SOMMARIO

Rev	Data	Redazione	Verifica	Approvazione	Descrizione
00	07.10.19	Dott.ssa Emanuela Raho Dott.ssa Federica Pierleoni Avv. Alessandra Cesarotti Dott.ssa Paola D'Eugenio Dr. Nicola Nardella Ing. Mauro Luciani Dott.ssa Donatella Giovannini	Dr. E. Berselli RAQ	Dr.ssa Maria Capalbo Direttore Generale	Prima stesura **VALIDITA' 2019-2020**
01	15.11.2021	Dott.ssa Emanuela Raho Dott.ssa Federica Pierleoni Avv. Alessandra Cesarotti Dott.ssa Paola D'Eugenio Dr.ssa Cristiana Cattò Ing. Mauro Luciani Dott.ssa Donatella Giovannini	Dr. E. Berselli RAQ	Dr.ssa Maria Capalbo Direttore Generale	Revisione dei seguenti paragrafi: paragrafo 3 paragrafo 4 **VALIDITA' NOVEMBRE 2023**

1. SCOPO

La presente istruzione ha la finalità di indicare a tutto il personale operante presso l'Azienda Ospedaliera Ospedali Riuniti Marche Nord (di seguito denominata "Azienda Ospedaliera") la modalità di gestione di un *data breach* - ovvero di un evento di violazione dei dati personali - nel rispetto dei principi e delle disposizioni contenute nel Regolamento (UE) 2016/679 sulla protezione dei dati (di seguito denominato "GDPR").

Nell'ambito dell'istruzione vengono esplicitate le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa della gestione del *data breach*, con particolare riferimento ai seguenti aspetti:

- Modalità e profili di segnalazione al Titolare del trattamento per il tramite del Responsabile della protezione dei dati
- Valutazione dell'evento verificatosi
- Modalità e profili di segnalazione all'Autorità Garante
- Eventuale comunicazione agli interessati.

2. CAMPO DI APPLICAZIONE

In presenza di possibili violazioni dei dati personali – siano essi contenuti in banche informatiche o cartacee – l'istruzione si applica a tutti i soggetti che, a vario titolo, svolgono attività nell'ambito delle diverse articolazioni organizzative dell'Azienda Ospedaliera.

3. RIFERIMENTI NORMATIVI E DOCUMENTALI

- 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)";
- 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)";
- Linee Guida WP 250 del Gruppo di lavoro Articolo 29 sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 - adottate il 3 ottobre 2017 e emendate il 6 febbraio 2018;
- Provvedimento del Garante del 30 luglio 2019 (9126951) sulla notifica delle violazioni dei dati personali (*data breach*);

- Determina DG n. 449 del 31 luglio 2018 "Regolamento UE 2016/679 (RGPD). Designazione Responsabile per la Protezione dei Dati (RPD)";
- Determina DG n. 135 del 20.03.2019 "Definizione degli aspetti organizzativi e funzionali per la gestione della Privacy ai fini dell'adeguamento dell'organizzazione aziendale al Regolamento Europeo 2016/679. Adozione";
- Determina DG n. 128 del 17.03.2021 "Misure organizzative *ex* Regolamento UE 2016/679 (GDPR). Aggiornamento criteri di designazione dei Responsabili interni del trattamento di cui alla determina DG 354/2019";
- Determina DG n. 375 del 23.07.2021 "Regolamento aziendale in materia di protezione dei dati personali. Adozione".

4. DEFINIZIONI, TERMINOLOGIA

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, n. 1 del 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, n. 2 del 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, n. 6 del 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, n. 7 del GDPR).
Titolare del trattamento è l'Azienda Ospedaliera nella persona fisica del Direttore Generale, in qualità di legale rappresentante *pro-tempore*.

Responsabile della protezione dei dati (RPD): la persona fisica nominata dal Titolare del trattamento con determina DG 449 del 31.07.2018, ai sensi degli artt. 37-39 del GDPR.

Gruppo di supporto al Responsabile della protezione dei dati: Gruppo multidisciplinare a supporto del Responsabile della protezione dei dati con competenze medico/sanitarie, tecnico/informatiche e giuridico/legali, costituito con determina DG 449 del 31.07.2019.

Designato in qualità di Responsabile "interno" del trattamento dei dati: la persona fisica che nell'ambito dell'organizzazione aziendale – in ragione dell'incarico ricoperto – svolge compiti e funzioni di vigilanza sul rispetto e attuazione delle istruzioni privacy da parte del personale autorizzato al trattamento di dati personali in servizio presso la struttura rispettivamente diretta; ciò secondo le specifiche istruzioni ricevute dal Titolare.
Sulla base della determina DG 128 del 17.03.2021 i Designati in qualità di Responsabili interni del trattamento sono i Direttori di Struttura Complessa (ovvero i sostituti ex art. 22 del CCNL Area Sanità 2016 – 2018 del 19.12.2019), i Responsabili di Struttura Semplice Dipartimentale, il Responsabile dell'Ufficio Relazioni con il Pubblico ed il Responsabile del Servizio di Prevenzione e Protezione.

Autorizzato/Incaricato al trattamento dei dati: tutte le unità di personale operanti presso le diverse Strutture/Servizi dell'Azienda Ospedaliera che, ai sensi dell'art. 29 del GDPR, effettuano attività di trattamento di dati personali sotto la vigilanza del Designato in qualità di Responsabile "interno" del trattamento e ai quali sono state fornite istruzioni in tal senso.
Il predetto personale è stato, parimenti, autorizzato al trattamento dei dati personali con determina DG n. 128 del 17.03.2021.

Responsabile "esterno" del trattamento dei dati: la persona fisica o giuridica (esterna all'Azienda Ospedaliera) l'autorità pubblica, il servizio o altro organismo che – ai sensi dell'art. 28 del GDPR – tratta dati personali per conto del titolare del trattamento sulla base di apposito atto di nomina.

Interessato: la persona fisica, identificata o identificabile, alla quale i dati si riferiscono.

Violazione dei dati personali (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, n. 12 del GDPR).

5. PROCESSO/MODALITA' OPERATIVE

5.1 Premessa

Una violazione dei dati personali (*data breach*) può - se non gestita in modo adeguato e tempestivo - provocare danni fisici, materiali o immateriali alle persone fisiche (interessati), quali, a titolo esemplificativo, perdita di controllo dei dati personali che le riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione di 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 rilevante per la persona fisica interessata.

5.2 Gestione del *data breach* all'interno della struttura

Ogni operatore aziendale autorizzato a trattare dati personali, qualora venga a conoscenza di un potenziale caso di *data breach*, avvisa tempestivamente il Responsabile interno del trattamento a cui il medesimo afferisce (Direttore/Responsabile di UOC o Responsabile di UOSD).
Il Responsabile interno del trattamento - valutato l'evento - se ritiene confermata la segnalazione di potenziale *data breach*, ne fornisce comunicazione al Responsabile della Protezione dei dati a mezzo e-mail utilizzando, a tal fine, l'allegato modulo (MOD01_IOdgenT003_ORG).
Il Responsabile della Protezione dei dati effettua a sua volta una valutazione dell'evento avvalendosi del supporto e della collaborazione di professionalità interne all'Azienda Ospedaliera, necessarie per la corretta analisi di contesto, quali:

- Servizio Informatico
- Gruppo di supporto al RPD
- Direzione Medica dei Presidi
- Direttori/Responsabili di struttura coinvolti nell'evento.

A seguito delle determinazioni sul punto raggiunte e solo qualora si debba ritenere che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche interessate, il Responsabile della Protezione dei Dati – con lo specifico contributo delle professionalità coinvolte - supporta il Titolare del trattamento nella predisposizione della notificazione all'Autorità Garante, utilizzando a tal fine apposito modulo reso disponibile dalla stessa Autorità Garante sul proprio sito *web* istituzionale. Detta notificazione deve essere inviata senza ingiustificato ritardo e, ove possibile, entro 72 ore da intendersi decorrenti dal momento in cui il Titolare sia venuto a conoscenza della violazione di dati, ovvero da quanto il Titolare abbia raggiunto un ragionevole grado di certezza sul fatto che l'incidente di sicurezza comporti una violazione di 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 di ulteriori indagini e verifiche sull'evento.
La scelta e le motivazioni che hanno condotto a non notificare l'evento devono risultare documentate a cura del Responsabile della Protezione dei Dati e delle professionalità coinvolte.

5.3 Gestione del *data breach* esterno alla struttura

Ogni Responsabile esterno del trattamento (Fornitore/Ditta) – incaricato dal Titolare ad effettuare attività di trattamento dati in nome e per suo conto sulla base di specifico contratto a tal fine stipulato tra le parti – qualora venga a conoscenza di un potenziale caso di *data breach*, ne dà avviso senza ingiustificato ritardo all'Azienda Ospedaliera, inviando alla stessa una comunicazione a mezzo PEC all'indirizzo

aomarchenord@emarche.it e utilizzando a tal fine l'allegato modulo (MOD02_IOdgenT003_ORG) che dovrà, pertanto, essere accluso all'atto di nomina stesso.

Per ingiustificato ritardo è da considerarsi la notizia pervenuta al Titolare del trattamento non oltre le 48 ore dalla presa di conoscenza iniziale da parte dello stesso Responsabile esterno.

Il RPD effettua a sua volta una valutazione dell'evento avvalendosi del supporto e della collaborazione di professionalità interne all'Azienda Ospedaliera, necessarie per la corretta analisi di contesto, quali:

- Servizio Informatico
- Gruppo di supporto al RPD
- Direzione Medica dei Presidi
- Direttori/Responsabili di struttura coinvolti nell'evento.

A seguito delle determinazioni sul punto raggiunte e solo qualora si debba ritenere che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche interessate, il Responsabile della Protezione dei Dati – con lo specifico contributo delle professionalità coinvolte - supporta il Titolare del trattamento nella predisposizione della notificazione all'Autorità Garante. Detta notificazione deve essere inviata senza ingiustificato ritardo e, ove possibile, entro 72 ore da intendersi decorrenti dal momento in cui il Titolare sia venuto a conoscenza della violazione di dati, ovvero da quanto il Titolare abbia raggiunto un ragionevole grado di certezza sul fatto che l'incidente di sicurezza comporti una violazione di 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 di ulteriori indagini e verifiche sull'evento.
La scelta e le motivazioni che hanno condotto a non notificare l'evento devono risultare documentate a cura del Responsabile della Protezione dei Dati e delle professionalità coinvolte.

5.4 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 fisiche interessate, queste ultime devono essere informate senza ingiustificato ritardo al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali pregiudizi derivanti dalla violazione.
Il Responsabile della Protezione dei dati supporta il Titolare del trattamento nella predisposizione della comunicazione all'interessato/agli interessati, da inviarsi nei tempi e con le modalità che il Titolare stesso, sempre attraverso la funzione consulenziale del Responsabile della Protezione dei dati, individuerà come più opportuna anche tenendo conto di eventuali indicazioni all'uopo fornite dall'Autorità Garante. La comunicazione descriverà con linguaggio semplice e chiaro la natura della violazione dei dati personali, le probabili conseguenze derivanti dalla stessa, oltreché le relative misure individuate per porvi rimedio.

5.5 Registro delle violazioni

Presso l'Ufficio del Responsabile della Protezione dei dati è istituito il registro delle violazioni nell'ambito del quale vengono documentati tutti gli eventi di *data breach* occorsi presso l'Azienda Ospedaliera dall'entrata in vigore del GDPR e il cui aggiornamento avviene a cura del Responsabile della Protezione dei dati per conto del Titolare. A tal fine si allega alla presente istruzione relativo modello del predetto registro (MOD03_IOdgenT003_ORG).

6. ELENCO ALLEGATI

ALLEGATO N°	DESCRIZIONE ALLEGATO
MOD01_IOdgenT003 _ORG	Modulo per la segnalazione di un sospetto caso di *data breach*
MOD02_IOdgenT003 _ORG	Modulo per la segnalazione di un sospetto caso di *data breach* da parte di Responsabile esterno del trattamento (Fornitore/Ditta)
MOD03_IOdgenT003 _ORG	Registro delle violazioni