SOMMARIO

Referenti della Procedura:
Ing. Savigni Roberto (parte tecnologica)
Dr. Giorgio Bertacchini (parte normativa)

Gruppo di Lavoro:
Componenti del Gruppo Privacy aziendale su documento guida redatto dal gruppo responsabili ICT e referenti privacy riuniti in AVEN: Ing. Savigni Roberto (Servizio Tecnologie dell'Informazione - STI), Dr. Giorgio Bertacchini (Segreteria Generale – Settore Legale Assicurazioni e Privacy), Ing. Lugli Mario (Servizio Tecnologie dell'Informazione - STI)

REDAZIONE		
Data	**Funzione**	**Visto**
3/03/2021	Ref. proc.	Ing. R. Savigni
2/03/2021	Ref. proc.	Dr. G. Bertacchini

APPROVAZIONE		
Data	**Funzione**	**Visto**
5/03/2021	Direttore Amministrativo	Dr. L. Broccoli

VERIFICA								
Serv. Tecnologie dell'Informazione			**Serv. Segreteria Generale**			**Serv. Assicurazione Qualità**		
Data	**Funzione**	**Visto**	**Data**	**Funzione**	**Visto**	**Data**	**Funzione**	**Visto**
4/3/21	Direttore	Ing. M. Lugli	1/03/2021	Direttore	Dr.ssa C. Vandelli	05/3/21	RAQ Az.	Dr.ssa B. Trevisani

1. MODIFICHE

REV.	PAGINE O DOCUMENTI MODIFICATI	TIPO/ NATURA DELLA MODIFICA
1	*Pag. 3,6*	Esteso da 12 h a 24 h il tempo entro il quale i responsabili del trattamento dei dati personali devono comunicare all'Azienda un eventuale episodio di Data Breach.

2. OGGETTO E SCOPO

Il presente documento si prefigge lo scopo di indicare a tutto il personale operante per l'Azienda Ospedaliero-Universitaria di Modena le modalità di gestione del *data breach*, ovvero di un episodio di violazione di dati personali, 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 (c.d. GDPR).
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. CAMPO DI APPLICAZIONE

La procedura si applica a tutto l'ambito aziendale e a tutti i soggetti che, a vario titolo, svolgano attività presso l'Azienda Ospedaliero Universitaria di Modena
La procedura si applica inoltre in presenza di possibili violazioni di dati personali siano essi contenuti in banche informatiche o cartacee.

4. RESPONSABILITÀ

Referenti di procedura	Sono il riferimento per l'aggiornamento della procedura alla luce di variazioni legislative, normative interne o esterne ed alla luce delle evoluzioni tecnologiche, strutturali e di contesto. Sorvegliano l'applicazione della procedura e promuovono le opportune azioni correttive laddove se ne ravvisi la necessità, per la loro parte di competenza

5. INDICATORI APPLICABILI

Indicatore	Frequenza di elaborazione	Foglio raccolta dati	Report
Rispetto tempi di segnalazione caso sospetto da parte dei Responsabili esterni (24 ore)	annuale		
Rispetto tempi di segnalazione al Garante (72 ore)	annuale		

6. 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).*
- *D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018..*
- *Delibera n° 90 del 16/05/2018 " RECEPIMENTO DELLA DELIBERA DELL'AUSL DI MODENA N. 110 DEL 27/04/2018 E DESIGNAZIONE DEL DATA PROTECTION OFFICER (DPO) NELLA PERSONA DELLA DR.SSA ERICA MOLINARI."*

- *Delibera n° 99 del 25/05/2018 "REGOLAMENTO UE N. 2016/679 (GDPR) RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHE' ALLA LIBERA CIRCOLAZIONE DI ESSI. RICOGNIZIONE DELLE PRINCIPALI AZIONI DI ADEGUAMENTO DELL'AOU DI MODENA."*
- *Delibera n° 150 del 6/09/2018 "REGOLAMENTO (UE) N. 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (GDPR) – RIDEFINIZIONE DEI PROFILI DI RESPONSABILITÀ IN TEMA DI PROTEZIONE DEI DATI PERSONALI E NUOVE MODALITÀ DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AD ESEGUIRE OPERAZIONI DI TRATTAMENTO."*

7. 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, § 1, n 1 GDPR).

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, § 1, n. 2 GDPR).

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, § 1, n. 6 GDPR).

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, § 1, n.7 GDPR). In questo contesto, il titolare del trattamento è l'Azienda Ospedaliero-Universitaria di Modena.

Gruppo privacy: Le persone designate dal titolare (v.si delibera D.G. n. 99/2018) a formare un gruppo di studio e lavoro in materia di privacy, per studiare e seguire tutti gli adempimenti necessari a dare attuazione alla normativa relativa al trattamento dei dati personali.

Referente privacy: la persona che coordina il gruppo privacy aziendale il quale all'interno dell'AOU operativamente si occupa delle *policy* di privacy, propone la stesura dei relativi regolamenti sulla privacy e sul trattamento dati ed effettua e valuta controlli sugli stessi.

Referente data breach: la persona designata con provvedimento del D.G., (V.si delibera DG n. 99/2018) che all'interno dell'AOU operativamente si occupa delle segnalazioni provenienti dai delegati interni del titolare, dai responsabili esterni, dagli interessati e da qualunque altro soggetto esterno all'AOU e dà attuazione agli adempimenti previsti dalla norma e della presente procedura.

Data Protection Officer (DPO): La persona individuata dal Titolare del Trattamento (vedi Delibera n° 90/2018) quale Responsabile della protezione dei dati personali, così come previsto dal GDPR per tutte le pubbliche amministrazioni.la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR.

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 (v.si delibera DG n. 150/2018 che ha designato i responsabili di struttura complessa, di struttura semplice dipartimentale e degli uffici di staff).

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

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo esterno all'AOU che tratta dati personali per conto del titolare del trattamento (art. 4, § 1, n. 8 GDPR).

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, § 1, n.12 GDPR).

8. CONTENUTO

8.1. 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.

8.2. Gestione del data breach interno alla struttura

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 (di norma il Direttore o il Responsabile della Struttura presso la quale presta servizio).
Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale *data breach*, lo segnala tempestivamente, via e-mail, al referente data breach nonché al referente privacy utilizzando il modulo allegato (All. 1), disponibile nella sezione Privacy dell'Intranet aziendale.
Il referente data breach effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità necessarie per la corretta analisi della situazione.
Sia il responsabile data breach sia i componenti del gruppo privacy potranno avvalersi del DPO per eventuali funzioni consulenziali.
Ai fini di una corretta classificazione dell'episodio, il referente data breach utilizzerà lo schema di scenario di *data breach*, allegato alla presente procedura.
Pertanto, sulla scorta delle determinazioni raggiunte, e solo qualora ritenga che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche il referente data breach

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 del data breach previa consultazione con il gruppo privacy.

8.3. Gestione del data breach esterno alla struttura

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].

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 data breach e al referente privacy tramite il modulo allegato (All.2), che dovrà far parte degli allegati al contratto, anche con rinvio al sito istituzionale dell'AOU.
Per *"ingiustificato ritardo"* si considera la notizia pervenuta al titolare al più tardi entro 24 ore dalla presa di conoscenza iniziale da parte del responsabile.
Il referente data breach effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità necessarie per la corretta analisi della situazione.
Sia il responsabile data breach sia i componenti del gruppo privacy potranno avvalersi del DPO per eventuali funzioni consulenziali.
Ai fini di una corretta classificazione dell'episodio il referente data breach utilizzerà lo schema di scenario di *data breach* allegato alla presente procedura.
Pertanto, sulla scorta delle determinazioni raggiunte, e solo qualora ritenga che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il referente data breach 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 del data breach previa consultazione con il gruppo privacy.

8.4. Modalità di comunicazione agli interessati

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.

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, supportato dal gruppo 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 tenendo anche conto di eventuali indicazioni fornite dall'Autorità Garante. La comunicazione descriverà, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali, le probabili conseguenze della stessa, nonché le misure individuate per porvi rimedio.

8.5 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 di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili • Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti	• 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

	non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	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		
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 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	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

	regolamento dell'organizzazione.			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.

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.

8.6. Registro delle violazioni

Il referente data breach tiene il relativo registro delle violazioni e ne cura l'aggiornamento, ai sensi dell'art. 33, § 5 del GDPR.

9. ALLEGATI

Allegato 1 – Modello per la segnalazione di un sospetto caso di data breach da parte di un delegato interno
Allegato 2 – Modello per la segnalazione di un sospetto caso di data breach da parte di Responsabile esterno