All. n.1

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Area Vasta Emilia Nord

Schema di procedura per la gestione di *Data Breach* ai sensi del GDPR (Regolamento Europeo 679/2016) nelle aziende sanitarie di AVEN

Redattori del documento: gruppo responsabili ICT e referenti privacy riuniti in AVEN
Data di ultima revisione del documento: 16/05/2018
Stato del documento: Bozza

Sommario

Schema di procedura per la gestione di Data Breach ai sensi del GDPR (Regolamento Europeo 679/2016) nelle aziende sanitarie di AVEN 1
1. Premessa 1
2. Scopo del documento e ambito di applicazione 1
3. Definizioni 1
4. Normativa e documenti di riferimento 2
5. Gestione del data breach interno alla struttura 3
5.1 Premesse 3
5.2 Modalità e profili di notifica all'Autorità Garante Privacy 3
6. Gestione del data breach esterno alla struttura 3
6.1 Premesse 3
6.2 Modalità e profili di notifica all'Autorità Garante Privacy 3
7. Modalità di comunicazione agli interessati 4
8. Schema di valutazione scenari – data breach 4
9. Registro delle violazioni 5

1. Premessa

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

2. Scopo del documento e ambito di applicazione

Il presente documento si prefigge lo scopo di indicare alle Aziende Sanitarie afferenti all'Area Vasta Emilia Nord (AVEN) le opportune modalità di gestione del *data breach*, nel rispetto

della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.
In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del *data breach*, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare per il tramite del referente privacy
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati

3. Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); 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 (art. 4, punto 1).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

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

Referente privacy: la persona fisica (direttamente o indirettamente) afferente ad un'azienda sanitaria che operativamente si occupa delle *policy* di privacy, propone la stesura dei regolamenti sulla privacy e sul trattamento dati ed effettua e valuta controlli sugli stessi. Nelle aziende si è talvolta chiamato come coordinatore privacy o responsabile privacy.

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

Delegato del trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'azienda sanitaria che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).

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

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

4. Normativa e documenti di riferimento

- *Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34*
- *Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)*

5. Gestione del *data breach* interno alla struttura

5.1 Premesse

È necessario che ogni azienda sanitaria dia notizia a tutti gli operatori in merito alla presente procedura mediante idonea delibera e circolare.
In ogni azienda è individuato il referente privacy ed è opportuno che sia affiancato da un gruppo privacy (gruppo multidisciplinare di professionisti che supportano il referente privacy per specificità tecniche quali ICT, SIC, area giuridica, area del personale…).
Il referente privacy assume, ai fini della presente procedura, il ruolo di responsabile del processo.

5.2 Modalità e profili di notifica all'Autorità Garante Privacy

Ogni operatore aziendale autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il delegato al trattamento.
Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale *data breach*, lo segnala tempestivamente al referente privacy utilizzando il modulo allegato (All. 1).
La segnalazione perviene al referente privacy tramite le consuete modalità di gestione dei flussi documentali già in uso nelle singole aziende.
Il referente privacy effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità necessarie per la corretta analisi della situazione.
Quest'ultimo può avvalersi del DPO per eventuali funzioni consulenziali.
Ai fini di una corretta classificazione dell'episodio, il referente privacy utilizzerà lo schema di scenario di *data breach*, allegato alla presente procedura.
Pertanto, sulla scorta delle determinazioni raggiunte, il referente privacy predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy.

6. Gestione del *data breach* esterno alla struttura

6.1 Premesse

Ogniqualvolta l'azienda/titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di *data breach* sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*[1].
Ad ogni responsabile del trattamento deve essere comunicato il contatto del referente privacy al quale effettuare la predetta segnalazione (PEC ad uopo designata dall'azienda sanitaria).

6.2 Modalità e profili di notifica all'Autorità Garante Privacy

Ogni responsabile del trattamento, qualora venga a conoscenza di un potenziale *data breach* che riguardi dati di cui l'azienda sia titolare, ne dà avviso senza ingiustificato ritardo al referente privacy tramite il modulo allegato (All.2)
Per "ingiustificato ritardo" si considera la notizia pervenuta al titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile.
Il referente privacy effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità necessarie per la corretta analisi della situazione.
Quest'ultimo può avvalersi del DPO per eventuali funzioni consulenziali.
Ai fini di una corretta classificazione dell'episodio il referente privacy utilizzerà lo schema di scenario di *data breach* allegato al presente schema di procedura.
Pertanto, sulla scorta delle determinazioni raggiunte, il referente privacy predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy.

1NB: Rimane salva la possibilità che sia il responsabile del trattamento ad effettuare una notifica per conto del titolare del trattamento, se il titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del GDPR. La responsabilità legale della notifica rimane in capo al titolare del trattamento. In questa procedura si esamina solamente il caso d'uso ordinario in cui la notifica venga effettuata dal titolare del trattamento.

7. Modalità di comunicazione agli interessati

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

Il referente privacy predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

8. Schema di valutazione scenari – *data breach*

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

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	. Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	• Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. • Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente • Incendio di archivio cartaceo delle cartelle cliniche. • Distruzione di campioni biologici	• Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) • Rottura di un PC che non contiene dati personali originali (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	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili • Dati relativi a più	• Smarrimento di chiavetta USB contenente dati originali • Smarrimento di fascicolo cartaceo personale dipendente	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

	di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	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 e 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		
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Caratteristiche: • Modifiche sistematiche e su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup • Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery • Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile • Modifica di un documento non ancora validato dal proprio autore.

Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Malfunzionamento del sistema di oscuramento del sistema dipartimentale che invia a SOLE • Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	• Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione ed invia a SOLE. • Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico	• Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi • Accesso non autorizzata di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	• Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

	tempo che lede i diritti dell'interessato.		backup • cancellazione accidentale dei dati da parte di una persona non autorizzata • perdita della chiave di decrittografia di dati crittografati in modo sicuro • irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve	

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

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

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach,* ma è considerato un normale errore procedurale (esempio l'invio di un referto alla rete SOLE in cui il testo del referto è di un paziente mentre l'anagrafica è di un altro). Questo poiché:

- chi riceve non può sapere a quale paziente fisico è riferito il testo;
- il paziente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

9. Registro delle violazioni

Il referente privacy cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, comma 5 del GDPR.