DETERMINA DEL DIRETTORE GENERALE

N. 841 /DG **DEL** 18 OTT. 2018

Oggetto: Approvazione della "procedura di gestione delle violazioni" (data breach) e schema "Registro delle violazioni" in attuazione del Regolamento UE 2016/679.

IL DIRETTORE GENERALE

- . - . -

VISTO il documento istruttorio, riportato in calce alla presente determina, dal quale si rileva la necessità di provvedere a quanto in oggetto specificato;

RITENUTO, per i motivi riportati nel predetto documento istruttorio e che vengono condivisi, di adottare il presente atto;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario, ciascuno per quanto di rispettiva competenza;

- D E T E R M I N A -

1. Adottare la "procedura aziendale di gestione della violazione" *(data breach)* e relativi allegati **(documento n. 1)**, che allegata al presente atto, ne costituisce parte integrante e sostanziale;

2. Adottare, lo schema di "Registro delle violazioni", che, allegato al presente atto **(documento n. 2)** ne costituisce parte integrante e sostanziale, in cui devono essere documentate tutte le violazioni riscontrate e che deve essere esibito, se richiesto, all'Autorità di controllo (Garante per la privacy) durante le attività ispettive;

3. Disporre la pubblicazione dei documenti allegati al presente provvedimento sul sito istituzionale *(www.ospedaliriuniti.marche.it – sezione privacy e note legali);*

4. Disporre, altresì, che i documenti di cui al precedente punto 3. possono essere oggetto di modifica senza necessità di ulteriori atti determinativi ma mediante mera pubblicazione

dell'allegato modificato sul medesimo sito, previa sua protocollazione e ferma restando la pubblicazione degli allegati precedentemente adottati nella sezione *"archivio modelli"*;

5. Dare atto che dall'adozione del presente provvedimento non deriveranno costi aggiuntivi a carico del bilancio aziendale;

6. Trasmettere il presente atto al Collegio Sindacale a norma dell'art. 17 della L.R. 26/96 e s.m.i.;

7. Dare atto che la presente determina non è soggetta al controllo della Giunta Regionale ai sensi dell'art. 4 della Legge 412/91 e dell'art. 28 della L.R. 26/96 e s.m.i. e diventerà esecutiva dalla data di pubblicazione all'albo pretorio dell'Azienda (art. 28, comma 6, L.R. 26/96 e s.m.i.).

Il Direttore della S.O. Direzione Amministrativa di Presidio e U.R.P. attesta la regolarità del presente atto e ne certifica la conformità alle disposizioni vigenti.

IL DIRETTORE S.O.
(Fabio Benni)

IL DIRETTORE GENERALE
(Michele Caporossi)

IL DIRETTORE AMMINISTRATIVO
(Antonello Maraldo)

IL DIRETTORE SANITARIO
(Alfredo Cordoni)
ASSENTE

- DOCUMENTO ISTRUTTORIO -
(SO Direzione Amministrativa di Presidio e URP)

Normativa di riferimento:

- Regolamento UE 2016/679, Regolamento generale sulla protezione dei dati;
- Guidelines on Personal data breach notification under Regulation 2016/679 (adopted on 3rd October 2017, as last Revised and Adopted on 6th February 2018);
- D. Lgs. 196/2003 così come modificato dal D. Lgs. 10 agosto 2018, n. 101

Motivazione

L'entrata in vigore del Regolamento UE 2016/679 ("Regolamento") ha determinato l'introduzione di alcune prescrizioni in capo al titolare del trattamento dei dati.

In particolare gli artt. 33 e 34 del Regolamento medesimo prescrivono l'obbligo di notificazione all'autorità di controllo (Garante per la privacy) della violazione di dati personali che comporti un rischio per i diritti e le libertà fondamentali dell'interessato e, qualora tale violazione presenti un rischio elevato, l'obbligo di comunicazione della violazione all'interessato medesimo.

Specifica infatti l'art. 33 del Regolamento, rubricato "*Notifica di una violazione dei dati personali all'autorità di controllo*", che "*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche[...]*".

Inoltre l'art. 34 del Regolamento, rubricato "*Comunicazione di una violazione di dati personali all'interessato*", chiarisce che la stessa debba essere effettuata "*Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo [...]*".

Il Regolamento precisa, altresì, all'art. 4 che per violazione dei dati personali deve intendersi "*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*".

Ritenuto che, nel disciplinare il principio di responsabilizzazione, l'art. 24 del Regolamento statuisce che *"[...] il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento"*

Pertanto risulta necessario – nel rispetto del suddetto principio e al fine di adeguarsi alle prescrizioni dettate al riguardo dal Regolamento in materia di violazione dei dati personali, innanzi citate - regolamentare le modalità di gestione di una violazione di dati personali mediante predisposizione di una "procedura aziendale di gestione della violazione" *(data breach).*

Inoltre, al fine di procedere all'obbligo di documentare la rilevazione di eventuali violazioni e la loro conservazione - così come prescritto dall'art. 33, comma 5, del Regolamento laddove afferma che *"[..]Il titolare del trattamento documenta qualsiasi violazione dei dati personali comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"* – risulta, altresì necessario predisporre un modello di "Registro delle violazioni" che sia atto a rilevare tali informazioni.

Per quanto sopra esposto, pertanto,

SI PROPONE

1. Adottare la "procedura aziendale di gestione della violazione" *(data breach)* e relativi allegati **(documento n. 1)**, che allegata al presente atto, ne costituisce parte integrante e sostanziale;

2. Adottare, lo schema di "Registro delle violazioni", che, allegato al presente atto **(documento n. 2)** ne costituisce parte integrante e sostanziale, in cui devono essere documentate tutte le violazioni riscontrate e che deve essere esibito, se richiesto, all'Autorità di controllo (Garante per la privacy) durante le attività ispettive;

3. Disporre la pubblicazione dei documenti allegati al presente provvedimento sul sito istituzionale *(www.ospedaliriuniti.marche.it – sezione privacy e note legali);*

4. Disporre, altresì, che i documenti di cui al precedente punto 3. possono essere oggetto di modifica senza necessità di ulteriori atti determinativi ma mediante mera pubblicazione dell'allegato modificato sul medesimo sito, previa sua protocollazione e ferma restando la pubblicazione degli allegati precedentemente adottati nella sezione *"archivio modelli"*;

Il Responsabile del procedimento
(Marianna Catalini)

Il Direttore S.O.
(Fabio Benni)

- ALLEGATI -

Documento n. 1: Procedura di gestione della violazione (data breach) e relativi allegati
Documento n. 2: Schema Registro delle violazioni

Azienda Ospedaliero Universitaria
OSPEDALI RIUNITI
Umberto I - G.M.Lancisi - G.Salesi
Ancona

PROCEDURA DATA BREACH

Con la presente procedura si intendono fornire le istruzioni necessarie a tutto il personale per le procedure da attivare in caso di violazione di dati personali.

Al riguardo si specifica che per violazione dei dati personali si intende 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.

Di seguito alcuni esempi di violazioni di sicurezza.

A) Distruzione: un insieme di dati personali che a seguito di incidente o azione fraudolenta non è più nella disponibilità del titolare, né di altri e qualora tali dati siano richiesti dall'interessato non possono essere forniti.

1. Incendio di archivi cartacei contenenti documentazione relativa a dati personali e in particolare documentazione sanitaria.

2. Guasto non riparabile dell'hard disk contenente un numero cospicuo di referti che in violazione al Regolamento europeo 679/2016 erano salvati solo localmente.

3. Distruzione di campioni biologici.

B) Perdita: un insieme di dati personali che a seguito di un incidente o azione fraudolenta non sono più nella disponibilità del titolare, ma di terzi non autorizzati e quindi qualora tali dati siano richiesti dall'interessato non sarebbe possibile produrli ed il terzo potrebbe essere in possesso del dato in modo illegittimo

1. Smarrimento supporto di memoria rimovibile.

2. Smarrimento documentazione contenente dati personali.

C) Modifica: un insieme di dati personali che a seguito di un incidente o azione fraudolenta è stato irreversibilmente modificato senza possibilità di rispristinare lo stato originale e in caso di richiesta da parte dell'interessato non sarebbe possibile produrlo con certezza che sia stato alterato

1. Guasto tecnico che altera parte di contenuti di un sistema clinico compromettendo anche i backup.

2. Azione involontaria o fraudolenta di chiunque che porti all'alterazione del dato in modo non tracciato e irreversibile.

C) Divulgazione non autorizzata: un insieme di dati personali che a seguito di un incidente o azione fraudolenta viene trasmesso a terzi senza il consenso dell'interessato o senza che ciò sia possibile sulla base delle disposizioni di legge e regolamentari

1. Trasmissione di dati personali ad opera del personale incaricato al trattamento a soggetti terzi non autorizzati a trattare il dato come ad esempio l'invio di referti a paziente diverso dall'interessato.

D) Accesso non autorizzato: un insieme di dati personali che sono messi a disposizione per un intervallo di tempo a persone non titolate a compiere quel trattamento specifico

1. Accesso alla rete aziendale ad opera di terzi.

2. Accesso a dati personali di altro paziente rispetto all'interessato per errore di profilazione.

3. Accesso a dati personali per i quali non si ha l'autorizzazione al trattamento.

E) Indisponibilità temporanea del dato: un insieme di dati personali che a seguito di un incidente o azione fraudolenta è non disponibile per un periodo di tempo che lede i diritti dell'interessato

1. Cancellazione accidentale di dati che non possono essere immediatamente ripristinati.

Gli esempi sopra indicati sono a titolo esemplificativo e non esaustivo, pertanto, in caso di dubbio circa il fatto se si è in presenza di una violazione o meno bisogna, comunque, seguire la procedura di seguito descritta.

PROCEDURA DI COMUNICAZIONE AL TITOLARE DEL TRATTAMENTO

Viene di seguito riportata la procedura da seguire:

1. Chiunque riscontri una violazione di dati personali come sopra specificata **comunica immediatamente** appena ne abbia conoscenza con qualsiasi mezzo (e-mail, telefono, a voce) la violazione di dati al Direttore della struttura organizzativa di appartenenza o, in caso di assenza, al suo sostituto e in caso di assenza di quest'ultimo al Direttore di Dipartimento.

2. Il Direttore della struttura organizzativa o colui che lo sostituisce e ha ricevuto la segnalazione **comunica** con qualsiasi mezzo (e-mail, telefono, a voce) la violazione non oltre le **12 (dodici) ore** da quando ne è venuto a conoscenza al Referente aziendale per la privacy.

3. Il Referente aziendale per la privacy informa il DPO e prende in carico la segnalazione, valuta se si tratta di violazione e, in caso positivo, acquisisce le informazioni relative alla violazione compilando "il modulo rilievo violazione" **(doc. n. 1)** che verrà sottoscritto dal Direttore della struttura (o dal suo sostituto e in caso di assenza di quest'ultimo dal Direttore di Dipartimento) che ha effettuato la segnalazione. Il Referente aziendale per la privacy, informa, altresì, il titolare e contestualmente, in presenza di violazione di dati che impattano sui sistemi informatici, il Direttore SIA o suo delegato.

4. Il DPO, ricevuta la segnalazione di cui al punto 3), esprime il proprio parere con eventuali prescrizioni.

5. In caso di violazione, il Referente aziendale per la privacy:

a) con la collaborazione del DPO e - in caso di violazione incidente su dati contenuti in un sistema informatico - del Direttore del SIA o di altri soggetti coinvolti avuto riguardo alla natura della violazione, procede all'analisi della violazione e alla valutazione dei rischi sulla base del modello allegato **(doc. n. 2)**;

b) in collaborazione con i soggetti coinvolti, individua le azioni correttive da compiersi e le misure tecnologiche ed organizzative ritenute necessarie a contenere gli effetti della violazione e ad evitare quelle future, sulla cui attuazione il DPO controlla;

c) iscrive, comunque, la violazione nel "Registro delle violazioni";

d) qualora le risultanze dell'analisi e della valutazione dei rischi di cui alla lettera a) mettano in evidenza che la violazione comporti **un rischio per i diritti e le libertà degli interessati,** provvede **entro 72 (settantadue) ore** dal momento in cui ne è venuto a conoscenza:

I) alla notifica al Garante per la privacy sulla base del modello allegato **(doc. n. 3)**;

II) alla comunicazione agli interessati **qualora la violazione dei dati presenti un rischio elevato** per i diritti e le libertà degli interessati sulla base del modello allegato **(doc. n. 4)**.

Qualora il numero degli interessati coinvolti sia particolarmente cospicuo il termine di 72 ore sopra indicato per la comunicazione agli interessati potrà essere prorogato per il tempo strettamente necessario ad adempiere.

Viene allegato al presente documento il modulo riassuntivo dei tempi e delle modalità della procedura data breach **(doc. n. 5)**.

Azienda Ospedaliero Universitaria
OSPEDALI RIUNITI
Umberto I - G.M.Lancisi - G.Salesi
Ancona

Si allegano:
Doc. n. 1: Modulo rilievo violazione
Doc. n. 2: Modulo di valutazione del rischio connesso al data breach
Doc. n. 3: Comunicazione al Garante per la privacy
Doc. n. 4: Comunicazione agli interessati
Doc. n. 5: Modulo riassuntivo dei tempi e delle modalità della procedura data breach

Doc. n. 1: Modulo rilievo violazione

Azienda Ospedaliero Universitaria
OSPEDALI RIUNITI
Umberto I - G.M.Lancisi - G.Salesi
Ancona

Data scoperta violazione	_____/_____/_____
Data dell'incidente (se individuabile)	_____/_____/_____
Luogo delle violazione (specificare la SO/SOD/SOSD)	
Responsabile della SO/SOD/SOSD in cui è avvenuta la violazione	
Responsabile del Dipartimento	
Nome della persona che ha riferito la violazione (indicare anche i dati di contatto)	☐ Interno _____ ☐ Esterno _____
Indicazione del trattamento oggetto del data breach e breve descrizione della violazione dei dati ivi trattati	_____ _____ _____ _____ _____
Indicare il tipo di dispositivo oggetto di violazione	☐ Computer (specificare se aziendale o personale)_____ ☐ Rete _____ ☐ Dispositivo mobile _____ ☐ File o parte di file _____ ☐ Strumento di back up_____ ☐ Documento cartaceo _____ ☐ Altro (specificare) _____
Indicare il tipo di dati che sono stati oggetto di violazione	☐ Dati anagrafici/codice fiscale_____ ☐ Dati di accesso/identificazione_____ ☐ Dati relativi a minori_____ ☐ Dati sensibili_____ ☐ Dati giudiziari _____ ☐ Altro (specificare)_____
Categoria e numero approssimativo di interessati coinvolti nella violazione:	
Descrizione di eventuali azioni poste in essere al momento della scoperta della violazione.	_____ _____ _____ _____

Il Direttore della SO/SOD/SOSD (o suo sostituto)

Doc. n. 2: Modulo di valutazione del rischio connesso al *data breach*

Azienda Ospedaliero Universitaria
OSPEDALI RIUNITI
Umberto I - G.M.Lancisi - G.Salesi
Ancona

Tipo di violazione dei dati	☐ Distruzione ☐ Perdita ☐ Modifica ☐ Divulgazione non autorizzata ☐ Accesso
Natura dei dati oggetto di violazione	☐ Dati sensibili ☐ Dati NON sensibili
Numero di soggetti interessati coinvolti	
Tipologia di soggetti interessati (ad esempio: minori, fragili,…)	
Descrizione delle misure tecniche ed organizzative in essere sul dato fino alla data della violazione	
Verifica circa l'esistenza del *back up* dei dati oggetto di violazione	☐ Dati NON sono stati oggetto di back up ☐ Dati sono stati oggetto di back up
Descrizione delle misure tecniche ed organizzative correttive adottate nell'immediatezza	
Descrizione dell'incidenza della violazione sui diritti e sulle libertà fondamentali (ad esempio: immagine, riservatezza, reputazione, incidenza su aspetti economici e sociali)	
Descrizione delle conseguenze della violazione sui soggetti interessati	
Probabilità che si verifichino situazioni dannose per l'interessato	☐ Nulla ☐ Bassa ☐ Media ☐ Alta

N.B. E' possibile ai fini dell'analisi e della valutazione del rischio allegare altra documentazione o altri elementi utile alla valutazione della specifica violazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 2 luglio 2015**, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: **databreach.pa@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Allegato 1

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro :

Allegato 1

Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di *backup*
- ☐ Documento cartaceo
- ☐ Altro :

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ N. _____ persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, 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 personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro :

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il

☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Doc. n. 4: Comunicazione agli interessati

Azienda Ospedaliero Universitaria
OSPEDALI RIUNITI
Umberto I - G.M.Lancisi - G.Salesi
Ancona

Gentile *<nome e cognome dell'interessato>*,

Con la presente Le comunichiamo che i suoi dati personali hanno subito la seguente violazione *(specificare la tipologia di violazione).*

In particolare è accaduto quanto di seguito descritto.

<descrizione sintetica della violazione in relazione alla quale si ritiene necessaria la comunicazione all'interessato ed indicazione dei dati personali violati>

Dall'analisi interna dei fatti sopra riportati, in considerazione della natura della violazione e della tipologia di dati personali coinvolti, riteniamo che le conseguenze di questa violazione per Lei dovrebbero consistere in *<descrizione sintetica delle conseguenze della violazione>*. Come previsto dall'art. 33 del Regolamento UE 2016/679 abbiamo già provveduto a notificare questa violazione al Garante Privacy.

Non appena siamo venuti a conoscenza dell'incidente abbiamo tempestivamente agito in modo tale da porre rimedio alla violazione dei dati personali anche, al fine ulteriore, di attenuare eventuali effetti negativi ponendo in essere le seguenti misure tecnico - organizzative:

< descrizione sintetica delle azioni intraprese per informare l'interessato sulle misure adottate>.

Potrà ricevere informazioni contattando il Responsabile della protezione dei dati (RDP) e/o il Responsabile aziendale per la privacy i cui dati di contatto sono reperibili sul sito istituzionale (www. ospedaliriuniti.marche.it – nella sezione privacy e note legali) e che vengono di seguito riportati:

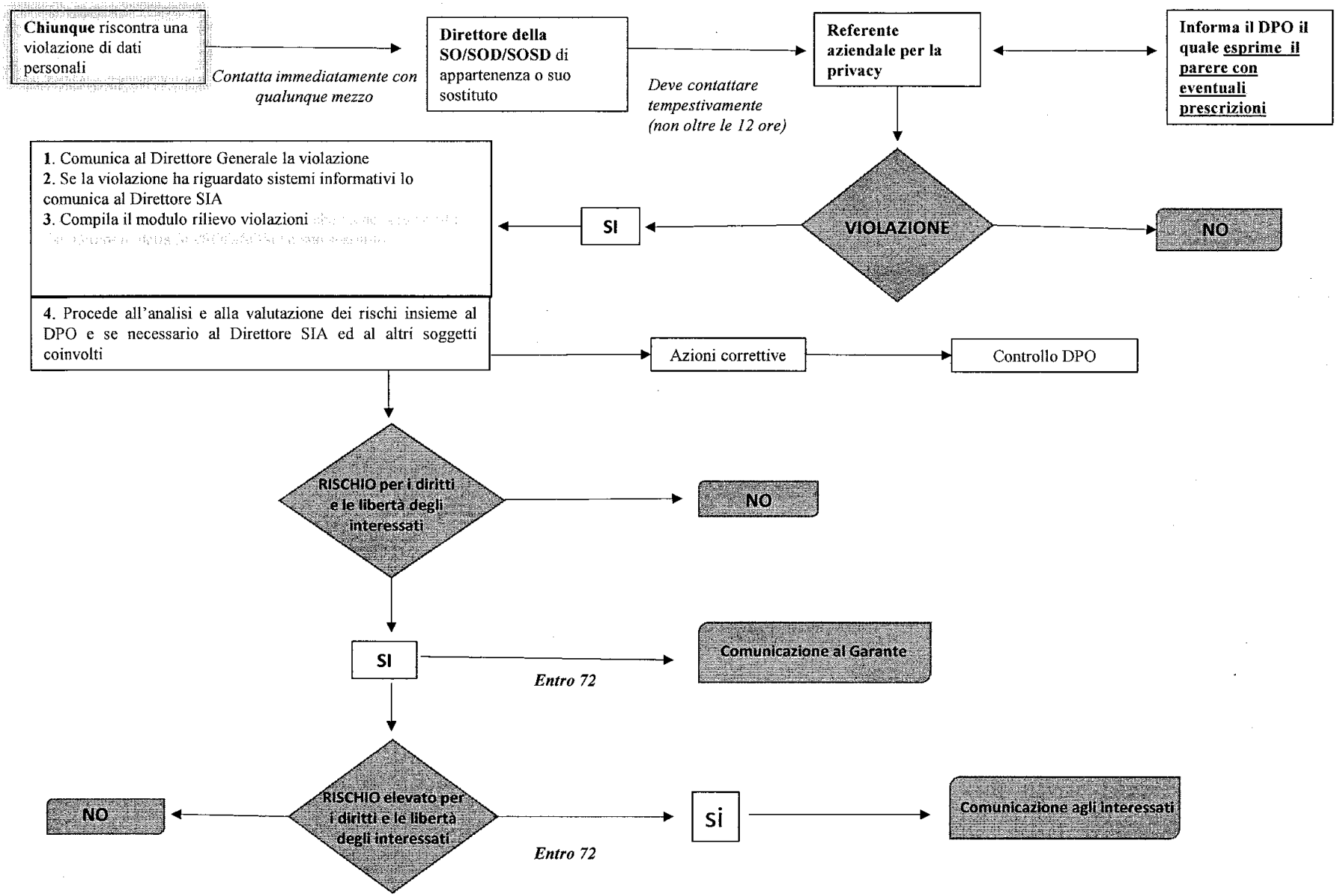
Responsabile per la protezione dei dati
e-mail: marianna.catalini@ospedaliriuniti.marche.it
telefono: 071/5965136

Referente aziendale per la privacy
e-mail: fabio.benni@ospedaliriuniti.marche.it
telefono. 071/5965657

Distinti saluti

Il Direttore Generale

PROCEDURA DATA BREACH



Protocollo della violazione (anno/numero progressivo)	**Data dell'incidente**	**Luogo delle violazione** (specificare la SO/SOD/SOSD)	**Responsabile della SO/SOD/SOSD in cui è avvenuta la violazione**	**Responsabile del Dipartimento**	**Protocollo del modello interno di comunicazione**	**Nome della persona che ha riferito la violazione** (indicare anche i dati di contatto e specificare se soggetto interno o esterno)	**Indicazione del trattamento oggetto del data breach e breve descrizione della violazione dei dati ivi trattati**	**Indicare il tipo di dispositivo oggetto di violazione**	**Indicare il tipo di dati che sono stati oggetto di violazione**	**Categoria di interessati coinvolti nella violazione**	**Numero approssimativo di interessati coinvolti nella violazione**	**Descrizione delle misure tecniche ed organizzative poste in essere prima della violazione**	**Descrizione di eventuali misure tecniche ed organizzative poste in essere al momento della scoperta della violazione.**	**Data notifica al Garante** ("n.d." se mancante)	**Data comunicazione agli interessati** ("n.d." se mancante)
xxxx/xx								Altro							

CERTIFICATO DI PUBBLICAZIONE

La determina n. 841/DG del 18-10-2018 viene pubblicata all'Albo Pretorio Informatico dell'Azienda Ospedaliera "Azienda Ospedali Riuniti Umberto I – G.M. Lancisi – G. Salesi" il 18 OTT. 2018 ai sensi dell'art. 32, c. 1, Legge n. 69/2009, ove rimarrà per 15 giorni consecutivi.

IL DIRIGENTE RESPONSABILE
Silvana Giorgioni

COLLEGIO SINDACALE

La presente determina è stata inviata al Collegio Sindacale con nota n. 70604 del 18 OTT. 2018.

REGIONE MARCHE

La presente determina, soggetta a controllo preventivo ai sensi dell'art. 28 della L.R. n. 26/1996 e s.m.i., è stata inviata alla Giunta Regionale delle Marche con nota n. _____ del _____ e da questa ricevuta in data _____.

ESECUTIVITA'

La presente determina:

- [x] è stata dichiarata esecutiva ai sensi dell'art. 28, sesto comma, della L.R. n. 26/1996 e s.m.i..
- [ ] è stata (approvata/annullata parzialmente/annullata) dalla Giunta Regionale delle Marche con deliberazione n. _____ del _____.

IL DIRIGENTE RESPONSABILE
Silvana Giorgioni

CERTIFICATO DI CONFORMITA' ALL'ORIGINALE

La presente copia composta da n. _____ pagine è conforme all'originale esistente agli atti di questa Azienda Ospedaliera.

Ancona, _____

IL DIRIGENTE RESPONSABILE