POLICLINICO DI **SANT'ORSOLA**

FRONTESPIZIO DELIBERAZIONE

AOO: AOPSO_BO

REGISTRO: Deliberazione

NUMERO: 0000265

DATA: 19/12/2018 19:11

OGGETTO: REGOLAMENTO (UE) 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI: RIDEFINIZIONE DEI PROFILI DI RESPONSABILITA' IN TEMA DI PROTEZIONE DEI DATI PERSONALI E NUOVE MODALITA' DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AD ESEGUIRE OPERAZIONI DI TRATTAMENTO DEI DATI PERSONALI (ORGANIGRAMMA DELLE RESPONSABILITÁ PRIVACY AZIENDALI).

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Messori Antonella in qualità di Direttore Generale
Con il parere favorevole di Spagnoli Gianbattista - Direttore Sanitario
Con il parere favorevole di Fornaciari Davide - Direttore Amministrativo

Su proposta di Luisa Capasso - ANTICORRUZIONE TRASPARENZA E RAPPORTI CON L'UNIVERSITA' che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [01-01]
- [07-03]

DESTINATARI:

- Collegio sindacale
- U.O. GASTROENTEROLOGIA - BAZZOLI
- U.O.ORTOPEDIA E TRAUMATOLOGIA-LAUS
- DIPARTIMENTO DELL' APPARATO DIGERENTE
- ANTICORRUZIONE TRASPARENZA E RAPPORTI CON L'UNIVERSITA'
- U.O.CHIRURGIA VASCOLARE - M.GARGIULO
- IGIENE E INFEZIONI OSPEDALIERE
- RICERCA ED INNOVAZIONE
- U.O.NEONATOLOGIA - FALDELLA
- UFFICIO RELAZIONI CON IL PUBBLICO E RAPPORTI CON LE ASSOCIAZIONI DI VOLONTARIATO

- INGEGNERIA CLINICA
- MEDICINA LEGALE E GESTIONE INTEGRATA DEL RISCHIO
- ACCESSO E NURSING NEI PERCORSI AMB. INT.
- U.O.CHIRURGIA PEDIATRICA - LIMA
- UFFICIO PRIVACY
- LOGISTICA SANITARIA - PERCORSO CHIRURGICO
- U.O.ANGIOLOGIA E MALATT.COAGULAZIONE
- SSD MALAT. INFIAMM.CRONICHE INT-CAMPIERI
- PROG.DIP.ANESTESIA T.I.TRAPIANTI ADD. E CHIRURGIA EPATOBIL.
- U.O.SEMEIOTICA MEDICA
- U.O.CHIRURGIA GENERALE - MINNI
- U.O.MEDICINA DEL LAVORO - VIOLANTE
- U.O.ANATOMIA ISTOL.PATOLOGICA D'ERRICO
- U.O.MALATTIE INFETTIVE - VIALE
- U.O.EMATOLOGIA - CAVO
- U.O.CENTRO RIF.TRAPIANTI SANGIORGI
- U.O.NEUROLOGIA
- U.O.MEDICINA D'URGENZA E P.S.- CAVAZZA
- U.O.GERIATRIA
- U.O.MEDICINA INTERNA - ZOLI
- U.O.CARDIOCHIRURGIA
- U.O.CARDIOL.PEDIAT.ETA' EVOLUTIVA
- U.O.ANESTESIOL.RIANIMAZ - FRASCAROLI
- U.O.CHIRURGIA TORACICA
- SSD ONCOLOGIA GINECOLOGICA - DE IACO
- U.O.MEDICINA INTERNA STANGHELLINI
- U.O.NEFROL.DIALISI E TRAPIANTO LA MANNA
- U.O.MICROBIOLOGIA - RE
- PROGR.DIP. CHIRURGIA IN URGENZA CERVELLERA
- U.O. ANESTESIOLOGIA E TERAPIA DEL DOLORE - MELOTTI
- U.O.CH.ORALE MAXILLO FACCIALE-MARCHETTI
- PROG.DIP.IMPLEMENTAZIONE E COORDINAMENTO DELL'INNOVAZIONE TERAPEUTICA NELLE EPATOPATIE CRONICHE VIRA
- U.O. GENETICA MEDICA - SERI
- PR.DIP.GEST.MAL.REUMATICHE E CONNETTIVO E MAL MET.OSSO
- U.O.UROLOGIA - BRUNOCILLA
- U.O.NEUROPSICHIATRIA INFANTILE
- U.O .PEDIATRIA - PESSION
- U.O.PEDIAT.D'URG. P.S. E OBI LANARI
- U.O.CARDIOLOGIA - RAPEZZI
- U.O.PNEUMOLOGIA T.I. RESP - NAVA
- U.O.MEDICINA NUCLEARE - FANTI
- DIPARTIMENTO TECNICO
- U.O.RADIOLOGIA
- DIPARTIMENTO DI ONCOLOGIA E DI EMATOLOGIA
- DIPARTIMENTO DELLA DONNA, DEL BAMBINO E DELLE MALATTIE UROLOGICHE

- DIPARTIMENTO CARDIO-TORACO-VASCOLARE
- SETTORE AMMINISTRATIVO DEL DIPARTIMENTO TECNICO
- SERVIZIO LEGALE ED ASSICURATIVO
- SERV. UNICO METR.AMMINISTR.DEL PERSONALE
- PROGETTAZIONE, SVILUPPO E INVESTIMENTI
- GESTIONE DEL PATRIMONIO
- PR.DIP.COORD.PER OGANIZZ.TECNOLOGICA DIP CARDIO TORACO VASC
- U.O.GERIATRIA - LUNARDELLI
- U.O.CHIR.GENERALE E DEI TRAPIANTI
- CENTRO LOGISTICO
- SERVIZI DI SUPPORTO ALLA PERSONA SETTORE TRASPORTI
- FARMACIA CLINICA
- SERVIZIO PREVENZIONE E PROTEZIONE AZIENDALE
- IGIENE OSPEDALIERA E PREVENZIONE MANONI
- CONTROLLO DI GESTIONE E SISTEMA INFORMATIVO
- ATTIVITA' LIBERO PROFESSIONALE E COORDINAMENTO DAI
- PROGR.PROGETTI UNIF.REVIS.RETI CLIN.INTEGRATE AREA SERVIZI
- SSD C.R.R.INSUF.INT.CRON.BENIGNA-PIRONI
- SSD GASTR.DIAG.TR. MAL.VIE BILIARI-FESTI
- FISICA SANITARIA
- U.O.EMOLINFOPATOLOGIA
- U.O.MEDICINA INTERNA - BOLONDI
- U.O.MEDICINA INTERNA - BORGHI
- U.O.MEDICINA FISICA E RIABILIT - TARICCO
- SSD ANDROLOGIA - COLOMBO
- SSD P.S. OSTETRICO GINEC. E OBI - MOLLO
- GOVERNO CLINICO, QUALITA', FORMAZIONE
- DIREZIONE DELLE PROFESSIONI SANITARIE
- COMUNICAZIONE E UFFICIO STAMPA
- PROGR.COORD.GEST.TECNOL.STRUM.E INFORMATICHE LUM
- GESTIONE DELLE RELAZIONI SINDACALI
- LOGISTICA SANITARIA - PERCORSI AMBULATORIALI INTEGRATI
- LOGISTICA SANITARIA - PERCORSO INTERNISTICO
- LOGISTICA SANITARIA - PERCORSO ALTA SPECIALITA' E TRAPIANTI D'ORGANO
- PROGR.LOGIST.SAN.PERCORSO MATERNO INFANTILE
- SSD ANESTESIOLOGIA
- U.O.CHIRURGIA GENERALE - TAFFURELLI SO
- SSD NEURORADIOL D.I.- PASTORE TROSSELLO
- ATTIVITA' GENERALI ED ISTITUZIONALI
- U.O.CHIRURGIA GENERALE - POGGIOLI
- U.O.CHIRURGIA PLASTICA - CIPRIANI
- PROGR DIP.ATT.WEEK SURGERY OSP.BUDRIO GRECO
- U.O. ANESTESIOL.TER.INT.POLIVAL- RANIERI
- SSD ONCOLOGIA MEDICA ADDARII - ZAMAGNI
- SSD DIAGN. IST.MOL.ORG.S./TRAP- D'ERRICO
- U.O.ANESTESIOL. RIANIMAZIONE - CARAMELLI

- DIPARTIMENTO DELLE INSUFFICIENZE D'ORGANO E DEI TRAPIANTI
- DIPARTIMENTO DELLA MEDICINA DIAGNOSTICA E DELLA PREVENZIONE
- PROG.DIP.CHIRURGIA PELVICA COMPL.CONCETTI
- U.O. RADIOLOGIA - GOLFIERI
- U.O.ENDOCRINOLOGIA - PAGOTTO
- SSD MAL.MET.DIET.CL-MARCHESINI REGGIANI
- DIPARTIMENTO DELL' EMERGENZA-URGENZA
- U.O.OSTETR.MED. ETA' PRENATALE - RIZZO
- DIPARTIMENTO TESTA, COLLO E ORGANI DI SENSO
- DIPARTIMENTO MEDICO DELLA CONTINUITA' ASSISTENZIALE E DELLE DISABILITA'
- PROGR.VALUTAZIONE DEL PERSONALE
- FUNZIONI TRASVERSALI DI DIREZIONE SANITARIA

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000265_2018_delibera_firmata.pdf	Capasso Luisa; Fornaciari Davide; Messori Antonella; Spagnoli Gianbattista	5D39884A8921EF7BE2C8F0E738668E4E D9FBB36630E1D264D4B31328F661A194
DELI0000265_2018_Allegato1.docx:		3818607553A4428A6233182835F7FC5AD DBC6701333A54C5BB0DF6E6E55B4D4A
DELI0000265_2018_Allegato2.docx:		B8B95460AFE691DF9C5E4FC56E35AA14 FB0C5485D99ABA8A5BA714A76273557B
DELI0000265_2018_Allegato3.docx:		78BD6ECF1FF568329E39B382BEC131167 3C72BA3F726EA443E0B21AEE6EAF30E

DELIBERAZIONE

OGGETTO: REGOLAMENTO (UE) 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI: RIDEFINIZIONE DEI PROFILI DI RESPONSABILITA' IN TEMA DI PROTEZIONE DEI DATI PERSONALI E NUOVE MODALITA' DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AD ESEGUIRE OPERAZIONI DI TRATTAMENTO DEI DATI PERSONALI (ORGANIGRAMMA DELLE RESPONSABILITÁ PRIVACY AZIENDALI).

IL DIRETTORE GENERALE

PREMESSO CHE:

- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (in seguito per brevità "GDPR"), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi sui diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure che ritiene a ciò più idonee ed opportune (c.d. principio di responsabilizzazione o *accountability*);

- il decreto legislativo n. 101 del 10.08.2018 recante Disposizioni per l' Adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo ha introdotto disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il Codice Privacy di cui al D. Lgs. 196/2003;

- il richiamato GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le Aziende Sanitarie;

- il "sistema privacy" delineato dal GDPR implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset informativo di un'organizzazione, con particolare attenzione ai dati di salute (ivi compresi i dati biometrici e genetici);

- tale nuovo approccio deve coinvolgere tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione aziendale, con assunzione delle relative responsabilità.

Richiamata la DGR Regione Emilia Romagna n. 919 del 10/4/2018 "Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l'anno 2018" che prevede fra gli obiettivi indicati al punto 4.6 dell'allegato B, oltre la nomina del DPO e l'adozione del registro delle attività di trattamento, la ri-definizione e l'articolazione delle specifiche responsabilità privacy aziendali.

Richiamata inoltre la Delibera n. 149 del 28.06.2018 di nomina del Data Protection Officer (DPO) dell'Azienda Ospedaliero Universitaria di Bologna Policlinico S. Orsola Malpighi che presso le varie Aziende svolge le seguenti attività:

- informa e fornisce consulenza alle Aziende/Enti, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Per il tramite dei referenti/responsabili privacy aziendali individuati dalle singole Aziende/Enti dovrà altresì assicurare attività di informazione/consulenza ai Responsabili del trattamento nonché ai dipendenti che, in qualità di autorizzati al trattamento, eseguono operazioni di trattamento dati;

- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti/responsabili privacy aziendali individuati dalle singole Aziende/Enti;

- fornisce, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

- coopera con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;

- supporta le strutture aziendali deputate alla tenuta del Registro del trattamento delle singole Aziende/Enti al fine di uniformarne la predisposizione;

- garantisce il corretto livello di interlocuzione con gli altri DPO delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE, ARA, GRU, GAAC);

- promuove iniziative congiunte tra le Aziende/Enti affinchè l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e cooerenti nelle singole Aziende/Enti;

- favorisce il coordinamento dei DPO delle altre aziende sanitarie regionali relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna, nota PG/2018/0482475 del 5 luglio 2018.

Considerato che in Azienda sono presenti:

- il Responsabile Privacy Aziendale, che garantisce e coordina le attività aziendali correlate alla normativa in materia di protezione dei dati personali supportando il Titolare del trattamento dei dati e il DPO negli adempimenti previsti dalla normativa,

- il Responsabile dell'Information & Communication Technology (ICT), che affianca il Responsabile Privacy nel supportare il Titolare del trattamento nel soddisfacimento dei requisiti posti dal GDPR sul sistema informativo (es. identificazione di adeguate misure tecniche ed organizzative, rispetto di quanto richiesto dall'AGID, ecc…), oltre che ad incentivare la diffusione della cultura digitale mediante la promozione di una maggiore attenzione ai temi della sicurezza informatica,

e sarà costituito il Gruppo Aziendale Privacy coordinato dal Responsabile Privacy Aziendale, che in attuazione dei principi di informazione e sensibilizzazione richiamati dal GDPR, ha il compito di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali. Il gruppo svolgerà le seguenti attività:

- supportare i Referenti Privacy nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Azienda a seguito degli approfondimenti e delle analisi effettuate dal coordinatore del GAP con il DPO nel Tavolo di area metropolitana;

- supportare i Referenti Privacy nell'aggiornamento del Registro dei trattamenti di dati personali effettuati dalle strutture di appartenenza e nella eventuale valutazione di impatto;

- fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO;

- coordinare le richieste di parere da sottoporre al DPO formulate dai singoli Referenti Privacy

Considerato che oltre al DPO, il GDPR - con riferimento ai soggetti - disciplina espressamente le figure del “titolare del trattamento” e del “responsabile del trattamento”, riferendosi con quest'ultima espressione ai soli soggetti esterni alla organizzazione che trattano dati personali per conto del titolare del trattamento.

Considerato altresì che:

- il medesimo GDPR pur non prevedendo più le figure del “responsabile [interno] del trattamento” e dell' "incaricato" del trattamento (come in precedenza individuati dagli artt. 29 e 30 del D. Lgs. 196/2003 - Codice Privacy), tuttavia non ne esclude la presenza all'interno di una organizzazione, in quanto introduce la categoria delle "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare [...]" (art. 4, n. 10);

- a sua volta, l'Autorità Garante per la protezione dei dati personali “ritiene opportuno che titolari [.....] del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni” (cfr. Guida all´applicazione del Regolamento europeo in materia di protezione dei dati personali).

Richiamato l’art. 4 del GDPR che definisce 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”.*

Rilevato che il titolare del trattamento, ai sensi dell’art. 32 del GDPR, tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Rilevato, inoltre, che gli artt. 29 e 32 del GDPR dispongono che chiunque agisca sotto l’autorità del titolare del trattamento e abbia accesso a dati personali possa trattare tali dati solo se adeguatamente istruito.

Ritenuto pertanto, alla luce delle premesse, delle novità introdotte dal GDPR e delle raccomandazioni del Garante Privacy sopra richiamate, di dover garantire continuità rispetto alle scelte organizzative negli anni assunte dalla Azienda, in ordine ai profili delle responsabilità e alla individuazione dei soggetti designati ad eseguire operazioni di trattamento, nel rispetto degli adempimenti previsti dalla normativa vigente, individuando una diversa modalità di designazione di tali soggetti, utilizzando altresì una terminologia in linea con il GDPR.

Richiamato l'art 97, commi 2 e 3 della Costituzione e ritenuto pertanto di designare all'interno della organizzazione, qualificati soggetti cui assegnare compiti e funzioni connessi al trattamento di dati personali, in continuità con il precedente organigramma privacy ove venivano nominati i "Responsabili (interni) del trattamento" ai sensi della deliberazione n. 115 del 15.03.2012 e successive integrazioni.

Ritenuto quindi, di designare quali Referenti Privacy i soggetti competenti al trattamento dei dati in considerazione della natura gestionale e della complessità delle strutture in termini di attività di trattamento dati e personale assegnato solo alcune figure già individuate nella deliberazione n. Delibera n. 115 del 15.03.2012 e successive integrazioni quali Responsabili (interni) di trattamento e, in relazione ai rispettivi ambiti di competenza, specificatamente:

- Direttori di Struttura Complessa
- Responsabili di Struttura Semplice Dipartimentale
- Responsabili di Programmi o altre strutture/articolazioni purchè con gestione di risorse

Stabilito che la designazione e nomina dei Referenti Privacy è conseguente all'assunzione/conferma degli incarichi di responsabilità come sopra specificati o all'assegnazione della funzione "ad interim" e di "facente funzioni", e che pertanto, tale atto reca in sé la nomina a Referenti Privacy, con specificazione circa i compiti/istruzioni assegnati (Allegato 1 - T03/IOS01).

Precisato inoltre che l'individuazione di soggetti Referenti privacy può rendersi necessaria anche per altri soggetti in virtù della particolarità organizzativa e funzionali delle attività di competenza e o della tipologia dei dati trattati (es. responsabili di strutture semplici).

Ritenuto inoltre, con riferimento specifico alle preesistenti figure degli "incaricati del trattamento", di superare l'attuale nomina "a cascata" ad personam, che prevedeva la designazione da parte del rispettivo "responsabile (interno) del trattamento", definendo d'ora innanzi di autorizzare al trattamento dei dati personali tutti i soggetti che operano sotto la diretta autorità del Titolare del trattamento, e quindi tutti i dipendenti/collaboratori/titolari di rapporto di lavoro autonomo e tutti i soggetti operanti stabilmente ad altro titolo nell'ambito delle strutture organizzative aziendali, compresi i medici in formazione specialistica, gli studenti di medicina e chirurgia nel periodo di tirocinio obbligatorio, i frequentatori volontari, i dottorandi e assegnisti di ricerca autorizzati all'attività di assistenza, ognuno per il proprio specifico ambito di competenza professionale, attribuendo loro la qualifica di personale autorizzato al trattamento dei dati (Autorizzati), con riferimento ai dati trattati nelle UO afferenti (complessa, semplice dipartimentale, o altra struttura individuata dal titolare) cui sono formalmente addetti come risultante del registro dei trattamenti e dalle funzioni attribuite all'UO/struttura/programma di apparenza, specifichiate nell'Atto Aziendale e nel relativo Regolamento Organizzativo Aziendale (ROA).

Ritenuto di comunicare tale autorizzazione al trattamento a tutti i dipendenti/collaboratori/titolari di rapporto di lavoro autonomo e quindi a tutti i soggetti operanti stabilmente ad altro titolo nell'ambito delle strutture aziendali, compresi i i medici in formazione specialistica, gli studenti di medicina e chirurgia nel periodo di tirocinio obbligatorio, i frequentatori volontari, i dottorandi e assegnisti di ricerca autorizzati all'attività di assistenza, attraverso la pubblicazione del predetto atto nell'area Privacy della intranet aziendale e all'interno del profilo personale del Portale del dipendente (GRU).

Precisato che, per i trattamenti di dati con procedura informatizzata l'attivazione delle credenziali di autenticazione informatica per il personale autorizzato di cui sopra resta in capo al Referente Privacy che deve specificare a quali dati e tipi di operazioni ciascun autorizzato può accedere in relazione ai propri compiti e la conseguente disattivazione in caso di cessazione dell'incarico.

Precisato invece che la nomina delle persone che devono essere volta per volta autorizzate al trattamento dei dati in quanto non stabilmente operanti all'interno delle strutture aziendali (a titolo di esempio non esaustivo ci si riferisce a lavoratori socialmente utili, volontari, tirocinanti diversamente inquadrati rispetto a quelli sopradescritti, ecc..) rimane ad personam ed in capo al Referente Privacy (responsabile della struttura a cui afferisce) ed avviene utilizzando la specifica nomina (Allegato 3 - R02/IOS01).

Considerato che tutti i soggetti autorizzati al trattamento dei dati operano sotto la diretta autorità del Titolare e del rispettivo Referente Privacy a cui afferiscono, attenendosi alle istruzioni operative impartite dagli stessi nei documenti di nomina o in altri eventuali documenti specifici ed integrativi (Allegato 2 – T04/IOS01).

Tenuto conto che i principi generali in tema di trattamento dei dati e le istruzioni richiamate, integrano le istruzioni/informazioni/indicazioni/direttive di carattere generale che il Titolare rende disponibili nella sezione della rete intranet aziendale dedicata alla privacy, anche alla luce del quadro normativo in evoluzione, è fatto obbligo a ciascun Referente Privacy e personale autorizzato al trattamento, di consultare gli aggiornamenti della documentazione aziendale in materia, sul sito intranet aziendale nella sezione sopra citata.

Preso atto della non sussistenza di oneri conseguenti al presente provvedimento a carico del redigendo bilancio economico preventivo dell'anno in corso.

Acquisito il parere favorevole della Dott.ssa Federica Banorri in qualità di DPO.

Attestata la regolarità tecnica e la legittimità del presente provvedimento da parte dei responsabili che sottoscrivono in calce.

Delibera

per le motivazioni esposte in premessa e che si intendono qui integralmente riportate:

1. ridefinire nuovi profili di responsabilità in tema di protezione dei dati personali in ordine alla individuazione dei soggetti designati ad eseguire operazioni di trattamento e ai profili delle responsabilità in tema di protezione dei dati personali, garantendo continuità rispetto alle scelte organizzative negli anni assunte dalla Azienda, pur modificando tuttavia parzialmente il preesistente organigramma delle responsabilità privacy aziendali e individuando, inoltre, una nuova modalità di designazione dei soggetti preposti al trattamento dei dati personali;

2. di designare e nominare quali Referenti Privacy, con particolare riferimento alle previgenti figure dei responsabili (interni) del trattamento i Direttori di Struttura Complessa, i Responsabili di Struttura Semplice Dipartimentale e i Responsabili di Programmi o altre strutture/articolazioni purchè con gestione di risorse;

3. di stabilire che l'attribuzione dei compiti e delle funzioni inerenti il trattamento di dati personali ai titolari dei suddetti incarichi, sia inerente ed insita all'incarico stesso ricoperto, senza necessità di separata nomina ad personam;

4. di affidare ai Referenti Privacy lo svolgimento di compiti elencati, non in modo esaustivo e tassativo, nelle istruzioni allegate alla nomina (Allegato 1 - T03/IOS01);

5. di rilevare che la nomina a Referente Privacy, essendo connessa all'affidamento di incarico come indicato al punto 2) e al punto 4), è condizionata alla durata dell'incarico e si intende decaduta a tutti gli effetti alla cessazione dell'incarico medesimo, fermo restando in ogni caso la facoltà del Direttore Generale, in qualità di Titolare del trattamento dei dati, di ritirarla in caso di inadempimento;

6. di specificare che, al fine di conferire continuità delle suddette responsabilità, i compiti e le funzioni in capo ai Referenti Privacy, si estendono ai dirigenti in caso di vacanza del ruolo di Direttori di Struttura Complessa, di Responsabili di Struttura Semplice Dipartimentale, Responsabili di Programmi o altre strutture/articolazioni purchè con gestione di risorse;

7. di fare salvi tutti gli effetti delle pregresse nomine a "responsabili [interni] del trattamento", d'ora in poi Referenti Privacy dichiarando tuttavia decadute le nomine non più compatibili con il nuovo assetto organizzativo;

8. con riferimento ai professionisti che assumono il ruolo di Direttore di Struttura Complessa e di Responsabile di Struttura Semplice Dipartimentale, Responsabili di Programmi con gestione di risorse, in un momento successivo alla adozione del presente atto, di prevedere la nomina a Referente Privacy, contestualmente alla sottoscrizione del relativo contratto di incarico, il quale recherà indicazione

dell'impegno in termini di protezione dei dati personali, dei relativi compiti e degli adempimenti assunti, che il dipendente sottoscriverà per ricevuta;

9. di dare mandato al SUMAP, per il futuro, di consegnare la presente deliberazione ai titolari di incarichi dirigenziali di cui al punto 2 a seguito di ogni conferimento/rinnovo o comunque di variazioni soggettive nella titolarità degli incarichi come sopra individuati, integrando altresì il contratto individuale con apposita clausola;

10. di precisare inoltre che l'individuazione di soggetti Referenti Privacy può rendersi necessaria anche per altri soggetti in virtù della particolarità organizzativa e funzionale, delle attività di competenza e o della tipologia dei dati trattati attraverso la designazione specifica da parte del Titolare;

11. di dare mandato all'Ufficio Privacy di aggiornare l'elenco dei "responsabili (interni) del trattamento dei dati", pubblicando l'elenco dei "Referenti Privacy", nell'area internet dedicata alla privacy garantendo la rappresentazione corretta dei nominativi indicati, corrispondente alla nuova organizzazione e alla terminologia ridefinita in linea con il GDPR, e di monitorare nel tempo le modifiche, sia organizzative sia riguardanti la titolarità degli incarichi sopramenzionati, che daranno luogo alla necessità di procedere ad un nuovo aggiornamento dell'elenco;

12. di superare la procedura di nomina aziendale sinora prevista, che prevedeva la designazione separata ad personam da parte del rispettivo "responsabile (interno) del trattamento", definendo ora di autorizzare al trattamento dei dati personali tutti i soggetti che operano sotto la diretta autorità del Titolare del trattamento, quindi tutti i dipendenti/collaboratori dell'Azienda Ospedaliero Universitaria di Bologna Policlinico S. Orsola Malpighi, compresi i medici in formazione specialistica, gli studenti di medicina e chirurgia nel periodo di tirocinio obbligatorio, i frequentatori volontari, i dottorandi e assegnisti di ricerca autorizzati all'attività di assistenza, i quali sono tenuti alla osservanza delle istruzioni di carattere generale ricevute dal titolare di trattamento per il corretto trattamento dei dati personali, oltre ad ulteriori ed eventuali istruzioni di carattere specifico che il Titolare del trattamento, anche per il tramite dei Referenti Privacy, impartirà loro con riferimento a particolari trattamenti di dati;

13. di notificare tale autorizzazione al trattamento, a tutti i dipendenti/collaboratori/titolari di rapporto di lavoro autonomo e a tutti gli altri soggetti operanti stabilmente ad altro titolo nell'ambito delle strutture organizzative aziendali, compresi i medici in formazione specialistica, gli studenti di medicina e chirurgia nel periodo di tirocinio obbligatorio, i frequentatori volontari, i dottorandi e assegnisti di ricerca autorizzati all'attività di assistenza, attraverso la pubblicazione del predetto atto all'interno dell'area privacy della intranet aziendale e del profilo personale del Portale del dipendente (GRU);

14. di definire, con riferimento alle persone che prenderanno servizio in data successiva alla adozione del presente atto, che la autorizzazione al trattamento dei dati personali opererà contestualmente alla

sottoscrizione del relativo contratto di lavoro o alla accettazione del relativo incarico, dando mandato al SUMAP, di procedere nei confronti del personale di nuova "assunzione" integrando altresì i (futuri) contratti di lavoro con apposita clausola;

15. di mantenere in capo ai Referenti Privacy il compito di nominare quale personale autorizzato al trattamento i collaboratori che debbano essere volta per volta autorizzati al trattamento dei dati in quanto non stabilmente operanti all'interno delle strutture aziendali (a titolo di esempio non esaustivo ci si riferisce a lavoratori socialmente utili, volontari, tirocinanti in quadrati diversamente rispetto a quelli sopradescritti, ecc..) utilizzando lo specifico atto di nomina (Allegato 3 - R02/IOS01);

16. di ritenere che tale autorizzazione al trattamento si esplichi, in particolare, nel rispetto delle istruzioni operative, di carattere generale, stabilite dal titolare di trattamento, per la consultazione delle quali si rinvia alla pagina della sezione intranet aziendale dedicata, nonché delle ulteriori istruzioni, di carattere specifico, eventualmente impartite dai Referenti Privacy;

17. di assegnare al personale autorizzato al trattamento i compiti riportati nell'atto di nomina la cui elencazione non può comunque ritenersi esauriente rispetto a tutti i compiti e gli adempimenti connessi ad una compiuta e corretta attività di protezione dei dati personali, e che potrà essere integrata, se necessario, da parte dei Referenti Privacy in base alle caratteristiche specifiche dei singoli trattamenti o in base alle mansioni dei singoli operatori autorizzati (Allegato 2 - T04/IOS01);

18. di riconoscere in capo ai Referenti Privacy come sopra individuati la responsabilità di richiedere le autorizzazioni al rilascio delle abilitazioni all'accesso degli applicativi informatici aziendali, mantenendo in essere le attuali modalità di invio delle richieste, nelle more della definizione di un nuovo percorso informatizzato;

19. di dare mandato ai Referenti Privacy di verificare che, nei contratti (o accordi, convenzioni, protocolli, etc.) sottoscritti per l'esternalizzazione di servizi ("outsourcing"), a soggetti pubblici o privati che operano per conto del titolare, e che comportino il trattamento di dati personali, sia prevista la nomina del soggetto quale "Responsabile (esterno) di trattamento" e, diversamente, di provvedere alla nomina utilizzando la modulistica fornita dal titolare di trattamento (Atto di designazione a responsabile del trattamento dei dati personali);

20. di avvalersi, con riferimento specifico all'ambito della ricerca e delle sperimentazioni cliniche, dell'attribuzione delle competenze e delle responsabilità in materia di protezione di dati personali e relativi compiti definiti per i Referenti Privacy, oltre a quelli ulteriori legati alla specifica attività, a ciascun Responsabile Scientifico volta per volta individuato nel provvedimento autorizzatorio emesso dal Direttore Generale per ciascun progetto di ricerca/sperimentazione clinica;

21. di precisare che dall'adozione del presente provvedimento non derivano oneri economici a carico del Bilancio dell'Azienda Ospedaliero Universitaria di Bologna Policlinico S. Orsola Malpighi.

Responsabile del procedimento ai sensi della L. 241/90:
Federica Filippini

Allegato 1 - T03/IOS01

COMPITI FUNZIONI E POTERI DEI REFERENTI PRIVACY

- Trattare i dati personali solo su istruzione del Titolare del trattamento e garantire la corretta applicazione del Regolamento generale per la protezione dei dati (GDPR) e del D.Lgs. 196/2003, come modificato dal D.Lgs.101/2018, nonché la conformità alle indicazioni dell'Autorità Garante per la protezione dei dati personali;
- osservare e fare osservare:
    a) le direttive aziendali in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento, anche per il tramite dell'Ufficio Privacy Aziendale, Gruppo Aziendale Privacy e del Servizio ICT Aziendale (es. istruzione operativa per l'utilizzo delle risorse informatiche (IOA44), Manuale Operativo per la gestione del DSE, Istruzione Operativa aziendale percorso di notifica dei violazione dei dati personali all'autorità di controllo e comunicazione della violazione dei dati personali all'interessato – IOA98);
    b) le istruzioni di carattere generale impartire dal Titolare a tutti i soggetti autorizzati al trattamento (di cui all'**allegato 2 – R02/IOS01**);
    c) eventuali ulteriori specifiche istruzioni predisposte dallo stesso in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.

- porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati, assicurando che i soggetti interessati (es. pazienti, dipendenti, fornitori…..) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt.13 e 14 del GDPR;
- provvedere alla designazione dei soggetti autorizzati al trattamento dei dati personali per i singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili, ecc..), attraverso la predisposizione dell'apposito modello di cui l'**allegato 3 - T04/IOS01**;
- vigilare sulla conformità dell'operato dei soggetti autorizzati ad essi afferenti alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto;
- verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;
- attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento e compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e soprattutto organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;
- partecipare ai momenti formativi organizzati dall'Azienda ed assicurare la partecipazione dei propri autorizzati;
- fornire le informazioni richieste dall'Ufficio Privacy Aziendale/Gruppo Aziendale Privacy e segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO;
- comunicare all'Ufficio Privacy Aziendale/Gruppo Aziendale Privacy i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale;
- collaborare con l'Ufficio Privacy Aziendale/Gruppo Aziendale Privacy ed il Servizio ICT per la predisposizione del documento della valutazione di impatto sulla protezione dei dati qualora ne ricorrano i presupposti in base all'art. 35 del GDPR;
- non porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
- provvedere, qualora tra le attività istituzionali della Struttura vi sia la stipula di contratti/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni quali "responsabili del trattamento" a norma dell'art. 28 del GDPR e delle condizioni ivi indicate e trasmettere copia dell'atto di designazione e dell'accettazione della nomina

all’Ufficio Privacy Aziendale anche ai fini dell’aggiornamento del registro aziendale delle attività di trattamento dei dati;

- comunicare tempestivamente all'Ufficio Privacy Aziendale potenziali casi di data breach all'interno della propria struttura e collaborare alla istruttoria del caso al fine di sottoporre al DPO ogni utile e opportuna determinazione in merito.

Allegato 2 – T04/IOS01

ISTRUZIONI di CARATTERE GENERALE impartire dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente privacy di afferenza garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;
- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- email e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali (es. IOA29, IOA44, istruzioni operative per l'utilizzo della posta elettronica e internet ecc…..)
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii..
- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerò porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.).

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Azienda.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. *Istruzione operativa per il corretto utilizzo dei sistemi informatici aziendali (IOA44);*
2. *Manuale Operativo sull'utilizzo del Dossier Sanitario elettronico;*
3. *Istruzione Operativa sull'utilizzo della posta elettronica e internet*

a cui si rinvia, reperibili sempre alle pagine intranet dedicate https://intranet.aosp.bo.it/content/la-privacy-azienda e http://qweb.aosp.bo.it/cgi-bin/isopubb/isopubb_gestione?search.

ATTO DI DESIGNAZIONE
DEL SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI
Ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003, così come modificato dal D.Lgs. n. 101/2018

Il sottoscritto_____
(indicare il nome del Referente Privacy di afferenza)

in qualità di Referente Privacy dell' UO/struttura/articolazione _____

DESIGNA

(indicare NOME e COGNOME)

in qualità di .....
(indicare funzione, ruolo,...)

SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI relativi

AMBITO DEL TRATTAMENTO (sede/i di assegnazione) DESCRIZIONE DEL TRATTAMENTO ARCHIVI BANCHE DATI

A seguito della suddetta designazione Lei è autorizzato a svolgere operazioni di trattamento, per il proprio ambito di competenza, secondo i principi generali di trattamento, le prescrizioni, le istruzioni operative generali impartite dal Titolare e le ulteriori eventuali istruzioni specifiche dal sottoscritto impartite.

Principi di carattere generale:

- ✓ trattare i dati di propria pertinenza in modo lecito, secondo corre
- ✓ ttezza e trasparenza;
- ✓ trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
- ✓ verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
- ✓ conservarli nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare (**allegate alla presente T01/IOS01**) e sempre consultabili nella sezione Privacy della rete intranet aziendale, dalle prescrizioni e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto in qualità di Referente Privacy di Sua afferenza.

Prescrizioni:

a. Rispettare l'obbligo di riservatezza e segretezza, mantenendo la segretezza delle informazioni di cui venga a conoscenza mediante accesso ai sistemi informativi aziendali, secondo il profilo di autorizzazione assegnato alle proprie credenziali di autenticazione (user e password), corrispondente alla classe di autorizzato di appartenenza;
b. trattare i dati di propria pertinenza in modo lecito, secondo correttezza e trasparenza;
c. trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
d. verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;

e. conservare i dati nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella sezione Privacy della rete intranet aziendale, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;
f. utilizzare le informazioni e i dati, con cui si entra in contatto per ragioni di lavoro, esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza, secondo quanto definito dalle regole aziendali, per tutta la durata dell'incarico ed anche successivamente al termine di esso, astenendosi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
g. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su tutti dispositivi in dotazione ad altri operatori e/o di lasciare, in caso di allontanamento anche temporaneo dalla postazione di lavoro il sistema operativo avviato con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
h. conservare correttamente i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che gli stessi siano accessibili a persone non autorizzate mettendo in atto tutte le misure di sicurezza previste dal Regolamento Europeo in materia di protezione dei dati n. 2016/679, dalla normativa nazionale, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella sezione sopra indicata, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;
i. astenersi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
j. segnalare al sottoscritto eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
k. informare senza ingiustificato ritardo il soggetto delegato al trattamento di qualunque fatto o circostanza, anche accidentale, che abbia causato perdita, distruzione dei dati, accesso non consentito o comunque non conforme ai principi sopradetti.

La S.V. prende atto di quanto previsto nella presente designazione ed assume la qualifica di **soggetto autorizzato al trattamento dei dati personali** impegnandosi a:

- ✓ rispettare i principi e le prescrizioni soprariportate, le istruzioni di carattere generale impartite dal Titolare, allegate al presente atto di designazione e disponibili nella sezione Privacy della rete intranet aziendale, e le eventuali istruzioni che Le verranno eventualmente impartite per l'ambito di competenza e del profilo professionale di appartenenza.

E' fatto obbligo a ciascun professionista autorizzato al trattamento consultare gli aggiornamenti della documentazione aziendale in materia sul sito intranet aziendale nella sezione sopra citata.

Ciò premesso, il presente atto costituisce pertanto conferimento formale dell'autorizzazione al trattamento dei dati connessi allo svolgimento dell'attività lavorativa connessa all'ambito del trattamento sopra individuato, secondo le istruzioni allegate e secondo le prescrizioni sopra riportate.

Tale DESIGNAZIONE:

- ha validità per l'intera durata del rapporto di lavoro con l'Azienda.
- viene a cessare al modificarsi del rapporto di lavoro o con esplicita revoca dello stesso.

****

DICHIARAZIONE DI RICEVIMENTO DELL'ATTO DI DESIGNAZIONE E DI IMPEGNO ALL'OSSERVANZA DELLE ISTRUZIONI ALLEGATE

Il sottoscritto _____

(indicare NOME e COGNOME)

DICHIARA

1. di aver ricevuto la designazione a autorizzato al trattamento;
2. di aver attentamente letto e compreso il contenuto del presente atto e del suo allegato, e di impegnarsi ad osservare tutte e specifiche istruzioni impartite;
3. di obbligarsi ad osservare le ulteriori direttive/regolamentazioni aziendali reperibili alla sezione intranet dedicata .....
4. di dare atto che l'obbligo di riservatezza correlato all'incarico va osservato anche successivamente alla conclusione dello stesso

Data_____ Firma _____

Allegato 2 – T04/IOS01

ISTRUZIONI di CARATTERE GENERALE impartire dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente privacy di afferenza garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto

della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;

- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- email e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali (es. IOA29, IOA44, istruzioni operative per l'utilizzo della posta elettronica e internet ecc…..)
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii..
- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerò porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.).

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Azienda.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. Istruzione operativa per il corretto utilizzo dei sistemi informatici aziendali (IOA44);
2. Manuale Operativo sull'utilizzo del Dossier Sanitario elettronico;
3. Istruzione Operativa sull'utilizzo della posta elettronica e internet

a cui si rinvia, reperibili sempre alle pagine intranet dedicate https://intranet.aosp.bo.it/content/la-privacy-azienda e http://qweb.aosp.bo.it/cgi-bin/isopubb/isopubb_gestione?search.