: è quindi interesse dell'Azienda prendere tutte le iniziative possibili per limitare i danni per gli interessati.

7.7 Notifica al Garante della Privacy

Terminato il processo di valutazione:

- se i **rischi** per gli interessati sono **trascurabili**, la procedura può terminare: dopo aver informato l'eventuale Titolare e la Direzione Aziendale e documentato il processo e le scelte operate (misure messe in atto adeguate alla minaccia occorsa). In questo caso la Fase di Miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria;

- se si ritiene che vi sia stata **una violazione di dati personali** e se vi è una ragionevole certezza che essa presenti un rischio per i diritti e le libertà delle persone fisiche, il Gruppo Gestione Data Breach informa entro 36 ore la Direzione Aziendale, fornendole tutti i dati raccolti.

La Direzione Aziendale, acquisite le informazioni raccolte provvede, tramite il Gruppo di Gestione Data Breach a predisporre la Notifica, utilizzando Modello reso disponibile dal Garante della privacy – Allegato "C", contenente: .

- la descrizione della violazione dei dati personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- l'indicazione del nome ed i relativi dati di contatto del RPD;
- la descrizione delle probabili conseguenze della violazione;
- l'indicazione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e che, se del caso, per attenuare i possibili effetti negativi;

La notifica deve avvenire senza ingiustificato ritardo, entro i termini previsti per norma (72 ore), decorrenti dal momento in cui i soggetti designati, autorizzati, i Responsabili sono "ragionevolmente" certi che si è verificato un incidente di sicurezza che ha comportato una compromissione di dati"[1].
Alla scadenza delle 72 ore è opportuno fare una comunicazione significando che questa è l'inizio di una notifica in fasi. Si può valutare di fare una notifica cumulativa se una stessa compromissione ha riguardato la stessa tipologia di dati con le stesse modalità.

La notifica effettuata oltre i termini di norma deve essere accompagnata dei motivi del ritardo.

Nella predisposizione delle informazioni contenute nella Notifica occorre tener conto dei risultati della fase "Comunicazione agli Interessati" che viene esposta nel capoverso 7.9 della presente procedura.

7.8 Altre segnalazioni dovute

Il Titolare, per il tramite il Gruppo Gestione Data Breach, provvede ad informare, ricorrendone i presupposti, altri organi quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti), tra cui la Polizia Postale e delle comunicazioni;
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche);
- al Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale):
- All'Autorità Competente NIS, nel caso di incidente rilevante ex art. 12 c. 5 del D.Lgs. 65/2018.

7.9 Comunicazione agli interessati

Mentre per far scattare l'obbligo di notifica è sufficiente una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione è necessario che il rischio sia elevato.

[1] Par. 2, lettera a) punto2 delle Linee Guida sulla notifica delle violazioni, adottate il 03/10/2017 del Gruppo di Lavoro art.29

In tal caso il Titolare provvede ad informare, senza ingiustificato ritardo, gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio, utilizzando il Modulo "Allegato "D".

La comunicazione deve contenere, con linguaggio semplice e chiaro (art.34.2 GDPR), almeno le seguenti informazioni:

- la natura della violazione dei dati personali;
- i dati di contatto del DPO o altro referente competente a fornire informazioni necessarie;
- le probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Tra le misure proposte possono figurare anche le misure che sono suggerite agli interessati per limitare i danni: l'individuo può mettere in atto le misure suggerite per limitare i danni.
Si ricorda che in base all'art. 82 del GDPR Titolari e Responsabili rispondono in solido dei danni arrecati: è quindi interesse dell'Azienda prendere tutte le iniziative possibili per limitare i danni per gli interessati.

La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta quando:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
- la comunicazione richiederebbe sforzi sproporzionati.

Tenuto conto della tipologia della violazione o del numero di interessati coinvolti, qualora la segnalazione ai singoli interessati comporti sforzi sproporzionati il Titolare, tramite il Gruppo Gestione Data Breach, coinvolge immediatamente l'Ufficio Stampa e l'Ufficio Relazioni con il Pubblico per procedere ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

7.10 Inserimento dell'evento nel registro delle violazioni

L'art. 33 paragrafo n. 5 del DGPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Pertanto, il Gruppo di Gestione Data Breach dovrà provvedere all'inserimento nel registro delle violazioni dell'evento che in questo modo sarà documentato, tracciabile e in grado di fornire evidenza nelle sedi competenti.

Per quanto riguarda la documentazione delle violazioni, Il Titolare del trattamento tiene conto del parere del RPD in merito alla struttura, all'impostazione e all'amministrazione della documentazione stessa.

7.11 Azioni correttive specifiche e per analogia

Il Titolare, tramite il Gruppo Aziendale Privacy e sentito il Gruppo di Gestione Data Breach, nonché figure tecniche-professionali competenti, al termine dell'analisi dell'incidente individua le aree vulnerabili, promuovendo l'adozione delle seguenti azioni di miglioramento:

- Audit specifico e tempestivo sui trattamenti coinvolti da parte del Gruppo Privacy e del DPO;
- Adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme;
- Individuazione di controlli e misure di sicurezza che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- Valutazione su possibilità di copertura assicurativa;
- Programmazione azioni informative rivolte ai dipendenti;
- Revisione delle relazioni con Clienti e Fornitori;
- Pianificazione test periodici per verificare la validità della presente procedura;
- Revisione della procedura, se necessaria, e di eventuali altri documenti collegati.

8. Indicatori

Criterio	Indicatore	Standard
Tempestività	Numero ore da accertamento violazione a notifica	Entro 72 ore
Sicurezza	Numero di incidenti segnalati	Crescente
Sicurezza	Gravita degli incidenti segnalati	Decrescente
Sicurezza	Numero di violazioni annue	Tendente a zero

Sicurezza	Numero di notifiche al Garante rispetto al numero di violazioni	100%
Sicurezza	Numero di comunicazioni agli interessati rispetto al numero di violazioni rischio alto	100%

9. Documenti collegati

Documenti e Individuazione dei soggetti “Designati” e dei dipendenti “Autorizzati” al Trattamento dei dati personali.

10. Archiviazione

Pagina Web Aziendale

Intranet- sezione Privacy