PROCEDURA DATA BREACH

SEZIONE SCHEDE SINOTTICHE – SCHEDE ESEMPLIFICATIVE E ALLEGATI

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

Per ogni fase vengono sinteticamente descritti i soggetti coinvolti, la tempistica e le modalità di azione.

0	Predisposizione strumenti

Come?	Rigorosa applicazione dei principi previsti all'art. 5 del GDPR (principio di minimizzazione, periodo di conservazione dei dati, pertinenza delle informazioni gestite rispetto alle finalità,soggetti autorizzati, applicazione dei principi di Privacy by design)
Come?	Adozione misure tecniche ed organizzative

1	Rilevazione Evento Acquisizione Notizia avvenuto incidente

Chi?	Qualsiasi soggetto interno (es. personale dipendente, personale convenzionato, stagisti, tirocinanti, borsisti, specializzandi etc.) o esterno (es. cittadini, pazienti, utenti, responsabili, contitolari, titolari).
A Chi?	Per gli **interni**: al Direttore/Dirigente della Struttura di afferenza, o a suo delegato/sostituto 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 Per gli esterni quali cittadini o utenti: all'URP Per i soggetti **esterni** quali Titolari/contitolari/Responsabili: al DEC.
Quando?	Per gli interni: appena se ne viene a conoscenza e comunque entro la giornata. Per gli esterni: entro le 24 ore
Come?	Per gli interni: verbalmente, anche tramite contatto telefonico, o via e-mail. Per gli esterni esterni quali cittadini o utenti : con qualsiasi mezzo a loro disposizione (di persona, telefonicamente, con posta elettronica, inviata a URP@sanluigi.piemonte.it; Per i soggetti esterni quali Titolari/contitolari/Responsabili: verbalmente, tramite contatto telefonico ed invio di una PEC indirizzata al relativo DEC

2	Analisi preliminare e invio segnalazione

Chi?	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
A Chi?	Gruppo di Gestione Data Breach
Quando?	Nel più breve tempo possibile
Come?	Compilando il modulo per la segnalazione "All. A" e inviandolo in Direzione Sanitaria

3	Gestione e valutazione gravità dell'evento

Chi?	Gruppo di Gestione Data Breach DPO
A Chi?	Titolare del trattamento. Nel caso di necessità di notifica la comunicazione al Titolare va effettuata entro 36 ore.
Quando?	Appena ricevuta la comunicazione (All. A)
Come?	Valutando, la gravità dell'impatto della violazione sulla base delle informazioni raccolte sulla base dei parametri e criteri indicati nel modulo "Allegato B"

4	Notifica al Garante Privacy

Chi?	Il Titolare, acquisite le informazioni raccolte provvede, tramite il Gruppo di Gestione Data Breach
A Chi?	Al Garante Privacy
Quando?	Senza ingiustificato ritardo, entro i termini previsti per legge (72 ore) dall'avvenuta conoscenza dell'incidente. Nel caso di ritardo è necessario esplicitare la motivazione
Come?	Utilizzando Modello reso disponibile dal Garante della privacy – Allegato "C",. Anche in fasi qualora sano necessari approfondimenti Anche cumulativa se una stessa compromissione ha riguardato la stessa tipologia di dati con le stesse modalità.

5	Altre segnalazioni dovute: (es. agli organi di Polizia e, nel caso di incidente informatico, a CERT-PA)

Chi?	Il Titolare, per il tramite il Gruppo Gestione Data Breach
A Chi?	- CERT-PA (se 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 - CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche). - 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
Quando?	Tempestivamente
Come?	Via e-mail

6	Comunicazione agli interessati, ove necessario, e raccolta riscontro dell'avvenuta comunicazione

Chi?	Il Titolare, per il tramite il Gruppo Gestione Data Breach
A Chi?	Alle persone fisiche i cui dati sono stati violati
Quando?	Senza ingiustificato ritardo
Come?	Utilizzando il Modulo "Allegato D" e inviandolo ai diretti interessati o, qualora la segnalazione ai singoli interessati comporti sforzi sproporzionati, coinvolgendo Ufficio stampa e l'URP per altre forme di comunicazioni accessibili alle categorie di interessati.

7	Inserimento dell'evento nel Registro delle Violazioni (Comprese le violazioni che non richiedono la notifica)

Chi?	Gruppo Gestione Data Breach
A Chi?	Al Gruppo Aziendale Privacy Direttore/Dirigente della Struttura di afferenza, o a suo delegato/sostituto 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
Quando?	Tempestivamente sia in caso di archiviazione che di avvenuta notifica al Garante
Come?	Inserendo l'evento nel registro delle violazioni (Applicativo informatico dedicato)

.

8	Azioni correttive specifiche e per analogia

Chi?	Il Titolare, tramite il Gruppo Aziendale Privacy e sentito il Gruppo di Gestione Data Breach, nonché figure tecniche-professionali competenti
A Chi?	Alle strutture interessate
Quando?	Al termine dell'analisi dell'incidente e dell'individuazione del le aree vulnerabili
Come?	Comunicazione con le proposte di azioni di miglioramento

Azioni da intraprendere in funzione della determinazione di livello del rischio stimato:

Livello di Rischio (LR)	Ove possibile entro 72 h Notifica all'Autorità	Senza ingiustificato ritardo Comunicazione agli interessati
Rischio alto/Molto Alto	SI	SI
Rischio Medio	SI	NO
Rischio Basso/Trascurabile	NO	NO

Situazione 1

Il rischio per i diritti e le libertà delle persone fisiche

NON E' ELEVATO

Situazione 2

Il rischio per i diritti e le libertà delle persone fisiche

E' PROBABILE MA NON E' ELEVATO

Situazione 3

Il rischio per i diritti e le libertà delle persone fisiche

E' PROBABILE ED ELEVATO

Il Titolare non deve notificare al Garante o dare comunicazione agli interessati.

E' tenuto a documentare sul REGISTRO DELLE VIOLAZIONI l'analisi dei rischi effettuati

Il Titolare deve effettuare la notifica al Garante senza indebito ritardo, comunque entro 72 ore

Il Titolare deve notificare la violazione al Garante e dare comunicazione agli interessati

NOTIFICA E COMUNICAZIONE VANNO DOCUMENTATE NEL REGISTRO

TABELLA 1. ESEMPI VIOLAZIONI TRATTI DALLE LINEE GUIDA ADOTTATE DAL GRUPPO DI LAVORO ART. 29.

Vengono riportati da *"WP 250 Guidellines on personal data breach notification under Regulation 2016/679 del 03.10.2017"* diversi scenari di violazione dei dati personali che si possono verificare da valutare come probabili data breach e che possono essere di aiuto nella gestione dell'evento:

Esempio	Notifica al Garante?	Comunicazione all'interessato?	Note/raccomandazioni
Il Titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché 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.
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce agli utenti di accedere al servizio.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5 del GDPR
Il 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. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	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 onseguenze.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, 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.
I dati sanitari di un Ospedale non sono disponibili per un periodo di trenta ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei	Si, informare le persone fisiche coinvolte .	
I dati personali di un grande numero di studenti vengono inviati per errore ad una mailing list sbagliata, con più di mille destinatari	Sì	Si, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze	

TABELLA 2. ESEMPI POSSIBILI SCENARI DI VIOLAZIONE IN OSPEDALE

Sia per quanto riguarda i trattamenti cartacei che quelli elettronici, gli eventi che possono dare origine a potenziali situazioni di data breach possono essere di natura dolosa o accidentale.

Tipologie di violazione	Definizione	Quando segnalare	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non più nella disponibilità del Titolare e/o di altri. Non è possibile produrre il dato all'interessato nel caso di sua richiesta.	Dati non recuperabili o provenienti da procedure non ripetibili. I soli dati appartenenti a **documenti definitivi e validati**	Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. Guasto non riparabile dell'hard disk contenente dati particolari 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 (in unica copia) Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
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). Non è possibile produrre il dato all'interessato nel caso di sua richiesta.. E' possibile che terzi possano avere impropriamente accesso al dato.	Dati non sono recuperabili o provengono da procedure non più ripetibili. Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato 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 Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	Smarrimento di chiavetta USB con dati originali; smarrimento di un telefonino aziendale nel caso in cui contenga dati personali e non sia stato opportunamente cifrato. Smarrimento di fascicolo personale cartaceo dei dipendenti. Smarrimento di una cartella clinica in originale e impossibilità a ricostruirne il contenuto.	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. Non è possibile produrre il dato all'interessato	I dati sono stati alterati irreversibilmente senza possibilità di ripristinare lo stato originale. Rientrano i dati appartenenti a documenti definitivi e validati	. Guasto tecnico che altera e compromette i 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	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 alla alterazione di dati tracciata e reversibile Modifica di un documento non ancora

	nel caso di sua richiesta.		tracciato e irreversibile Azione involontaria di un lavoratore che porta alla compromissione di alcuni dati sullo stato giuridico del personale	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	I dati appartenenti a documenti definitivi e validati	Spedizione di dati ad indirizzo non corretto o consegna a persona non autorizzata di dati di pazienti su supporto informatizzato Trasmissione non autorizzata di dati non ancora validati Violazione della segretezza dei dati di pazienti per informare gli organi di stampa	Il medico su AREAS seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi, inserendo l'anamnesi e il referto. 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), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione	I dati appartenenti a documenti definitivi e validati	Accesso alla rete aziendale da parte di persone esterne tramite vulnerabilità insite ne Accesso da parte di un utente a dati non di sua pertinenza I sistema Accesso ed uso improprio dei dati di pertinenza	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.	I dati non sono disponibili per un periodo di tempo che lede i diritti dell'interessato	Infezione del sistema che comporta temporanea perdita e impossibilità di recupero Cancellazione accidentale di dati da parte di personale non autorizzato Perdita di chiave di decrittografia di dati crittografati	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

TABELLA 3. ESEMPI PER LA VALUTAZIONE DEL RISCHIO

Cosa verificare	Cosa verificare	Esempi
Tipo di violazione	Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche?	Una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici sono stati persi e non sono più disponibili.
Natura e volume dei dati personali coinvolti	La natura dei dati personali compromessi dalla violazione: maggiore è il rischio di danni per gli interessati ove questi rientrino nelle categorie particolari di dati,. Fermo quanto precede, ai fini di una puntuale valutazione occorre prendere in considerazione anche altri elementi, posto che anche la semplice violazione di dati comuni potrebbe comportare un rischio rilevante ai fini della notifica e della comunicazione. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale. Analogamente, una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, mentre una vasta gamma di dettagli può rivelare molte più informazioni in merito alla stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.	Ad esempio, violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità.
Facilità di identificazione delle persone fisiche	Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei	Ad esempio, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4, punto 5 del GDPR come "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*") può ridurre la probabilità che le persone fisiche

	corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.	vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.
Gravità delle conseguenze per le persone fisiche	A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto nei casi di furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Parimenti, se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. In caso di violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati danni.	Il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione. Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine

Caratteristiche particolari dell'interessato	Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.	Violazioni relative a dati sulla salute relative a determinate patologie (es. paziente affetto da sclerosi multipla, HIV, etc.) possono causare rischi di discriminazione per l'interessato.
Numero di persone fisiche interessate	Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.	Un interruzione di rete per più di una giornata può riguardare dati di molte persone, determinando un maggior impatto della violazione.

ALLEGATO A- SEGNALAZIONE INCIDENTE RELATIVO ALLA SICUREZZA

La compilazione del presente modulo è a cura del Direttore della Struttura cui si riferiscono i dati oggetto della violazione, o del Medico di Direzione Sanitaria reperibile nel caso di incidente occorso nelle ore notturne o nelle giornate festive.

DATI DEL SEGNALANTE	
Nome, cognome, qualifica	
Recapito telefonico, mail	
Struttura di appartenenza	
DATA DELL'INCIDENTE	
Quando si è verificata la violazione dei dati personali?	[] Il ___/___/_____ [] Tra il ___/___/____e il [] In un tempo non ancora determinato [] E' possibile che sia ancora in corso
LUOGO DELL'INCIDENTE	
Dove si è verificata la violazione dei dati personali?	
DESCRIZIONE DELL'INCIDENTE	
Classificazione dell'incidente	[ ] Violazione della riservatezza [ ] Violazione dell'integrità [ ] Violazione della disponibilità
Tipo di violazione	[ ] **Lettura** (presumibilmente i dati sono stati consultati, ma non sono stati copiati) [ ] **Copia** (I dati sono ancora presenti sul sistema/device, ma sono stati anche copiati altrove) [ ] **Alterazione** (I dati sono presenti sul sistema/device, ma sono stati alterati) [ ] **Cancellazione** (I dati non sono più sul sistema/device e non li ha più l'autore della violazione) [ ] **Furto di dati** (I dati non sono più sul sistema/device e li ha l'autore della violazione) [ ] **Furto di device o supporto di memorizzazione o materiale cartaceo** (es. computer, chiavetta USB, documenti cartacei contenenti particolari categorie di dati) - Specificare quale device, supporto di memorizzazione _____ [ ] **Furto di materiale cartaceo contenente categorie particolari di dati (es. cartelle ciniche, referti, etc.)** - Specificare la tipologia di documentazione_____ [[ ] **Furto di credenziali di accesso a** (es. account personale, password, applicazioni: AREAS, Concerto, etc.) [ ] **Accesso abusivo al sistema informatico:** - Denominazione del sistema _____ - Collocazione fisica del sistema (se interno o esterno all'Azienda) [ ] **Divulgazione non autorizzata o non voluta di dati personali** [ ] Altro _____

Oggetto della violazione	[ ] PC [ ] Rete [ ] Dispositivo mobile [ ] File o parte di un file [ ] Strumento di Backup [ ] Materiale cartaceo [ ] Altro
Quali categorie di soggetti interessati sono coinvolti dalla violazione?	[ ] Dipendenti [ ] Utenti [ ] Altro
Tipo di dato oggetto della violazione	[ ] Dati personali (es. dati anagrafici/codice fiscale/indirizzo di posta elettronica) [ ] Dati di accesso e di identificazione (username, password) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica [ ] Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati genetici [ ] Dati biometrici [ ] Dati relativi alla salute [ ] Dati relativi alla vita sessuale o all'orientamento sessuale [ ] Dati giudiziari [ ] Dati sanitari relativi a persone sieropositive, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool [ ] Altro :
Numero approssimativo degli interessati coinvolti nella violazione	[ ] numero certo di persone ____ [ ] numero presunto di persone____ [ ] numero sconosciuto di persone _____
Livello di gravità della violazione dei dati	[ ] Basso/trascurabile [ ] Medio [ ] Alto [ ] Molto alto
Effetti e conseguenze della violazione:	
Quali misure tecniche ed organizzative sono state adottate per contenere la violazione dei dati e prevenire violazioni future	
L'incidente è occorso presso un Responsabile Esterno del trattamento dei dati personali?	[ ] Si, specificare i trattamenti oggetto di nomina _____ [ ] No

ALLEGATO B- VALUTAZIONE DEL RISCHIO

Classificazione dell'incidente	[ ] Violazione della riservatezza [ ] Violazione dell'integrità [ ] Violazione della disponibilità
Tipo di dato oggetto della violazione	[ ] Dati personali (es. dati anagrafici/codice fiscale/indirizzo di posta elettronica) [ ] Dati di accesso e di identificazione (username, password) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica [ ] Dati personali idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati genetici [ ] Dati biometrici [ ] Dati relativi alla salute [ ] Dati relativi alla vita sessuale o all'orientamento sessuale [ ] Dati giudiziari [ ] Dati sanitari relativi a persone sieropositive, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, [ ] Altro
Tipo di violazione	[ ] **Lettura** (presumibilmente i dati sono stati consultati, ma non sono stati copiati) [ ] **Copia** (I dati sono ancora presenti sul sistema/device, ma sono stati anche copiati altrove) [ ] **Alterazione** (I dati sono presenti sul sistema/device, ma sono stati alterati) [ ] **Cancellazione** (I dati non sono più sul sistema/device e non li ha più l'autore della violazione) [ ] **Furto di dati** (I dati non sono più sul sistema/device e li ha l'autore della violazione) [ ] **Furto di device o supporto di memorizzazione o materiale cartaceo** (es. computer, chiavetta USB, documenti cartacei contenenti particolari categorie di dati) - Specificare quale device, supporto di memorizzazione _____ - Consente l'accesso a _____ [ ] **Furto di materiale cartaceo contenente categorie particolari di dati (es. cartelle ciniche, referti, etc.)** - Specificare la tipologia di documentazione_____ [ ] [ ] **Furto di credenziali di accesso a** (es. account personale, password, applicazioni: AREAS, Concerto, etc.) - nome account_____ - consente l'accesso a _____ [ ] [ ] **Accesso abusivo al sistema informatico:** - Denominazione del sistema _____ - Collocazione fisica del sistema (se interno o esterno all'Azienda) [ ] **Divulgazione non autorizzata o non voluta di dati personali** [ ] Violazione che riguarda una notevole quantità di dati personali [ ] Violazione che riguarda un vasto numero di interessati [ ] Violazione [ ] Altro_____

Effetti sui dati personali	[ ] Distruzione illecita [ ] Distruzione accidentale [ ] Perdita illecita [ ] Perdita accidentale [ ] Divulgazione non autorizzata [ ] Accesso illecito [ ] Altro
Eventi dannosi che potrebbero verificarsi nei confronti dell'interessato	[ ] Discriminazione [ ] Furto o usurpazione di identità [ ] Perdite finanziarie [ ] Pregiudizio per la reputazione [ ] Perdita di riservatezza dei dati personali protetti da segreto professionale [ ] Decifratura non autorizzata della pseudonimizzazione [ ] danno economico o sociale significativo [ ] Privazione o limitazione di diritti o libertà [ ] Perdita di controllo sui dati personali dell'interessato [ ] Danni fisici, materiali o immateriali alle persone fisiche [ ] Altro :
Quali misure tecniche e organizzative sono state adottate preventivamente? (es. Pseudonimizzazione e cifratura dei dati personali, conservazione documentazione in locali accessibili solo da personale	
Successivamente alla violazione sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti le libertà degli interessati?	
Livello di gravità della violazione dei dati personali	[ ] **Basso/trascurabile**: le persone fisiche possono incontrare alcuni piccoli inconvenienti, superabili senza alcun problema (es. reinserendo le informazioni) [ ] **Medio:** le persone fisiche possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (es. costi aggiuntivi, rifiuto di accesso ai servizi aziendali, stress) [ ] **Alto**: le persone fisiche possono incontrare conseguenze significative che dovrebbero essere in grado di superare anche se con gravi difficoltà (es. peggioramento della salute) [ ] **Molto alto**: le persone fisiche possono avere conseguenze significative o addirittura irreversibili, che non possono superare (es. danni gravi alla salute) Altro: _____
Notificazione del data Breach all'Autorità Garante	[ ] Si [ ] No Note _____
Comunicazione del data Breach agli interessati	[ ] Si [ ] No Note _____

Allegato C: Schema di notifica: reperibile sulla pagina web del Garante

Allegato D

MODELLO DI COMUNICAZIONE DEL DATA BREACH ALL'INTERESSATO

Gentile (*nome e cognome dell'interessato*),

Con la presente si comunica che l'Azienda Ospedaliero-Universitaria San Luigi Gonzaga di Orbassano, Titolare del trattamento in data_____ è venuta a conoscenza di un evento che potrebbe aver coinvolto i Suoi dati personali.

In particolare, è accaduto quanto di seguito descritto.

Inserire breve descrizione dell'incidente in relazione al quale si ritiene necessaria la comunicazione all'interessato ed indicazione dei dati personali violate.

Dall'analisi dei fatti sopra riportati, in considerazione della natura della violazione e della tipologia di dati personali coinvolti, si comunicano le possibili conseguenze dell'evento:

Inserire descrizione delle probabili conseguenze del data breach

L'Azienda, venuta a conoscenza dell'incidente, ha tempestivamente posto in essere le seguenti misure tecniche ed organizzative:

Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del data breach

Come previsto dall'art. 33 del Regolamento UE 2016/679 l'Azienda ha provveduto a notificare questa violazione al garante Privacy.

Per ricevere ulteriori conformazioni, può contattare:

rpd@sanluigi.piemonte.it
urp@sanluigi.piemonte.it
011-9026

Distinti saluti

Il Titolare del Trattamento

_____