DETERMINA DEL DIRETTORE DELLA AREA VASTA N. 5 N. 680/AV5 DEL 19/05/2017

Oggetto: Individuazione e nomina responsabili del trattamento dei dati in attuazione del DPCM n.178 del 29 settembre 2015 "Regolamento in materia di fascicolo sanitario elettronico" e del Decreto Legislativo 30 giugno 2003 n.196 e s.m.i.

IL DIRETTORE DELLA AREA VASTA N. 5

- . - . -

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;
VISTA l'attestazione del Dirigente/Responsabile della Ragioneria/Bilancio in riferimento al bilancio annuale di previsione.

- D E T E R M I N A -

1. Di nominare quali Responsabili dei trattamenti dei dati personali - sanitari contenuti nel Fascicolo Sanitario Elettronico, i Direttori medici di Dipartimento e i Dirigenti/Direttori medici delle Unità Operative semplici e complesse, individuati con Determina n.226/AV5 del 28/02/2014, Determina n.1299/AV5 del 29/11/2016, ovvero da individuarsi ad esito del completamento delle procedure di attribuzione degli incarichi dirigenziali ai sensi della Determina ASUR n.481/2016 e s.m.i. secondo le disposizioni di cui agli art.6 e 7 del Regolamento Organizzativo Privacy dell'ASUR, e delle disposizioni relative al Fascicolo Sanitario Elettronico, adottando l'allegato schema di nomina e accettazione (All.1).

2. Di dare atto che i Responsabili di cui al Punto 1) procedono alla identificazione e alla nomina, nelle proprie strutture, degli Incaricati al trattamento dei dati personali, secondo le disposizioni di cui all'art.9 Regolamento Organizzativo Privacy dell'ASUR, adottando l'allegato schema di nomina e accettazione (All.2).

3. Di dare mandato al Responsabile privacy in AV5 di procedere con gli adempimenti di conseguenti e necessari derivanti dal presente provvedimento.

4. Di dare atto che dal presente provvedimento non derivano oneri di spesa a carico del bilancio dell'ASUR – AV5.

5. Di dare atto che, a norma dell'art.28 c.6 della L.R. 26/96, così come modificata ai sensi dell'art.1 dalla L.R. 36/2013, il provvedimento diventa efficace dal giorno della pubblicazione nell'albo pretorio informatico di questa Area Vasta.

6. Di trasmettere la presente determina al Collegio Sindacale a norma dell'art.17 della L.R. 26/96 e s.m.i.

7. Di dare atto che la presente determina non è sottoposta a controllo ai sensi dell'art.4 della Legge 412/91 e dell'art. 28 della L.R.26/96 e s.m.i.

IL DIRETTORE AREA VASTA 5
(Avv. Giulietta Capocasa)

Per il parere infrascritto:

RAGIONERIA, BILANCIO E CONTROLLO DI GESTIONE
I sottoscritti, viste le motivazioni espresse nel documento istruttorio e la dichiarazione del Direttore di UOC, attestano che dall'adozione del presente atto non derivano oneri economici a carico del budget dell'Area Vasta 5.

Il Dirigente U.O.C
Controllo di gestione
(Dott. Alessandro Ianniello)

Il Dirigente f.f.
U.O.C Attività Economico - Finanziarie
(Dott. Cesare Milani)

La presente determina consta di n.13 pagine di cui n.8 pagine di allegati che formano parte integrante della stessa.

- DOCUMENTO ISTRUTTORIO -

U.O.C. SEGRETERIA DI DIREZIONE ARCHIVIO E PROTOCOLLO

Normativa:

- Decreto Legge 179 del 18 ottobre 2012 art. 12 "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario" convertito in Legge n. 221 del 7 dicembre 2012;
- DPCM n.178 del 29/09/2015 recante "Regolamento in materia di fascicolo sanitario elettronico";
- D.Lgs. 30 giugno 2003 n. 196, recante "Codice in materia di protezione dei dati personali" e ss.mm.ii.;
- Decreto del Dirigente Servizio Sanità n.1 del 6 febbraio 2017 avente per oggetto "Fascicolo Sanitario Elettronico - Consenso dei cittadini - formalizzazione modulistica e procedure per la raccolta";
- Regolamento Regionale 4 Gennaio 2007 n.1, recante "Regolamento per il trattamento di dati sensibili e giudiziari della Giunta regionale, delle Aziende del servizio sanitario regionale, degli Enti e delle Agenzie regionali e degli altri Enti controllati e vigilati dalla Regione in attuazione del decreto legislativo 30 giugno 2003, n. 196 (articolo 20, comma 2, e articolo 21, comma 2)" (B.U.R. 18 gennaio 2007 n. 6);
- Provvedimenti dell'Autorità Garante per la Protezione dei dati personali;
- Legge Regionale 20 giugno 2003 n.13, recante "Riorganizzazione del Servizio Sanitario Regionale" e ss. mm. ii.;
- Determina n.148/ASURDG del 14/02/2013: "Approvazione nuovo "Regolamento organizzativo Privacy", in attuazione del Decreto Legislativo 30 giugno 2003 n. 196 e ss.mm.ii.";
- Determina n.481/ASURDG del 02/08/2016 "Ridefinizione dell'assetto organizzativo aziendale";
- Determina n.705/ASURDG del 18/09/2013: "Strutture complesse Area territoriale – determinazioni"

Motivazione:

Con Decreto Legge 179 del 18 ottobre 2012, art.12 *"Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario"*, convertito in Legge n. 221 del 7 dicembre 2012, è stato istituito il Fascicolo Sanitario Elettronico, che è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario, generati da eventi clinici presenti e trascorsi, riguardanti l'assistito.

Con D.P.C.M. n.178 del 29/09/2015 recante "Regolamento in materia di fascicolo sanitario elettronico", è stato disciplinato il Fascicolo Sanitario Elettronico, che per quanto concerne la titolarità e il trattamento dei dati e la loro conservazione fa riferimento alle norme contenute nel Decreto Legislativo n. 196/03 - "Codice in materia di protezione dei dati personali".

Il D.G. ASUR ha approvato, con Determina n.148 del 14/02/2013, il nuovo "Regolamento organizzativo Privacy" dell'Azienda Sanitaria Unica Regionale delle Marche, che ha sostituito il precedente Regolamento di cui alla determina n. 531/DG del 14.7.2006.

Con Determina n.481/DGASUR del 02/08/2016 (successivamente rettificata, per correzione di mero errore materiale, con la successiva Determina n.486 del 04/08/2016), la Direzione Generale ASUR ha apportato modifiche alla propria precedente Determina n.350 del 14/5/2015, adottando il nuovo modello organizzativo aziendale in attuazione del percorso di revisione delle reti cliniche della Regione Marche. Con la citata Determina n.481/2016, la Direzione Generale ASUR ha definito l'organigramma delle strutture complesse, semplici dipartimentali e strutture semplici delle varie Aree Vaste.

Con Determina del Direttore di Area Vasta n.1299 del 29/11/2016 si prendeva atto della Determina n.481/DG del 02/08/2016 (con le rettifiche di cui alla Determina ASUR n.486 del 04/08/2016) con la quale è stato definito il nuovo assetto organizzativo aziendale con peculiare riferimento, per quanto di specifico interesse della Area

Vasta 5, all'individuazione dei Dipartimenti, delle strutture complesse e semplici anche a valenza dipartimentale individuate nell'Allegato e) al citato provvedimento

Alla luce del D.L. n.179 del 18 ottobre 2012 art.12 "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario" convertito in Legge n.221 del 7 dicembre 2012, del D.P.C.M 178 del 29/09/2015 recante "*Regolamento in materia di fascicolo sanitario elettronico",* del D.Lgs. 30 giugno 2003 n.196, recante "*Codice in materia di protezione dei dati personali*" e s.m.i.; del Decreto del Dirigente Servizio Sanità n.1 del 6 febbraio 2017 avente per oggetto "*Fascicolo Sanitario Elettronico - Consenso dei cittadini - formalizzazione modulistica e procedure per la raccolta"* nonché dei provvedimenti riorganizzativi citati, è necessario procedere, all'interno dell'AV5, alla nomina dei nuovi Responsabili medici dei trattamenti dei dati personali - sanitari contenuti nel F.S.E.

Rilevato che il vigente Regolamento Organizzativo Privacy ASUR all'art.7, prevede che gli stessi siano "*individuati tra soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Di regola, vengono nominati Responsabili del trattamento dei dati i Dirigenti/Direttori delle Unità Operative semplici e complesse e, nei casi in cui manchi la figura dirigenziale, il Coordinatore/Titolare di Posizione Organizzativa"*.

Per quanto sopra e sulla base dell'assetto organizzativo in essere nell'AV5, si ritiene opportuno designare quali Responsabili medici dei trattamenti dei dati personali - sanitari, contenuti nel Fascicolo Sanitario Elettronico, i Direttori medici di Dipartimento e i Dirigenti/Direttori medici delle Unità Operative semplici e complesse individuati con Determina n.226/AV5 del 28/02/2014, Determina n.1299/AV5 del 29/11/2016, ovvero da individuarsi ad esito del completamento delle procedure di attribuzione degli incarichi dirigenziali ai sensi della Determina ASUR n.481/2016 e s.m.i. secondo le disposizioni di cui agli art.6 e 7 del Regolamento Organizzativo Privacy dell'ASUR, e delle disposizioni relative al Fascicolo Sanitario Elettronico, adottando l'allegato schema di nomina e accettazione (All.1).

Successivamente i Responsabili procedono ad identificare e nominare, all'interno delle proprie strutture, gli Incaricati al trattamento dei dati personali **-** sanitari contenuti nel F.S.E. secondo le disposizioni di cui all'art.9 del Regolamento Organizzativo Privacy dell'ASUR, adottando l'allegato schema di nomina e accettazione (All.2).
Per le considerazioni sopra esposte

SI PROPONE

1. Di nominare quali Responsabili dei trattamenti dei dati personali - sanitari contenuti nel Fascicolo Sanitario Elettronico, i Direttori medici di Dipartimento e i Dirigenti/Direttori medici delle Unità Operative semplici e complesse, individuati con Determina n.226/AV5 del 28/02/2014, Determina n.1299/AV5 del 29/11/2016, ovvero da individuarsi ad esito del completamento delle procedure di attribuzione degli incarichi dirigenziali ai sensi della Determina ASUR n.481/2016 e s.m.i. secondo le disposizioni di cui agli art.6 e 7 del Regolamento Organizzativo Privacy dell'ASUR, e delle disposizioni relative al Fascicolo Sanitario Elettronico, adottando l'allegato schema di nomina e accettazione (All.1).

2. Di dare atto che i Responsabili di cui al Punto 1) procedono alla identificazione e alla nomina, nelle proprie strutture, degli Incaricati al trattamento dei dati personali, secondo le disposizioni di cui all'art.9 Regolamento Organizzativo Privacy dell'ASUR, adottando l'allegato schema di nomina e accettazione (All.2).

3. Di dare mandato al Responsabile privacy in AV5 di procedere con gli adempimenti di conseguenti e necessari derivanti dal presente provvedimento.

4. Di dare atto che dal presente provvedimento non derivano oneri di spesa a carico del bilancio dell'ASUR – AV5.

5. Di dare atto che, a norma dell'art.28 c.6 della L.R. 26/96, così come modificata ai sensi dell'art.1 dalla L.R. 36/2013, il provvedimento diventa efficace dal giorno della pubblicazione nell'albo pretorio informatico di questa Area Vasta.

6. Di trasmettere la presente determina al Collegio Sindacale a norma dell'art.17 della L.R. 26/96 e s.m.i.

7. Di dare atto che la presente determina non è sottoposta a controllo ai sensi dell'art.4 della Legge 412/91 e dell'art. 28 della L.R. 26/96 e s.m.i.

Il Responsabile del Procedimento
P.O. Privacy in AV5
(Dott. Antonio del Duca)

IL DIRIGENTE DELL'U.O.C SEGRETERIA DI DIREZIONE ARCHIVIO E PROTOCOLLO
Il sottoscritto attesta la regolarità tecnica e la legittimità del presente provvedimento e ne propone l'adozione al Direttore di Area Vasta.

Il Direttore U.O.C
Segreteria di Direzione Archivio e Protocollo
(Dott. Marco Ojetti)

- ALLEGATI -

Allegato 1 – atto di nomina del Responsabile trattamento dati FSE;
Allegato 2 – atto di nomina ad Incaricato trattamento dati FSE.

Allegato 1

ATTO DI NOMINA

a RESPONSABILE del trattamento dei dati personali e sanitari contenuti nel fascicolo sanitario elettronico presso il Dipartimento/U.O.C./U.O.S./U.O.S. dipartimentale ai sensi del Decreto Legge 179 del 18 ottobre 2012 art.12 "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario" convertito in legge n.221 del 7 dicembre 2012, del DPCM n.178 del 29/09/2015 recante "Regolamento in materia di fascicolo sanitario elettronico"; del vigente Regolamento Organizzativo Privacy ASUR e dell'art. 29 del Codice in materia di protezione dei dati personali (D.Lgs.196/2003) e relativi compiti.

L'Azienda Sanitaria Unica Regionale (ASUR), con sede legale in Via Oberdan n. 2 — 60122 Ancona — c.f. e Partita IVA:02175860424, titolare del trattamento dei dati personali e sanitari del Fascicolo Sanitario Elettronico, ai sensi del DPCM n. 178 del 29/09/2015 e dell'art.4 comma l lett. F) del D.Lgs.n.196/2003, nella persona del legale rappresentante p.t., Direttore Generale, Dott. Alessandro Marini, domiciliato per la carica presso la sede dell'Ente medesimo, che delega l'Avv. Giulietta Capocasa, Direttore della sede operativa Area Vasta 5, sulla scorta dell'art.6 del Regolamento Organizzativo Privacy ASUR, ad agire in nome e per conto dell'ASUR,

RITENUTO CHE

per l'ambito di attribuzioni, funzioni e competenze conferite sulla base del vigente assetto organizzativo di questa Area Vasta, la S.V. abbia i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali — sanitari contenuti nel Fascicolo Sanitario Elettronico, ivi compreso il profilo relativo alla sicurezza;

con il presente atto

NOMINA

Il Dott. _____

in qualità di _____ _____

(Direttore di Dipartimento/Dirigente/Responsabile della U.O.C./U.O.S.)

RESPONSABILE DEL TRATTAMENTO DATI F.S.E.

in relazione ai trattamenti di DATI PERSONALI E DATI SENSIBILI effettuati dal medesimo e dal personale assegnato all'Unità Operativa gestita.

In attuazione di quanto previsto dall'art.29 del Codice in materia di trattamento dei dati personali, si forniscono le seguenti indicazioni:

Il Responsabile del trattamento dei dati ha il dovere di compiere tutto quanto è necessario per il rispetto delle disposizioni normative vigenti in materia e del Regolamento organizzativo privacy ASUR di cui alla determina n.148 del 14/02/2013.

ln particolare, il Responsabile del trattamento dei dati deve:

- attenersi ai principi dettati dall'art.11 del Codice per la Privacy in ordine alle modalità di trattamento e di requisiti dei dati;
- assicurare il rispetto delle misure minime di sicurezza previste dal Codice Privacy (artt. 33, 34, 35 e 36; e allegato B "Disciplinare tecnico in materia di misure minime di sicurezza") (vedi allegato);
- attenersi alle istruzioni impartite dal Titolare e osservare e far osservare le misure precauzionali e quelle che si rendano necessarie sulla base di valutazioni di buon senso, nonché di rispetto della dignità e della libertà delle persone;
- **nominare formalmente come incaricati** le persone fisiche (dipendenti dell'Azienda, soggetti con incarico libero professionale ai sensi dell'art.7 del D.Lgs 165/2001, soggetti ammessi allo svolgimento del tirocinio o della frequenza volontaria o che fruiscono di istituti similari) che nell'ambito dei trattamenti aziendali di sua diretta competenza effettuano operazioni di trattamento dei dati personali e sanitari contenuti nel F.S.E.; impartire loro le istruzioni idonee alle attività da svolgere e vigilare sul loro operato;
- elaborare un piano di formazione destinato agli Incaricati, con il supporto della U.O.C. Sistemi Informativi;
- assicurarsi che ad ogni incaricato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato, eventualmente associato a un codice identificativo o a una parola chiave;
- prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso ed uso esclusivo dell'incaricato;
- assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri Incaricati, neppure in tempi diversi;
- assicurare che sia operata la cancellazione del codice identificativo personale in caso venga a cessare la necessità di accesso da parte dell'Incaricato o intervenga un'inattività per più di sei mesi;
- prevedere, con criteri restrittivi, profili di autorizzazione di accesso per ogni singolo Incaricato o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti;
- verif¡care, ad intervalli almeno annuali, le autorizzazioni in essere;
- richiedere all'UOC. Sistemi Informativi che sugli elaboratori vengano installati idonei programmi contro il rischio di intrusione e accesso abusivo in accordo ai requisiti di legge da aggiornare comunque ogni sei mesi ed in occasione di ogni versione disponibile dalla casa costruttrice; inoltre inviare la segnalazione della presenza di vulnerabilità nei programmi utilizzati e, richiederne l'aggiornamento;

  Inoltre per il trattamento di dati sensibili, cioè quelli di cui al art.4 comma d) del D.Lgs. 196/2003, il Responsabile deve vigilare che l'eventuale memorizzazione dei dati sensibili su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'interessato, ovvero

---

Art.11 D. Lgs. 196/2003 (Modalità del trattamento e requisiti dei dati)

1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
2. 1 dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

che la memorizzazione dci dati sensibili sia cifrata o in alternativa che vi sia separazione tra i dati sensibili e gli altri dati personali che possano permettere l'identificazione dell'interessato;

E' fatto assoluto divieto, al Responsabile designato, della diffusione dci dati, della comunicazione non autorizzata a terzi e più in generale è fatto divieto di effettuare trattamenti non finalizzati all'esecuzione delle attività affidate.

Si precisa inoltre che:

a) è vietata la diffusione dei dati idonei a rivelare lo stato di salute;
b) il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza. Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dci dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile e) l'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega, lo stesso decade automaticamente alla scadenza o alla revoca dell'incarico di direzione/ responsabilità, di struttura affidato.

Per quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

L'ASUR-AREA Vasta 5
(Titolare del trattamento)

Luogo data _____

Per accettazione
II Direttore del Dipartimento/Dirigente Responsabile della U.O.C./U.O.S. _____

Dott./Dott.ssa

_____
(firma e timbro)

Allegati: artt. 33, 34. 35 e 36 del Codice Privacy e allegato B del codice Privacy "Disciplinare tecnico in materia di misure minime di sicurezza")

ESTRATTO DAL CODICE in MATERIA DI PROTEZIONE DEI DATI PERSONALI (Decreto legislativo 30 giugno 2003, n. 196 –Codice Privacy)

Capo II - Misure minime di sicurezza

Art. 33. Misure minime

Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1, Il trattamento di dati personali effettuato con strumenti elettronici è consentilo solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misuro minime;

a) autenticazione informatica:
b) adozione dl procedure di gestione dette credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'Individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici:
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti Illeciti dl dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) [soppressa];
h) adozione di tecniche di cifratura o di codici Identificativi per determinati trattamenti dl dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

1 –bis abrogato

1-ter. Ai fini dell'applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e pre-contrattuali, alla gestione del rapporto di lavoro In tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale - assistenziale, di salute, igiene e sicurezza sul lavoro.

Art.35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici é consentito solo se sono adottate, noi modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia dl arti e documenti affidati egli incaricati per lo svolgimento dei relativi compiti;
c) previsione dl procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzala all'Identificazione degli incaricati.

Art.36. Adeguamento

1. Il disciplinare tecnico dl cui all'allegato El), relativo alle misure minime di cui al presente capo, é aggiornato periodicamente con decreto del Ministro della giustizia dl concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli Incaricali dotati di credenziali di autenticazione che consentano Il superamento dl una procedura di autenticazione relativa a uno specifico franamento o a un Insieme di trattamenti,
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associalo a una parola chiave riservala conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure In una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricate sono assegnalo o associale individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricali ò prescritto di adottare lo necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando é prevista dal sistema di autenticazione, é composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pa[p]i al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'Incaricato ed *è* modificata da quest'ultimo al primo utilizzo e, successivamente*,* almeno ogni sei mesi. In caso dl trattamento di dati sensibili o dl dati giudiziari la parola chiave ò modificata almeno ogni tre mesi.
6. Il codice per l'Identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Lo credenziali dl autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi dl gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono Impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso al dati e agli strumenti elettronici e consentito esclusivamente mediante uso delle componente riservata della *credenziale* per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente lo modalità con lo quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali é organizzata garantendo la relativa segretezza e Individuando preventivamente per iscritto I soggetti Incaricali della loro custodia, I quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non Si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione
12. Quando per gli Incaricati sono individuati profili dl autorizzazione di ambito diverso é utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee dl incaricati, sono individuati o configurati anteriormente all'Inizio dei trattamento, in modo de limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, *e* comunque almeno annualmente, é verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza
15. Nell'ambito dell'aggiornamento periodico cori cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentilo ai singoli Incaricati o addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee dl incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi dl cui all'art.*615- quinquies del* codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento é almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono Il salvataggio del dati con frequenza almeno settimanale,

Documento programmatico sulla sicurezza

19. [soppresso]

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art.615-ter del codice penale, mediante l'utilizzo di Idonei strumenti elettronici,
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzali e trattamenti non consentiti,
22. I supporti rimovibile contenenti dati sensibili o giudiziari se non utilizzato sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idoneo misure per garantire Il ripristino dell'accesso al dati In caso di danneggiamento degli stessi ig degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche dl dati con le modalità dl cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri Bali personali che permettono di Identificare direttamente gli Interessati, I dati relativi all'identità genetica sono trattali esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzali ad accedervi; il trasporlo dei dati all'esterno del locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico à cifralo.

Misure di tutela e garanzia
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'Intervento effettualo che ne attesta la conformità alte disposizioni del presente disciplinare tecnico.
26. [soppresso]

Trattamenti senza l'ausilio di strumenti elettronici
Modalità tecniche da adottare a cura del titolare*,* del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricali sono Impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'Individuazione dell'ambito del trattamento consentito ai singoli incaricali, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione,
28. Quando gli atti *e i* documenti contenenti dati personali sensibili o giudiziari sono affidati agli Incaricati del trattamento per lo svolgimento del relativi

compiti, i medesimi alti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione In maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine Mie operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllalo. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono Identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzale.

Allegato 2

ATTO DI NOMINA

ad INCARICATO/A del trattamento dati personali e sanitari contenuti nel Fascicolo Sanitario Elettronico presso il Dipartimento/U.O.C./U.O.S./U.O.S. dipartimentale

---

ai sensi del Decreto Legge 179 del 18 ottobre 2012 art.12 "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario" convertito in legge n. 221 del 7 dicembre 2012, del DPCM n. 178 del 29/09/2015 recante "Regolamento in materia di fascicolo sanitario elettronico"; dell'art.30 del D.Lgs n.196/2003 "Codice in materia di protezione dei dati personali" e del vigente Regolamento Organizzativo Privacy ASUR.

Il/La sottoscritto/a Direttore del dipartimento, della U.O.C./U.O.S./U.O.S. Dipartimentale nella sua qualità di Responsabile del trattamento dati, giusta nomina ai sensi del Decreto Legge n.179 del 18 ottobre 2012, art.12 "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario", convertito in Legge n.221 del 7 dicembre 2012, del DPCM n. 178 del 29/09/2015 recante "Regolamento in materia di fascicolo sanitario elettronico"; dell'art.29 del D.Lgs.n.196/2003 e del Regolamento Organizzativo Privacy ASUR ex Determina DG/ASUR n.148 del 14/02/2013, tenuto conto dei trattamenti dei dati personali –sanitari contenuti nel Fascicolo Sanitario Elettronico della propria struttura organizzativa

NOMINA

il/la destinatario/a della presente Incaricato/a ai sensi dell'art.30 del D. Lgs. n. 196/2003, e dell'art.1 lettera z) del DPCM n.178 del 29/09/2015 per i trattamenti relativi alla seguente attività come di seguito sintetizzata:_____
_____
_____
_____
i dati personali – sanitari contenuti nel Fascicolo Sanitario Elettronico che sono indispensabili per l'espletamento delle attività assegnate, con possibilità di reciproca sostituzione in ipotesi di più incaricati.
In ottemperanza del D.Lgs. n.196/2003 a ciascun incaricato è affidato il compito di:
1) trattare i dati personali c/o sensibili in modo lecito e secondo correttezza;
2) raccogliere i dati e registrarli per gli scopi inerenti l'attività svolta da ciascuno;

3) verificare, ove possibile, che i dati siano esatti e, se necessario, aggiornarli;
4) verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati, secondo le indicazioni ricevute dal Responsabile del trattamento;
5) conservare i dati nel rispetto delle misure di sicurezza previste dal D. Lgs.n. 196/2003 e dal Regolamento organizzativo privacy ASUR di cui alla Determina n.148 del 14/02/2013, consultabile sul sito aziendale;
6) adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ad uso esclusivo dell'incaricato.
7) non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
8) In caso di allontanamento, anche temporaneo, dal posto di lavoro, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti, di accedere a dati personali per i quali sia in corso un qualunque tipo di trattamento, sia cartaceo che informatizzato.
9) Nessun dato potrà essere comunicato a terzi o diffuso senza la preventiva autorizzazione del Responsabile del trattamento.
10) Per quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Responsabile del trattamento dei dati del
Fascicolo Sanitario Elettronico
Direttore/Responsabile UOC/UOS

_____
(Timbro e firma)

Luogo, data _____

Per presa visione e ricevuta copia:

_____
(Timbro e Firma)

Luogo, data _____