Asl5
Sistema Sanitario Regione Liguria

Sistema Sanitario Regione Liguria
Azienda Sociosanitaria Ligure 5
LA SPEZIA

DELIBERA DEL COMMISSARIO STRAORDINARIO

Delibera n. 403 del 29. LUG. 2020

Il Commissario Straordinario, Dott.ssa Daniela TROIANO

Su proposta del Responsabile Protezione Dati Dott.ssa Antonella Calò

adotta la seguente deliberazione:

Oggetto: Policy Privacy Regolamento Aziendale

IL PROPONENTE
Il Responsabile protezione Dati Aziendale

(Dott.ssa Antonella Calò)

☐ La spesa di € _____ prevista nella presente proposta, rientra nel Conto Economico del Bilancio Preventivo Economico anno _____ al Conto Economico _____ Autorizzazione n. _____

☐ La spesa di € _____ prevista nella presente proposta rientra nello Stato Patrimoniale dei Bilanci d'esercizio anni _____ al conto n. _____

☐ Gli introiti di € _____ previsti nella presente proposta, rientrano nel Conto Economico del/i Bilancio/i d'esercizio/i _____ al/ai Conto/i Economico/i n. _____ Autorizzazione n. _____

☒ Il presente provvedimento non comporta spesa

Il Direttore della Struttura Complessa
Gestione delle Risorse Economiche e Finanziarie
(Dott. Fabio CARGIOLLI)

Premesso che

- questa azienda, vigente il precedente regime normativo, declinato dalla direttiva europea 95/46/CE ad oggetto "regolamento generale sulla protezione dei dati" e dal D. Lgs. 30 giugno 2003, n.196, meglio noto come "Codice in materia di protezione dei dati personali" si era dotata del Regolamento di policy privacy approvato con deliberazione n. 244 del 14/03/2017 – con cui intendeva adeguare l'operato e l'organizzazione alle prescrizioni normative in materia di privacy e di sicurezza nella gestione dei dati;

Rilevato che il nuovo regime normativo comporta

- modifiche sostanziali nell' impostazione della policy privacy Aziendale quali la necessaria introduzione di nuove figure [ad es.: il Responsabile della protezione dei dati], di nuovi strumenti [ad es. : il registro dei trattamenti, la valutazione dei rischi ovvero la valutazione d' impatto privacy - Pia -]

- il necessario adeguamento ad una concezione della privacy e della correlata attività volta a proteggere i dati trattati più capillare e sostanziale tanto da permeare i progetti sin dall'inizio [privacy by design] sino a giungere ad una privacy per impostazione predefinita [privacy by default];

- la correlata definizione e revisione di ruoli e compiti all'interno dell'organigramma privacy e la contestuale rivisitazione degli schemi di incarico alla luce dei maggiormente pregnanti adempimenti in materia;

Considerato che pertanto, alla luce del principio di responsabilizzazione, il titolare è onerato di declinare in modo compiuto il sistema privacy, adottando l'organigramma prescelto con le correlate funzioni, le misure organizzative e tecniche prescelte a protezione dei dati, le relative misure di sicurezza, non solo informatiche, le modalità per consentire nel modo più agevole agli interessati l'esercizio di una serie diritti riconosciuti per legge, nonché un insieme di istruzioni generali e specifiche idonee a regolare i comportamenti del personale autorizzato / delegato in merito alle modalità di trattamento dei dati affidati;

Dato atto che

- quanto sopra è declinato specificamente nel documento di policy privacy allegato sub 1, al presente atto quale sua parte integrante e sostanziale;

- il documento in questione, di natura regolamentare, è già stato oggetto di disamina positiva in seno al gruppo di lavoro privacy costituito in Alisa giusta deliberazione n.173 del 6/7/2018 come risulta da nota prot. Alisa n. 10644 del 26.11.2018

Rilevato in sintesi che l'approccio esposto

- favorisce una gestione uniforme e sistematica della policy privacy aziendale favorendo l'introduzione di misure organizzative e tecniche da ritenersi prioritarie, nonché di ulteriori eventuali garanzie a tutela dei dati;

- persegue le esigenze di elevata tutela proprie di un titolare che, come questa azienda, tratta, per vocazione istituzionale, una serie di informazioni, particolarmente delicate, ad elevato rischio ed impatto privacy;

VISTI E RICHIAMATI i seguenti riferimenti normativi di settore:

- **il Regolamento dell'Unione Europea 2016/679 del 14.04.2016** *(G.U. UE del 4.maggio 2016)* con particolare riferimento :

- ai principi generali applicabili in materia di trattamento dei dati personali ed alle connesse misure tecniche ed organizzative volte a garantirne la sicurezza di sicurezza

- agli adempimento gravanti in capo al titolare del trattamento dati il quale, giusta il principio di responsabilizzazione, è tenuto ad adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l´applicazione del regolamento in parola;

- **il D.L.gs. 18 maggio 2018, n. 51** ad oggetto : "Attuazione della direttiva (UE) 2016/680 del Parla-mento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. *(GU n.119 del 24-5-2018);*

- **il D.L.gs 10 agosto 2018, n. 101** ad oggetto **"**Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE "(regola mento generale sulla protezione dei dati). *GU Serie Generale n.205 del 04-09-2018)*

Ritenuto pertanto, alla luce della vigente normativa e di quanto sopra esposto, che il documento in allegato, sia necessario ad ottemperare al dettato normativo, allineando ad esso percorsi ed azioni aziendali;

Tanto premesso

IL COMMISSARIO STRAORDINARIO

In virtù dei poteri conferitigli con Delibera di Giunta Regionale n. 612 del 16 luglio 2019;

Sentito il parere conforme del Direttore Amministrativo, del Direttore Sanitario e del Direttore Sociosanitario per quanto di rispettiva competenza;

DELIBERA

1. di considerare la premessa parte integrante e sostanziale del presente provvedimento;

2. Di dare atto

   a) dell'obbligo normativo, gravante sull'azienda, in forza del principio di accountability di approntare risorse, strumenti ed istruzioni volte a garantire la corretta applicazione delle norme vigenti in materia di protezione dati ;

   b) della conseguente necessità, di adeguare l'azione aziendale alle nuove disposizioni adottando un nuovo regolamento aderente al dettato normativo europeo quale allegato sub a) confermandone modalità ed impostazione e per l' effetto di approvarlo in ogni sua componente;

3. Di disporre la pubblicazione del presente provvedimento sul sito istituzionale aziendale, ai fini della massima trasparenza ed accessibilità totale, ai sensi della vigente normativa, e di pubblicarlo altresì all'Albo Pretorio informatico di questo Ente, ai sensi dell'art. 32 della Legge 69/2009.

4. Di trasmettere il presente provvedimento a tutte le SSCC ed SSD sanitarie ed amministrative disponendone altresì la pubblicazione permanente sul sito aziendale al link dedicato alla privacy.

IL DIRETTORE AMMINISTRATIVO
(Dott. Antonello MAZZONE)

IL DIRETTORE SANITARIO
(Dott.ssa Maria Antonietta BANCHERO)

Il DIRETTORE SOCIOSANITARIO
(Dr.ssa Maria Alessandra MASSEI)

IL COMMISSARIO STRAORDINARIO.
(Dott.ssa Daniela TROIANO)

Estensore del provvedimento: RPD ASL5 Dott.ssa Antonella Calò

Delibera n. 403 del 29 LUG. 2020 composta di n. pagine 4

POLICY PRIVACY AZIENDALE
REGOLAMENTO

SOMMARIO

Art. 1
Oggetto ed ambito di applicazione

Il presente regolamento disciplina, in ottemperanza ai principi fissati dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (RGDP) e relative norme di armonizzazione nonché alle disposizioni nazionali vigenti in materia di protezione dati, le operazioni di trattamento svolte da ASL 5 (di seguito azienda) e dai propri operatori, sui dati personali degli interessati, per finalità di terapia, diagnosi , cura e riabilitazione, comprensive delle attività di gestione aziendale, quali adempimenti contabili, amministrativi, statistici ed epidemiologici. L'azienda si impegna a garantire e garantisce che il trattamento di dati personali, ivi compresi quelli contenuti in archivi aziendali, anche automatizzati, sia gestito con modalità tali da rispettare i diritti, le libertà fondamentali e la dignità delle persone, secondo le disposizioni vigenti in materia di protezione dei dati e di digitalizzazione[1].
Al riguardo l'azienda intende assicurare ed assicura, in un percorso di miglioramento continuo, l'adozione di adeguate e preventive misure di sicurezza volte ad evitare situazioni di rischio, non conformità e/o alterazione dei dati utilizzati ed a facilitare l'esercizio dei diritti da parte dell'interessato[2].

Art. 2
Accountability e Sistema Privacy Aziendale

L'Azienda, in forza del principio di responsabilità e verifica, al fine di garantire e dimostrare che il trattamento dei dati personali effettuato è conforme alla normativa vigente, predispone adeguate misure tecniche ed organizzative, in relazione a: natura, ambito di applicazione, contesto, finalità del trattamento, possibili rischi di lesione a diritti e libertà degli interessati di cui tratta i dati per attività istituzionale.

Tali misure, soggette a riesame ed aggiornamento periodico ed ogniqualvolta si renda necessario, vanno a comporre il Sistema Privacy dell'Azienda, che include:

- il sistema di attribuzione delle responsabilità nel trattare i dati e le correlate autorizzazioni accordate formalmente per iscritto;
- il Responsabile aziendale per la Protezione dei dati(RPD/DPO) e il suo staff (per come successivamente definito);
- il Registro delle attività di trattamento dei dati ed analisi dei rischi connessa con il relativo documento di valutazione;
- la regolamentazione interna, la policy, le procedure e le disposizioni operative adottate per i singoli e specifici trattamenti di dati personali;
- la documentazione relativa ad informative, consensi, revoche, etc.;
- la documentazione relativa alle valutazioni preliminari di impatto;
- il sistema di audit e verifica periodica e programmata sulle modalità di trattamento adottate ;
- il sistema di prevenzione, contenimento e gestione delle violazioni dei dati personali;
- il sistema di formazione continua del personale aziendale in materia di protezione dati ;
- il rapporto tra l'Azienda, Titolare del trattamento dei dati personali, e gli Interessati con specifica attenzione alle scelte operate per garantire l' esercizio dei diritti.

---

[1] A titolo esemplificativo e non esaustivo si citano : Decreto Legislativo n. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"; Decreto Legislativo n. 82 del 2005 "Codice dell'Amministrazione digitale"; L. 241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti"; Decreto Legislativo n. 33 del 2013, "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"; Le nuove Linee guida del Garante privacy sulla trasparenza nella PA. Del 28.5.2014, le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito
pubblico" - 14 giugno 2007,le Linee guida emanate dal Garante Privacy il 1.3.2007 sull'utilizzo di posta elettronica e internet da parte del personale , le Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi ,effettuato da soggetti pubblici a fini di pubblicazione e diffusione sul web (2 marzo 2011); linee guida in tema di Fascicolo sanitario elettronico (FSE) e Dossier sanitario del 16 luglio 2009; Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri Enti obbligati del 28 maggio 2014; . Linee guida in materia di Dossier sanitario del 4 giugno 2015.

[2] La persona fisica a cui si riferiscono i dati ossia il loro proprietario cui compete l' esercizio di una serie di diritti e facoltà , esposti nel seguito del documento, espressione del diritto ad determinarsi liberamente riguardo alla propria sfera giuridica

Art. 3
Finalità del Trattamento Dati

Nel trattare i dati, ASL 5 persegue le seguenti finalità:

- svolge i compiti e le funzioni istituzionali proprie del Servizio Sanitario Nazionale, quali finalità di rilevante interesse pubblico, volte , in particolare, ad erogare terapia, diagnosi, cure, riabilitazione, prevenzione ed assistenza sanitaria, elaborare statistiche e report epidemiologici;
- eroga prestazioni sanitarie specialistiche, istituzionali ed in libera professione, (comprensive delle attività di supporto) per tutelare la salute e l'incolumità fisica di utenti, terzi e della collettività;
- svolge attività didattica e di formazione volte alla tutela della salute;
- tutela la sicurezza e la salute dei lavoratori e garantisce la sorveglianza igienico-sanitaria nelle proprie strutture;
- gestisce e tutela il patrimonio aziendale, materiale e immateriale, nonché le necessarie risorse umane, tecnologiche e strumentali
- gestisce i dati di dipendenti e collaboratori al solo fine di gestire il rapporto giuridico ed economico di lavoro con esclusione di altre / diverse finalità ivi inclusa la comunicazione dai a soggetti giuridici diversi da quelli previsti per legge , salvo ordine di esibizione dell' AGO .

Art. 4
Titolare[3] e Contitolare[4] del Trattamento Dati

L'Azienda, in persona del Direttore Generale, suo legale rappresentante, è il titolare del trattamento[5] dei dati personali affidati allo scopo di svolgere i propri compiti istituzionali. In tale veste è tenuta normativamente ad attuare le misure tecniche ed organizzative adeguate a garantire e dimostrare che i dati personali, afferenti l'azienda e da questa gestiti, sono trattati in conformità alla vigente normativa.
Nel caso in cui l'azienda determini, congiuntamente ad un altro Titolare, le finalità e i mezzi del trattamento, assume, unitamente a questi, la veste di Contitolare del trattamento.
I Contitolari stabiliscono, in modo trasparente, mediante atto scritto, il ruolo ricoperto da ciascuno ed i rapporti tra loro e con gli interessati, le rispettive responsabilità, anche riguardo all'esercizio dei diritti dell'interessato.
Gli interessati sono legittimati a conoscere i contenuti di tale accordo e ad esercitare, nei confronti di entrambi, i diritti legali loro attribuiti.

Art. 5
Compiti e funzioni dell'Azienda

L'Azienda, in qualità di Titolare, provvede a:

a) adottare le misure di sicurezza e quelle tecnico-organizzative adeguate a garantire la protezione dei dati personali, con particolare riferimento ed attenzione ai processi di digitalizzazione adottati in sanità;
b) designare il Responsabile aziendale della protezione, dotandolo delle necessarie risorse ad assolvere i compiti previsti per legge ed a mantenere l'indipendenza e le competenze specialistiche che gli sono proprie;
c) attivare, tenere ed aggiornare il Registro delle attività di trattamento dei dati personali;
d) assicurare l'informazione e la formazione obbligatoria del personale, in materia di protezione dei dati;

[3] Art.4 del RGPD punto 7 e considerandum 74
[4] Art.26 del RGPD e considerandum 79
[5] «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le modalità ed i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

e) nominare i soggetti autorizzati al trattamento dati[6], quali ad es. Responsabili interni, esterni, incaricati/autorizzati etc.;
f) impartire loro, con l'ausilio del RPD aziendale, direttamente, ovvero tramite i direttori di Struttura Complessa o Responsabili di SSD, le necessarie istruzioni per la corretta gestione e protezione dei dati trattati.

Nello svolgere tali funzioni è imprescindibile, fruire, in ragione del riparto interno delle competenze, della collaborazione dei Direttori/Responsabili di struttura e del RPD aziendale a cui, in particolare, è demandato il controllo sulla gestione dei dati personali a norma di legge.

Art. 6
Protezione dei dati personali dalla progettazione e per impostazione predefinita[7]

L'Azienda, nello stabilire modalità e strumenti per trattare i dati personali e tutelare i diritti degli interessati, valuta, in via preliminare, lo stato dell'arte, i costi di attuazione, la natura, l'ambito di applicazione, il contesto e le finalità del trattamento stesso, nonché i possibili rischi, in ragione della probabilità e gravità di loro incidenza su diritti e libertà degli interessati.
Le attività in parola sono svolte già in fase progettuale /precontrattuale e coniugate con le misure tecniche ed organizzative al fine di garantire, nell' arco del tempo, che, per impostazione predefinita, siano trattati soltanto i dati personali necessari ed indispensabili a perseguire la finalità specificamente correlata al relativo trattamento, con particolare attenzione a:

- ✓ quantità e qualità dei dati personali raccolti;
- ✓ portata del trattamento;
- ✓ periodo di conservazione;
- ✓ accessibilità;
- ✓ soggetti a cui è consentito il trattamento con correlato profilo
- ✓ sistema dei profili di accesso e gestione dei dati
- ✓ sistema di gestione dei consensi.
- ✓ sistema dei file di log
- ✓ sistema di individuazione e selezione dei dati i ragione delle tutele da garantire
- ✓ sistema di protezione informatica dei dati

Con tale impostazione si intende, inoltre, garantire di default, a seguito di revisione programmata delle procedure informatizzate, che siano utilizzati soltanto i dati personali indispensabili, e che gli stessi siano resi accessibili unicamente alle persone autorizzate, limitatamente al tempo necessario ad eseguire le attività di competenza[8].

Art. 7
Dati trattati e categorie di interessati

L'azienda tratta i dati personali[9] comprensivi di quelli identificativi[10], dei dati di salute e dei restanti dati afferenti alle cosiddette categorie particolari [11] , nonché soggetti a maggior tutela[12] e "giudiziari[13]" in oggi sostanzialmente

[6] trattamento dati :qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.
[7] ART 25 del RGDP e consideranda 75 e 78
[8] Tale valutazione di competenza della direzione aziendale di concerto con il SIA ed IL RPD non può comunque prescindere dal considerare reali esigenze di servizio da accordare tuttavia sempre in conformità alle norme vigenti
[9] dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile
[10] «dati identificativi»: i dati personali che permettono l'identificazione diretta dell'interessato ossia: nome e cognome, indirizzo di casa, indirizzo email numero identificativo nazionale, codice fiscale , numero di passaporto, indirizzo IP (quando collegato ad altri dati), numero di targa del veicolo,- numero di patente, volto, impronte digitali o calligrafia, numeri di carta di credito, identità digitale, data di nascita,- luogo di nascita, informazioni genetiche, numero di telefono , account name o nickname.
[11] «categorie particolari di dati»: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare |o stato di salute e la vita sessuale. I dati di salute non possono essere diffusi. Tali dati sono oggetto di comunicazione anche verso soggetti pubblici solo se previsto da disposizioni di legge o di regolamento.

rientranti nelle tipologie di cui all'art. 9 e 10 del RGPD relativi alle categorie di interessati di seguito riportate, a titolo esemplificativo e non esaustivo:

- cittadini utenti, assistiti, pazienti, loro familiari e/o accompagnatori;
- personale sanitario, amministrativo, tecnico e professionale della dirigenza e del comparto in rapporto di dipendenza, convenzione o collaborazione;
- soggetti che, per motivi di studio o volontariato, frequentano le strutture aziendali;
- clienti e fornitori;
- partecipanti a bandi, gare e selezioni.

Nei casi e con i limiti previsti dalle norme di settore, sono specificamente trattati i dati di salute[14] comprensivi di quelli soggetti a maggior tutela[15] per rilevare e curare una serie di malattie e patologie ad essi correlate e per finalità epidemiologiche, di trapianto di organi e tessuti e di monitoraggio della spesa sanitaria.

Il contenuto dei dati a maggior tutela, altamente pregiudizievole per la persona cui appartengono, comporta, per obbligo normativo di settore, il trattamento in forma anonima.

L'Azienda, quindi, per adottare le misure tecnico-organizzative adeguate al maggior rischio inerente/derivante da tale gestione, non potendo anonimizzare il dato[16], ha optato per l' oscuramento di default , laddove possibile, dei documenti indicizzati digitalmente con i codici prestazionali di riferimento (utilizzando SDO, DRG e LEA).

Qualora i dati a maggior tutela siano contenuti nella parte descrittiva di un documento sanitario la loro valutazione è rimessa al personale sanitario, onerato di avvisare interessato e di richiedergli se desidera esercitare il proprio diritto ad oscurare il dato.

I dati personali riguardanti particolari categorie sono trattati, qualora essenziali e necessari allo svolgimento delle attività istituzionali, di cui al precedente articolo 3 e nel caso in cui tali attività non possano essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Nei casi specificatamente previsti dalle norme vigenti, l'azienda assicura il diritto all'anonimato dell'interessato ovvero l'adozione di misure in grado di garantire un maggior grado di tutela della riservatezza quali ad es. l'esercizio del diritto all'oscuramento[17] con la correlata tutela a non rendere visibile tale scelta (oscuramento dell'oscuramento).

I dati personali trattati da ASL 5, nelle forme e nei limiti di quanto previsto dalla normativa vigente, sono raccolti:

- ✓ di norma, presso l'interessato ovvero presso persone diverse nei casi in cui questi sia minorenne o incapace o ancora si trovi di fatto nell' impossibilità/ incapacità di fornirli[18];
- ✓ anche presso enti del SSN, e/o altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti professioni/attività sanitarie[19].

Il trattamento dei dati personali, per fini di eventuale ricerca, ovvero in sede di sperimentazioni cliniche e mediche, viene effettuato su base volontaria, con il consenso dell'interessato, con l'osservanza delle tutele di legge e regolamentari di settore, con specifiche ed adeguate misure di sicurezza. I risultati di tali attività, pubblicati o comunque resi noti, non possono in alcun caso contenere dati personali/identificativi anche indiretti/ovvero dati biometrici[20] che rendano identificabili i soggetti ai quali si riferiscono.

---

[12] dati soggetti a maggior tutela ovvero super-sensibili sono dati il cui contenuto , altamente pregiudizievole per la persona cui appartengono comporta, per obbligo normativo di settore , il trattamento in forma anonima"

[13] L' azienda, e per essa i servizi competenti, può conoscere l' esistenza di contenzioso civile , penale , disciplinare , amministrativo e contabile afferente sia i propri dipendenti sia terzi ricoverati presso le proprie strutture ovvero in qualità di controparti a fini defensionali ed assicurativi

[14] dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

[15] malattie mentali,, veneree, a trasmissione sessuale, la siero-positività e le patologie correlate , le diverse tipologie di dipendenze, nonché le interruzioni di gravidanza, le patologie/ prestazioni erogate dalle strutture consultoriali / territoriali a favore di soggetti deboli , ovvero abusati/ oggetto di violenza

[16] i Dati anonimizzati sono stati privati di tutti gli elementi identificativi. L' anonimizzazione renderebbe estremamente difficoltosa la gestione del dato stesso senza creare disguidi tecnici e possibili danni alla persona posto che l' intero sistema aziendale è organizzato su base anagrafica e la sua modifica implicherebbe uno sforzo economico sproporzionato, laddove, obiettivo consimile può essere raggiunto con l'oscuramento di default corretto dalla possibilità per l'interessato di scegliere se rendere visibile il singolo documento all' atto di sua formazione con manifestazione di volontà espressa agli operatori sanitari

[17] L'oscuramento è una tecnica che serve a non rendere visibili i dati che il paziente ha deciso di non mostrare, in forza del principio di autodeterminazione proprio di ogni persona, quale garantito dalla costituzione e dalle carte internazionali dei diritti dell'uomo. Ogni paziente ha diritto ad oscurare i propri dati sensibili ovvero super-sensibili, quando ne ha contezza e prima che siano inseriti nel proprio fascicolo o dossier sanitario elettronico.

[18] Art.13RGPD e consideranda 60 e 62

[19] .Art.14 RGPD e consideranda 60 e 62

[20] dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Art. 8
Liceità del trattamento [21]

In generale l'Azienda può trattare, senza il consenso, i dati personali strettamente necessari a svolgere le attività istituzionali finalizzate ad erogare attività e prestazioni sanitarie previste e disciplinate da specifiche norme di legge.

I dati personali possono essere trattati soltanto:

- da Titolare, Contitolari, Responsabili (esterni ed interni ossia delegati dall'azienda), eventuali Sub-Responsabili[22], Soggetti Designati ex D. Lgs. n. 101/2018, Incaricati/Autorizzati del trattamento dei dati personali ed Amministratori di Sistema;

- se previsto per legge e se raccolti e registrati per scopi determinati, espliciti e legittimi, quando:

  a) nello specifico, il trattamento è necessario per:
     - ✓ motivi di rilevante interesse pubblico in proporzione / relazione alla finalità perseguita;
     - ✓ gestire/ erogare attività sanitarie e/o sociali qualificate attività di rilevante interesse pubblico;
     - ✓ finalità di medicina preventiva o di medicina del lavoro,
     - ✓ valutazione della capacita lavorativa del dipendente,
     - ✓ diagnosi, terapia, assistenza sanitaria e/o sociale
     - ✓ motivi di interesse pubblico nel settore della sanità pubblica finalizzati alla protezione da gravi minac-ce per la salute anche a carattere transfrontaliero o a garanzia di parametri elevati di qualità e sicurezza di medicinali e dispositivi medici nonché dell'assistenza sanitaria
     - ✓ tutelare un interesse vitale dell'interessato o di altra persona fisica, o per contenere la diffusione di epidemie ovvero adottare misure volte a evitare il contagio interno
     - ✓ assolvere gli obblighi normativi ovvero esercitare diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, sicurezza e protezione sociale;
     - ✓ finalità di ricerca scientifica, storica o statistica e di archiviazione nel pubblico interesse
     - ✓ accertare, esercitare o difendere un diritto in sede giudiziaria , in pendenza di giudizio ed ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni

  b) l'interessato ha prestato il consenso esplicito al trattamento dei dati personali per una o più finalità specifiche non rientranti nelle casistiche sopra riportate ovvero qualificabili o qualificate da norme di settore attività facoltative ed ulteriori;

I dati particolari e "giudiziari" oggetto di trattamento, le finalità di interesse pubblico perseguite, nonché le operazioni eseguibili sono individuati, per le attività istituzionali sanitarie nel Regolamento per i dati sensibili e giudiziari approvato dalla Conferenza Stato- Regioni e validato dal garante Italiano unitamente alle relative schede di rilevazione mantenute in vigore ai sensi dell'art. 6 par. 2 e 3 del RGPD. Altre tipologie di dati, comuni (diversi da dati particolari e "giudiziari"), sono trattati dall'Azienda nell'ambito di attività amministrative strettamente individuate dalla normativa Europea, Nazionale e Regionale, in conformità al principio di legalità.

Art. 9
Autorizzazione a trattare dati

Se l'interessato ha prestato il consenso esplicito al trattamento dei dati personali per una o più finalità specifiche ovvero qualificabili o qualificate da norme di settore quali attività facoltative ed ulteriori[23], è compito dell'azienda dimostrare che sia stato prestato liberamente a seguito di specifiche e corrette informazioni sul relativo trattamento dati.

[21] Art6 RGPD e consideranda 8, 10 dal 40 al 47 , 50 e 51
[22] Art.28 RGPD punto 4
[23] Art 6 c.1 lett. a) , art 7 RGPD oltre ai consideranda 42 e 43 ed art9 con i consideranda dal 51 al 56 i per consenso si intende : qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, in modo inequivocabile (dichiarazione o azione positiva inequivocabile), a che i dati personali che lo riguardano siano oggetto di trattamento. Circa la disciplina del consenso si rinvia al testo del D. Lgs. n. 101/2018.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta, inerente specifici trattamenti di dati personali, quali a titolo esemplificativo e non esaustivo il Dossier sanitario elettronico[24] ed il fascicolo sanitario elettronico[25], la richiesta di consenso è presentata in modo chiaro, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.
L' Azienda per policy privacy garantisce all' interessato il diritto di conservare, presso di sé, in formato cartaceo un originale del consenso espresso in precedenza, pertanto le strutture aziendali, cui è demandata la raccolta dei consensi, sono tenute a dotarlo di un originale in formato cartaceo. Secondo l'attuale quadro normativo, l'interessato deve autorizzare l'azienda sia a costituire il suo Dossier Sanitario Elettronico (in tal modo ASL 5 è autorizzata a gestire elettronicamente la sua storia clinica da ora in poi) sia ad integrare il suo dossier con i dati di salute raccolti in precedenza da ASL 5 (dal 2010 ad oggi) rendendoli visibili al personale sanitario aziendale.
Il sistema integrato di gestione informatizzata dei consensi, adottato in azienda, quale misura tecnico organizzativa idonea a contenere i rischi di illecito, permette:

- di verificare se gli utenti abbiano fornito le autorizzazioni necessarie che ,richieste una tantum, vengono registrate in procedura e rese visibili agli operatori.
- di segnalare, con alert specifico, agli operatori che l'interessato non ha prestato il proprio consenso sollecitandone la regolarizzare .

L'archiviazione dei consensi, espressi dagli interessati, segue modalità tali da assicurarne la fruibilità, rintracciabilità e consultabilità in formato digitale ed analogico.

Art. 10
Valutazione di impatto [26] e consultazione[27] dell'Autorità Garante[28]

L'Azienda, prima di attivare un nuovo trattamento dati personali, un nuovo progetto ovvero un acquisto che impatti o possa impattare sui dati personali, si assicura che sia effettuata un'apposita e preliminare valutazione delle modalità di impatto sui dati personali (impatto privacy), avvalendosi, qualora necessario, del RPD aziendale.

Tale valutazione viene effettuata nei casi e nei modi previsti dalle disposizioni vigenti, al fine di determinare:

- ✓ i rischi del trattamento;
- ✓ le misure previste per contenerli;
- ✓ le misure di sicurezza ed i meccanismi per garantire la protezione dei dati personali
- ✓ dimostrare la conformità alle norme vigenti, tenuto conto dei diritti degli interessati e delle finalità del trattamento.

Per effettuare la valutazione d'impatto, l'azienda adotta, di norma, il programma gratuito pubblicato sul sito dell'Autorità di Controllo. Qualora, applicando tale sistema, il trattamento presenti, nonostante l'adozione di misure di sicurezza, un rischio elevato, l'Azienda, ai sensi di legge, prima di procedere, consulta l'Autorità, avvalendosi del RPD aziendale .

La documentazione, relativa ad ogni valutazione preliminare di impatto, viene trasmessa al RPD aziendale e va a comporre il Sistema Privacy Aziendale a protezione dei dati. A cadenza periodica, ovvero qualora insorgano elementi di criticità o eventi che possano incidere sul rischio, è previsto il riesame della relativa procedura/progetto per una nuova valutazione.

---

[24] Per DSE si intende la storia clinica di un paziente elaborata da un solo titolare. Per definizione normativa il DSE:
- ✓ non è strumento di cura, posta la possibile non completezza delle informazioni in esso contenute, inserite e rese visibili informaticamente a discrezione dell' utente,
- ✓ è un trattamento dati facoltativo ed ulteriore soggetto ad autorizzazione dell' interessato.

[25] Per FSE si intende la storia clinica di un paziente elaborata da più titolari per definizione normativa il FSE:
- ✓ non è strumento di cura, posta la possibile non completezza delle informazioni in esso contenute, inserite e rese visibili informaticamente a discrezione dell' utente,
- ✓ è un trattamento dati facoltativo ed ulteriore soggetto ad autorizzazione dell' interessato

[26] Art.35 RGPD e consideranda 84,89,93,95
[27] ART.36 RGPD e Consideranda 94 e 96
[28] Autorità Garante Privacy»: l'autorità pubblica indipendente deputata al controllo del rispetto della normativa vigente in materia di protezione dei dati personali.

L'Azienda adotta inoltre le azioni necessarie a garantire la puntuale osservanza di misure e prescrizioni specifiche individuate dall'Autorità Garante, con particolare attenzione ai trattamenti resi possibili dai processi di innovazione digitale e dai diversi modelli di sistemi informativi sanitari integrati.

Art. 11
Informazioni all'interessato

Per qualsiasi trattamento di dati personali in ambito aziendale, siano essi :dati comuni, sanitari, riguardanti particolari categorie o giudiziari, è indispensabile somministrare all'interessato le informazioni di cui agli artt. 13 e 14 del RGPD. L'Azienda, riguardo ai trattamenti dati effettuati, predispone informazioni chiare e comprensibili volte a fornire, all'interessato, con un linguaggio semplice, conciso, trasparente ed accessibile, gli elementi relativi al trattamento necessari a formarne il libero convincimento ovvero a conoscere come l'azienda tratti i dati.
Le informazioni sul trattamento dei dati personali debbono riguardare almeno quanto normativamente previsto ossia:

- identità e dati di contatto del Titolare del trattamento e del RPD Aziendale;
- finalità del trattamento cui sono destinati i dati personali, nonché la base giuridica del trattamento;
- modalità di trattamento dei dati personali;
- obbligatorietà o meno del conferimento dei dati e le connesse possibili conseguenze derivanti dal loro mancato conferimento;
- il periodo di conservazione dei dati personali ovvero i criteri utilizzati per determinarlo ;
- coloro ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- se la comunicazione di dati personali è un obbligo legale ovvero contrattuale o un requisito necessario per la conclusione di un contratto;
- diritti e loro modalità di esercizio da parte dell'interessato ivi incluso il diritto di accesso ai propri dati e quello di reclamo all'Autorità Garante;
- diritto di oscurare i dati riguardanti particolari categorie ovvero soggetti a maggior tutela prima e dopo il loro inserimento a sistema ovvero di de-oscurarli in qualsiasi momento;
- il diritto di revocare, in qualsiasi momento, il consenso già prestato in tutto o in parte ;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione[29] e, almeno in tali casi, le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato;
- la fonte da cui hanno origine ovvero l'indicazione se i dati provengono da fonti accessibili al pubblico nel solo caso in cui i dati personali non siano stati ottenuti presso l'interessato.

In ragione del principio di economicità, le informazioni possono essere fornite in forma unificata, anche per più trattamenti, secondo procedure e modelli concordati con il RPD, attraverso:

- ✓ appositi documenti, in forma integrale e per estratto,
- ✓ manifesti affissi nei locali aziendali, ad accesso pubblico di maggior transito,
- ✓ la pubblicazione sul sito aziendale.

ASL 5 inoltre, tramite il sito aziendale ed Intranet, rende visibili ad utenti e dipendenti le iniziative assunte per applicare le prescrizioni in materia di protezione e riservatezza dei dati.
Le informazioni sul trattamento dei dati personali non vengono rilasciate all'interessato nel caso in cui questi già ne disponga o nel caso in cui comunicarle risulti impossibile o implichi uno sforzo sproporzionato, con particolare riguardo al trattamento finalizzato alla statistica, all' archiviazione nel pubblico interesse, alla ricerca scientifica e storica. In tali casi è necessario adottare , anche alla luce del principio di minimizzazione[30], misure tecniche e organizzative adeguate per la protezione dei dati, la tutela dei diritti e, delle libertà degli interessi legittimi degli interessati.

[29] Per profilazione si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti
[30] Il principio di minimizzazione nell' uso dei dati prevede che questi debbano essere sempre adeguati, pertinenti e limitati a quanto strettamente necessario per perseguire finalità per cui sono raccolti e trattati Resta fermo che tale valutazione è da effettuarsi caso per caso ovvero per categorie di dati anche in correlazione a reali esigenze operative a cui non si possa sopperire in modo differente.

Art. 12
Diritti dell'interessato e loro esercizio[31]

Per le questioni relative al trattamento dei dati personali ed all'esercizio dei relativi diritti, gli interessati, possono, a norma di legge, contattare il Titolare ovvero il RPD Aziendale, in nome proprio o tramite loro rappresentanti (persone fisiche o associazioni) a ciò delegati per iscritto anche con procura. Il Responsabile per la protezione dei dati, avvia il procedimento, avvalendosi dell'apporto e della collaborazione del Responsabile (interno/ esterno) del trattamento dei dati, ovvero dell'Amministratore di Sistema in ragione delle relative competenze.
L'esercizio dei diritti, riferito a dati personali concernenti persone decedute, è esercitabile da chiunque rechi un interesse giuridicamente rilevante, ferma restando la tutela cui soggiacciono taluni tipi di dati che, per il loro contenuto particolarmente pregiudizievole, potrebbero ledere l'immagine stessa del de cuius .
L'interessato ha diritto di ottenere dall'Azienda la conferma che sia o meno in corso un trattamento dati personali che lo riguarda ed ottenere, in tal caso, l'accesso ai dati personali e alle informazioni di cui al precedente art.11
Ha diritto inoltre di chiedere ed ottenere, a termini e secondo le disposizioni normative vigenti:

- la rettifica[32] dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- la limitazione[33] del trattamento dei dati personali che lo riguardano ossia una sospensione del loro trattamento mediante contrassegno informatico con l'obiettivo di limitarne il trattamento in futuro
- la cancellazione[34] dei dati personali che lo riguardano senza ingiustificato ritardo a cui , ricorrendone i presupposti , corrisponde l'obbligo, in capo al titolare di cancellarli senza ritardo;
- di opporsi[35] in qualsiasi momento al trattamento dei dati personali che lo riguardano a cui corrisponde , in capo all' azienda l' onere di astenersi dal trattarli ulteriormente salvo che dimostri l'esistenza di motivi

---

[31] I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
2. L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla

[32] Articolo 16 RGPD Diritto di rettifica: L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

[33] Perché l'interessato possa esercitare tale diritto deve ricorrere almeno una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali;
- i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al titolare del trattamento non servono più a fini del trattamento;
- l'interessato si è opposto al trattamento e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato.

In ciascuno di questi casi i dati possono essere trattati soltanto ai fini della loro conservazione, a meno che non vi sia il consenso dell'interessato o se tale trattamento sia necessario per "l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione Europea o di uno Stato Membro" (Art. 18 par 2 GDPR).Nel caso in cui i dati personali oggetto di limitazione siano stati comunicati ad altri soggetti, è onere del titolare del trattamento darne comunicazione a ciascuno dei destinatari, a meno che ciò sia impossibile o implichi uno sforzo sproporzionato (Art. 19 GDPR) . In ogni caso, il titolare del trattamento è tenuto a comunicare tali destinatari all'interessato che ne faccia richiesta. In un secondo momento la limitazione può essere revocata: prima che la revoca sia efficace però, il titolare del trattamento deve avvisare l'interessato.
modalità per limitare il trattamento dei dati personali:

- ✓ trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento;
- ✓ rendere i dati personali selezionati inaccessibili agli utenti;
- ✓ rimuovere temporaneamente i dati pubblicati da un sito web

Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato". (considerando67)

[34] se sussiste uno dei motivi seguenti:
a)i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b)l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c)l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1,del reg europeo e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2 del reg europeo;
d)i dati personali sono stati trattati illecitamente;
e)i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f)i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione

[35] diritto dell'interessato di opporsi in qualsiasi momento, e per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano; conseguenza dell'esercizio di tale diritto è l'obbligo, in capo al titolare, di astenersi dal trattamento dei dati. Questo particolare diritto riguarda però situazioni in cui il titolare sta lecitamente trattando dei dati personali: pertanto, è riconosciuta la facoltà per il titolare di dimostrare che i suoi interessi specifici connessi al trattamento prevalgono su quelli evidenziati dall'interessato.

legittimi cogenti prevalenti su interessi, diritti e libertà dell'interessato tra cui l'accertamento, ovvero l'esercizio o la difesa di un diritto in sede giudiziaria;

- la portabilità[36] dei dati ossia di ricevere i dati personali che lo riguardano, detenuti dall' azienda , in formato strutturato, di uso comune e leggibile da dispositivo automatico ovvero che vengano trasmessi ad altro titolare del trattamento;
- il diritto di proporre reclamo all'Autorità di Controllo[37];
- il diritto di revocare, in qualsiasi momento, in tutto o in parte, un consenso espresso in precedenza, in qualsiasi momento senza particolari formalità, anche compilando il modulo pubblicato ed inoltrandolo all' UREP ovvero al RPD dell' azienda. La revoca non comporta pregiudizio sul trattamento dati antecedentemente effettuato che resta lecito a tutti gli effetti;
- il diritto a non rendere visibili documenti sanitari che lo riguardano tramite il loro oscuramento .

Art. 13
Accesso agli atti e riservatezza

ASL 5, in conformità alle disposizioni vigenti in tema di riservatezza e di trasparenza, valuta, anche con riguardo ad altre norme e regolamenti specifici, caso per caso, la possibilità che soggetti terzi, ossia diversi dall'interessato accedano a documenti sanitari detenuti dall'azienda.
L'accesso ai dati/ documenti idonei a rivelare lo stato di salute o le abitudini sessuali è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, sia almeno di pari rango rispetto al diritto alla riservatezza ovvero consista in un diritto della personalità/altro diritto inviolabile o libertà fondamentale, quale ad esempio il diritto alla difesa considerato nella sua attualità ed immediatezza.

Art. 14
Comunicazione[38] dati all'Interessato

L'interessato ha il diritto di accedere ai propri dati/documenti, con particolare riferimento a quelli afferenti la salute, nell'immediato ovvero non appena formati, a semplice richiesta e senza particolari formalità.
Le relative comunicazioni possono avvenire attraverso:

a) la consegna di dati/documenti da parte del personale medico o di reparto;
b) una spiegazione orale o un giudizio scritto da parte di personale sanitario ovvero uno specialista;
c) modalità telematiche nei casi e nei modi previsti da norme di settore;
d) e-mail se espressamente indicata ed assentita dall'interessato;
e) altre modalità tecnico organizzative adottate dall'azienda per migliorare l'accessibilità dell'interessato ai propri documenti.

La documentazione sanitaria analogica, da consegnare in busta chiusa, può essere ritirata dall'interessato o da altra persona purché da questo delegata per iscritto, salvo il caso di documenti relativi a dati soggetti a specifiche norme che prevedono il ritiro diretto da parte del solo interessato.

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, ovvero per email purché sia comprovata, con altri mezzi, l'identità dello stesso.

Art. 15
Comunicazione[39] dati di salute a terzi[40] indicati dall'Interessato

---

[36] Nei seguenti casi :
- ✓ se il trattamento si basa sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);
- ✓ se il trattamento è effettuato con mezzi automatizzati.

L'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. L'esercizio di tale diritto non deve ledere i diritti e le libertà altrui.

[38] «comunicazione»: I dare conoscenza dei dati personali ad uno soggetto determinato diverso dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati/autorizzati, in qualunque forma, anche mediante loro messa a disposizione o consultazione;

[39] "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati/autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

[40] «terzo»: la persona fisica o giuridica, l'autorità pubblica, altro organismo che non sia l'"interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Per agevolare la continuità nelle cure, l'azienda, può estendere la visibilità on line dei documenti sanitari al MMG/PLS che ha in cura il paziente, se autorizzata dal paziente stesso, con espresso consenso, e se il MMG/PLS ha accettato la designazione a responsabile (esterno) del trattamento dati. Tale autorizzazione è valevole anche per i sostituti del medico curante limitatamente al tempo di sostituzione, e non si estende di default ad altri medici che fanno parte dello stesso gruppo ovvero AFT/UCCP .
Per permettere la comunicazione dei dati sanitari ad altre persone che non siano il paziente, l'azienda tramite i propri operatori, con il consenso espresso dello stesso, può comunicare i dati di salute che lo riguardano, ovvero il reparto di cura in cui è ricoverato alla/alle persone da questo espressamente indicate anche nominalmente.
Tale espressione di volontà, raccolta una tantum in formato cartaceo e registrata digitalmente, è visibile a tutti gli operatori dell'azienda. Le persone indicate possono essere modificate dall'interessato anche in relazione al singolo evento (ricovero), rivolgendosi al personale aziendale per la registrazione, in procedura, della nuova volontà manifestata. Tale modifica è valevole limitatamente al singolo evento.

Art. 16
Comunicazione dati all'esterno

La comunicazione dei dati personali all'esterno di ASL 5 è effettuata esclusivamente ad enti o aziende del SSR e del SSN della Pubblica Amministrazione e ad altri soggetti di natura pubblica e privata, in esecuzione di obblighi derivanti da norme vigenti ovvero per svolgere le funzioni istituzionali di cui al precedente art. 3. La suindicata trasmissione dei dati personali avviene in forma scritta ovvero telematica. E' vietata, senza le garanzie e le procedure di legge, ovvero in elusione a tali norme, ogni forma di comunicazione/trasferimento dati con paesi terzi ovvero extra U.E.

Art. 17
Registro delle attività di trattamento

L'azienda è tenuta, per legge, a censire le attività di trattamento, svolte sotto la propria responsabilità, redigendo ed aggiornando, a cadenza programmata, il relativo registro.
Il Registro è tenuto in forma scritta ed in formato elettronico e, su richiesta, è messo a disposizione dell'Autorità di controllo per la protezione dei dati.

Il documento deve contenere almeno le seguenti informazioni:

- nome e i dati di contatto del Titolare del trattamento, del RPD e del Contitolare del trattamento, ove applicabile;
- trattamenti svolti in ragione di SC / SSD;
- finalità del trattamento anche di pubblico interesse;
- categorie di interessati e di dati personali trattati;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati[41];
- eventuali trasferimenti di dati personali verso un paese terzo e la documentazione delle garanzie adeguate;
- termini di conservazione dei dati e quelli previsti per la cancellazione in ragione delle diverse categorie;
- analisi dei rischi in ragione della gravità e della probabilità che si verifichino[42];
- probabilità e gravità dell' incidenza dei rischi sui trattamenti;
- misure di sicurezza tecniche ed organizzative adottate per proteggere i dati personali oggetto di trattamento, ovvero adottande quale correttivo;
- modalità di esercizio dei diritti garantite agli utenti.

Art. 18
Politica di sicurezza aziendale[43]

[41] il destinatario della comunicazione spesso coincide con il responsabile esterno
[42] analisi dei rischi in ragione della gravità e della probabilità che si verifichino e probabilità e gravità dell' incidenza dei rischi sui trattamenti costituiscono la DVRA di cui al successivo art.29

L'Azienda, attesa la molteplicità di informazioni trattate è l'alto numero dei soggetti che necessariamente le gestiscono, adotta misure di sicurezza, tecniche ed organizzative adeguate e tali da assicurare e poter documentare che il trattamento dati è svolto con modalità tali da preservarne l'integrità e la confidenzialità.
Al riguardo ASL 5 attiva le necessarie risorse organizzative, tecnologiche e finanziarie, nei limiti delle disponibilità aziendali, in un percorso programmato di adeguamento e miglioramento graduali, affinché il trattamento dati personali, svolto sotto la propria autorità, sia conforme alle disposizioni vigenti in materia di protezione dei dati, di amministrazione digitale e vengano osservati i seguenti principi:

- «liceità, correttezza e trasparenza», cioè i dati siano trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- «limitazione della finalità », cioè siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con la finalità per cui sono stati raccolti;
- «minimizzazione dei dati», cioè debbono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- «esattezza», cioè siano esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti/ non conformi rispetto alle finalità del trattamento;
- «limitazione della conservazione», cioè siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità perseguite con il trattamento . Vengono fatte salve le norme di legge che impongono tempi di conservazione più lunghi ovvero per l'archiviazione di pubblico interesse, ricerca scientifica, storica o a fini statistici. In tali casi vengono attivate le misure tecniche ed organizzative adeguate richieste dalle norme di settore ovvero dal regolamento europeo a fini di tutela dei diritti e delle libertà dell'interessato;
- «integrità e riservatezza», cioè trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati ovvero ingiustificati o illeciti nonché dalla perdita, distruzione o danno accidentali;
- «responsabilizzazione[44]», cioè adottando le misure tecniche ed organizzative idonee ed essendo in grado di dimostrare che il trattamento dei dati viene svolto nel pieno rispetto della normativa vigente.

Art. 19
Responsabilità civile

Il Regolamento Europeo (UE) 2016/679 conferma il trattamento dei dati personali come attività pericolosa disciplinata dall'art.2050[45] del codice civile. La relativa responsabilità, aggravata dall'inversione dell'onere della prova[46], comporta, in capo a chi detiene i mezzi per gestire le modalità di trattamento[47], l'obbligo di risarcire i danni, patrimoniali e non, provocati all'interessato in conseguenza del trattamento stesso.
Ne consegue che il danno contestato non dà luogo a risarcimento se il titolare può dimostrare di aver adottato misure organizzative e di sicurezza efficaci ed adeguate (idonee) a prevenirlo, in relazione al progresso tecnologico e scientifico esistente all'epoca dei fatti, salva l'eccessiva onerosità delle stesse riferita alla capacità economica del titolare ovvero del responsabile del trattamento[48].
Nel caso in cui il trattamento violi le disposizioni del Regolamento UE e le norme nazionali vigenti in materia di privacy i soggetti, eventualmente responsabili, e quindi tenuti al risarcimento economico del danno possono essere il Titolare, il Contitolare ed il Responsabile del trattamento . Quest'ultimo, inoltre, risponde anche nel caso in cui agisca in modo difforme, ovvero contrario, rispetto alle legittime istruzioni impartite dal titolare.
Tale previsione normativa evidenzia l'importanza, per il titolare, di valutare le caratteristiche organizzative e le competenze del soggetto che verrà nominato responsabile del trattamento in una parola la sua affidabilità. Tale nomina ha natura di mandato e consiste nella designazione da parte del Titolare del soggetto delegato a trattare dati personali in vece propria. La ripartizione della responsabilità civile e dell'onere della prova, nel

[43] Art.32 RGPD e Considerandum 83 ed artt. 5 e 6 RGPD
[44] Principio dell'Accountability
[45] Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.
[46] È una responsabilità aggravata che prevede l'inversione dell'onere della prova ossia incombe sul titolare e sul responsabile l'onere di dimostrare di aver adottato tutte le misure idonee in relazione al progresso tecnologico per evitare il danno mentre l' interessato "leso" deve solo provare il nesso di causalità diretta tra il trattamento dei dati ed il danno subito
[47] ossia il Titolare/il contitolare / il responsabile del trattamento o entrambi in solido
[48] CFR articolo 82 del Regolamento europeo

rapporto tra titolare e responsabile si basa sul contenuto della nomina stessa[49]. Il danno risarcibile di natura non patrimoniale è dovuto nel solo caso in cui risulti superato il livello di tollerabilità ed il pregiudizio non possa ritenersi futile[50]. L'accertamento e la quantificazione del danno, sono rimessi al giudice di merito in relazione alle prove prodotte, ed al contesto temporale e sociale.
Pertanto, nella scelta del modello organizzativo privacy e degli interlocutori dell'azienda, diventano elemento determinante gli orientamenti giurisprudenziali, l'analisi della probabilità e la gravità del rischio legato al trattamento del dato personale, la connessa responsabilità civile ed il conseguente impatto economico legato alla quantificazione del danno, patrimoniale e non, e da ultimo , ma non per ultimo i precedenti ed i provvedimenti con cui l'Autorità di controllo ha risolto / sanzionato casi consimili .

Art. 20
Organigramma aziendale privacy

Premesso che il Regolamento Europeo (UE) 2016/679 dispone che il trattamento dei dati possa essere effettuato esclusivamente da soggetti autorizzati dal titolare, l'azienda, considerando la complessità organizzativa ed il numero di soggetti da autorizzare, per continuità gestionale, conferma il sistema di deleghe interne e la nomenclatura, quale adottata con il precedente regolamento[51] , poiché non in contrasto con le disposizioni europee .
Tale sistema individua i collaboratori, dotati dei requisiti di esperienza, capacità e affidabilità, normativamente previsti, ed evidenzia i diversi livelli di responsabilità loro attribuiti in relazione al trattamento dati di competenza.
All'interno dell'azienda essi si distinguono in: Responsabili interni ed Incaricati/Autorizzati del trattamento ed Amministratori di sistema ed all'esterno in Contitolari, Responsabili esterni e Sub-Responsabili.

L'Azienda designa i soggetti autorizzati a trattare dati, attraverso atti formali, accompagnati da specifiche indicazioni operative per il corretto svolgimento dei compiti delegati in materia di protezione dei dati. La funzione di Responsabile, Sub-Responsabile, incaricato/autorizzato del trattamento dati è attribuita ad personam e non è suscettibile di delega; le designazioni sono conservate dai servizi di appartenenza che tiene nell'elenco nominale trasmesso annualmente al RPD.

Art. 21
Responsabili (interni)[52] delegati dall'Azienda a trattare i dati

I Dirigenti di Struttura Complessa ed i Responsabile di Struttura Semplice Dipartimentale, già designati Responsabili del trattamento dati a norma del D.L.gs 196/2003, vengono confermati in tale veste sino a revisione degli incarichi ovvero della modulistica di designazione.
In casi eccezionali ed in ragione di particolari dislocazioni organizzative, la Direzione Aziendale, su proposta motivata del Direttore di Dipartimento o del Dirigente di Struttura Complessa, può designare, per iscritto, quale Responsabile del trattamento anche un Responsabile di Struttura Semplice ovvero un Dirigente.
I dipendenti dell'Azienda, autorizzati all'attività intra-moenia nelle strutture aziendali o private convenzionate, ed i Responsabili degli studi clinici ed osservazionali, limitatamente ai trattamenti che derivano da tali attività, sono considerati Responsabili interni del trattamento dati.
La nomina a responsabile interno del trattamento dati è effettuata dal Titolare con atto predisposto dal RPD aziendale in cui vengono indicati, in termini riassuntivi e specifici, i trattamenti dati dei quali viene conferita la responsabilità e le relative istruzioni.
Le Strutture Aziendali, deputate alla gestione delle risorse umane, delle attività intra-moenia e degli studi clinici ed osservazionali trasmettono tempestivamente al RPD ogni conferimento o modifica di responsabilità, in ambito

[49] Quest'obbligo è ribadito anche in caso di esternalizzazione della conservazione dei documenti informatici e, quindi, dei connessi dati personali. Infatti, le regole tecniche (Decreto del Presidente del Consiglio dei Ministri 3 Dicembre 2013 e ss mmii) sui sistemi di conservazione dei documenti informatici, dispongono che il processo di conservazione possa essere affidato ad un soggetto esterno mediante un contratto di servizio che preveda gli obblighi e le responsabilità e che quest'ultimo dovrà assumere il ruolo di responsabile del trattamento
[50] Le recenti decisioni della Cassazione (Cassazione civile, sez. I, 23/05/2016, n. 10638 Cassazione civile, sez. III, 13/10/2016, n. 20615, Cassazione civile sez. VI 11 gennaio 2016 n. 222, Cassazione Civile, sez. III, sentenza 15/07/2014 n° 16133) nello specificare che il danno patrimoniale derivante dal trattamento dei dati personali non si sottrae alla verifica della gravità della lesione e non può mai ritenersi in re ipsa, ma va debitamente allegato e provato da chi lo invoca, riducono le cause delle c.d. liti "bagatellari"
[51] Adottato con deliberazione n.244 del 14.3.2017.
[52] la persona fisica che tratta dati personali ,per conto del titolare del trattamento ,al quale è affidato il coordinamento e la vigilanza delle operazioni di trattamento dei dati personali effettuate dagli Incaricati/Autorizzati sottoposti alla sua direzione.

aziendale, affinché questi possa predisporre gli atti necessari alla relativa designazione. Il precedente iter e la correlata modulistica vengono abrogati per inconferenza con l'attuale sistema normativo.

I Responsabili interni possono trattare i dati personali soltanto se designati ed istruiti formalmente da ASL 5 ancorché, nell'ambito della sfera di competenza e dei connessi trattamenti, comprensivi dell' accesso alle relative banche dati, siano dotati di autonomia gestionale ed organizzativa.
Essi sono tenuti a:

1. rispettare e garantire, relativamente ai trattamenti assegnati, l'applicazione delle norme in materia di protezione delle informazioni, delle ulteriori linee guida in materia di riservatezza sui dati, ed inerenti l'amministrazione digitale ovvero previste nel presente Regolamento
2. rispettare e garantire, relativamente ai trattamenti assegnati, l'applicazione delle misure di sicurezza previste nel Registro dei trattamenti adottando ogni misura necessaria con particolare attenzione all'erogazione di prestazioni e servizi sanitari ;
3. trattare i dati alla luce dei principi di cui all' art.18 ed in particolare secondo il criterio di indispensabilità, per il solo tempo necessario al ricovero/all'erogazione di prestazioni/cura/terapia;
4. vigilare:
   a) sugli incaricati/autorizzati, sottoposti alla propria autorità, affinché applichino pari principi e rispettino il diritto degli interessati ad essere informati, a manifestare liberamente il proprio consenso, e ad esercitare il diritto di oscuramento sui singoli documenti;
   b) sul corretto uso di sistemi e procedure digitali utilizzati dai sottoposti per gestire i dati necessari all'attività lavorativa;
5. mettere a disposizione dell'azienda tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e contribuire alle attività di revisione, comprese le verifiche / audit, da questa effettuate;
6. verificare:
   a) che la documentazione cartacea e digitale e le procedure informatizzate, a supporto dell'attività di trattamento dati di propria competenza, rispondano ai principi di necessità, pertinenza e non eccedenza;
   b) periodicamente, l'esattezza e l'aggiornamento dei dati personali, nonché la loro pertinenza, completezza, non eccedenza e necessarietà, rispetto ai fini perseguiti, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa;
7. collaborare con il RPD aziendale comunicando:
   a) i dati e le informazioni necessarie per valutare le richieste avanzate dagli interessati, con particolare riferimento all'esercizio dei diritti, all'accesso ai propri dati, alla revoca dei consensi etc. ;
   b) le misure organizzative adottate ovvero le istruzioni interne e le indicazioni di comportamento per il proprio personale, per i pazienti e per i visitatori ;
   c) che un istruzione ricevuta viola il presente regolamento o altre disposizioni vigenti relative alla protezione dei dati personali, ovvero eventuali difficoltà emerse nell'applicazione di norme e procedure , utilizzando e- mail appositamente predisposta,
   d) periodicamente in merito allo svolgimento dei compiti specifici assegnati inclusa ogni problematica ad essi riferita;
   e) l'inizio o la cessazione di trattamenti di dati personali, al fine di permettere l'aggiornamento del Registro delle attività di trattamento dei dati personali;
8. collaborare, direttamente, ovvero tramite un referente, alla redazione del registro dei trattamenti svolti nella propria area di competenza, ai suoi aggiornamenti ed al censimento delle procedure e delle banche dati utilizzate fornendo, tempestivamente, le informazioni necessarie alla direzione aziendale;
9. designare, per iscritto, sotto la supervisione del RPD aziendale, gli operatori che agiscono sotto la propria direzione, incaricati/autorizzati del trattamento, secondo livelli differenziati e profili omogenei ed avendo cura di individuare compiti e mansioni cui sono adibiti al fine di formulare correttamente le istruzioni da impartire per trattare i dati;

10. registrare le designazioni effettuate in apposito elenco da aggiornare, ogni qual volta si renda necessario per avvicendamento/sostituzione/trasferimento dei sottoposti ed inviarne copia al RPD aziendale che provvede a conservarlo;
11. custodire gli atti di cui ai punti 9 e 10 in apposito contenitore esibire in caso di verifica interna ovvero di ispezione del Garante;
12. curare, fra gli incaricati/autorizzati del trattamento sottoposti alla loro autorità la diffusione di norme, linee guida e di ogni altra disposizione impartita dall'Azienda anche organizzando la formazione di reparto/dipartimento mirata all'aggiornamento continuo ed obbligatorio in materia di privacy, previsto per legge;
13. designare un Referente Privacy di struttura con finalità di supporto indicandone il nominativo al RPD;
14. rispondere al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale.

Art. 22
Incaricati /Autorizzati a trattare i dati

Le persone fisiche che, nelle singole Strutture, svolgono materialmente le operazioni di trattamento dati devono essere autorizzate in tal senso come "Incaricati/ Autorizzati del trattamento dati" dal responsabile del trattamento. Sono da designare Incaricati/ Autorizzati i dipendenti dell'azienda ed i collaboratori che, a qualsiasi titolo, prestano la loro opera, anche in via temporanea, all'interno delle strutture aziendali (ad esempio: tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti, consulenti, lavoratori interinali) o che comunque agiscono sotto l'autorità dell' Ente .
Per la designazione scritta è utilizzata apposita modulistica, da produrre, caso per caso, elaborata anche in ragione di compiti e funzioni proprie di determinate categorie, in collaborazione con il RPD aziendale.
Essa prevede:

- ✓ la data di inizio ed eventuale termine dell' attività all'interno della struttura;
- ✓ in modo sintetico, i trattamenti dati autorizzati, le banche dati e le procedure informatizzate cui si ha accesso in ragione del profilo e delle mansioni assegnate;
- ✓ specifiche e dettagliate istruzioni operative, riguardo alle corrette modalità di trattamento dati, in ragione del profilo ricoperto, dell' attività svolta, delle funzioni e delle competenze attribuite con particolare riguardo alle misure di sicurezza da osservare.

Gli Incaricati/ Autorizzati possono accedere ai soli dati indispensabili per assolvere alle attività istituzionali cui sono preposti che debbono trattare in conformità alla vigente normativa, al presente Regolamento ed alle disposizioni impartite dal Responsabile interno del trattamento.
Essi sono tenuti a:

- ✓ comunicare dati personali e/o sensibili agli altri soggetti autorizzati al trattamento solo in caso di necessità, ovvero quando non sia possibile perseguire gli stessi fini con dati anonimi o aggregati.
- ✓ conservare i dati personali sia su supporto analogico che digitale solo per il tempo previsto dalla normativa vigente e successivamente devono sottoporli a scarto d'archivio o distruzione.
- ✓ non permettere il trattamento dei dati personali che, anche a seguito di verifica, risulti eccedente, non pertinente ovvero non necessario, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
- ✓ trattare i dati osservando le istruzioni ricevute, anche con riferimento agli aspetti relativi alla sicurezza;
- ✓ qualora trattino dati con l'ausilio di strumenti informatici sono personalmente responsabili della gestione riservata della password loro assegnata, con divieto di cederla a terzi ovvero a colleghi;
- ✓ sono responsabili della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento con l' onere di restituirli e conservarli al termine dell' attività / orario di lavoro
- ✓ sono responsabili di ogni attività sui dati inerente/ derivate dall' attività di servizio .

L'atto di designazione ad Incaricato/ Autorizzato costituisce l'unico presupposto di liceità per il trattamento dei dati personali.

L 'originale di tale atto, controfirmato per presa visione dall'incaricato/autorizzato, è conservato presso il reparto/ servizio di assegnazione e riportato in un elenco trasmesso al RPD, che ne cura la conservazione e ne collega i dati al Registro delle attività di trattamento.

Art. 23
Amministratori di sistema[53]

L'Azienda e, per essa, il direttore del SIA

- designa gli Amministratori di Sistema con appositi atti corredati da istruzioni operative, conservati in originale presso il SIA stesso e comunicati in elenco al RPD che provvede a collegarli con il registro dei trattamenti e
- impartisce le opportune disposizioni perché sia assicurata l'effettività di tutte le misure e gli audit previsti dalla normativa vigente in tema di Amministratore di Sistema.

Gli Amministratori di Sistema sono tenuti, di norma, a rilasciare agli Incaricati/Autorizzati le credenziali per accedere alle procedure informatiche previa richiesta sottoscritta Responsabile del trattamento di riferimento
Gli stessi sono inoltre tenuti a inoltrare le richieste suindicate al RPD che ne verifica la congruità e le conserva unitamente agli originali degli atti di nomina ad Incaricato/Autorizzato.
I soggetti giuridici designati Responsabili esterni e Sub-Responsabili del trattamento cui sono state delegate competenze di gestione e protezione dei sistemi informativi e delle risorse hardware e software dell'azienda sono onerati di designare e coordinare l'attività dei propri Amministratori di Sistema e di provvedere a tutti gli adempimenti in materia previsti dalla normativa vigente, ivi incluso il rispetto delle misure sul controllo dell'attività.
Tali Responsabili esterni e Sub-Responsabili sono pertanto tenuti ad adottare le misure necessarie , ad assolvere agli audit previsti dalla normativa vigente in tema di Amministratore di Sistema ed a trasmettere al Titolare del trattamento evidenza delle nomine, delle ulteriori misure adottate e la relativa documentazione entro il mese di gennaio di ogni anno solare. Responsabili e Sub-Responsabili del trattamento sono tenuti a depositare presso il RPD la copia degli atti con cui hanno designato gli Amministratori di Sistema.

Art. 24
Formazione

L'Azienda, in ottemperanza al dettato normativo, inserisce nel proprio Piano Annuale di Formazione iniziative atte ad assicurare la formazione finalizzata al continuo aggiornamento di Responsabili interni, Soggetti designati ex D. L.gs. n. 101/2018, Incaricati/Autorizzati del trattamento da ed Amministratori di Sistema nonché del personale di nuova assunzione sul tema della protezione dei dati personali, dei diritti, doveri ed adempimenti previsti dalla vigente normativa.
I Responsabili interni ovvero i direttori di dipartimento organizzano all'interno della formazione dipartimentale o di Struttura complessa sessioni di formazione dedicate a temi specifici di rilevante interesse
Responsabili esterni e subdelegati del trattamento sono comunque tenuti a assicurare all' azienda che gli incaricati/autorizzati e gli Amministratori di Sistema che svolgono attività di trattamento di dati personali su loro mandato siano formati e continuamente aggiornati; di tale formazione dovrà essere data evidenza, su richiesta, al Titolare del trattamento.

Art. 25
Responsabili (esterni) del trattamento dati

Il Regolamento (UE) 2016/679 dispone all'articolo 28 che ogni Titolare del trattamento designa quale Responsabile del trattamento il soggetto esterno cui affida un'attività di trattamento dei dati personali.
ASL 5, in qualità di Titolare del trattamento, designa, con un apposito atto, Responsabili (esterni) del trattamento dati personali i soggetti esterni cui sono conferite attività di competenza aziendale o attività connesse, strumentali

[53] Persona fisica alle dipendenze del titolare che svolge funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (*system administrator*), amministratore di base di dati (*database administrator*) o amministratore di rete (*network administrator*), laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Tale designazione, a carattere individuale avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.,

e di supporto, ivi incluse quelle manutentive, che comportino necessariamente il trattamento di dati personali, esclusivamente in presenza delle garanzie di affidabilità, da verificarsi caso per caso, sufficienti ed idonee ad attuare misure tecniche ed organizzative adeguate a che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'interessato.
Tale atto, stipulato in forma scritta, vincola il Responsabile e l'eventuale Sub-Responsabile del trattamento all'Azienda, con particolare riferimento almeno a: durata, natura, finalità del trattamento, categorie di interessati, tipo di dati personali trattati, modalità di conservazione/distruzione degli stessi, obblighi e diritti del Titolare del trattamento, nonché modalità di esercizio dei diritti da parte degli interessati
Prevede inoltre almeno le istruzioni riportate di seguito a titolo esemplificativi e non esaustivo, ossia che il Responsabile del trattamento:

a. tratti i dati personali soltanto su istruzione documentata di ASL 5;
b. si attenga alle specifiche norme di settore ed ai principi di cui al precedente art.18
c. garantisca che i propri incaricati/autorizzati del trattamento dei dati personali mantengano la riservatezza sui dati affidati ;
d. adotti le misure di sicurezza indicate da ASL 5 e le ulteriori misure tecniche e organizzative capaci di garantire ai dati, oggetto di trattamento, un livello di sicurezza adeguato al rischio, tenendo conto del contesto, dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, della finalità del trattamento, della probabilità e gravità del rischio di incidenza sui diritti e le libertà delle persone fisiche;
e. assista ASL 5 con misure tecniche ed organizzative adeguate, tenendo conto della natura del tratta-mento e, nella misura in cui ciò sia possibile, collabori con questa a soddisfare le richieste di esercizio dei diritti da parte dell'interessato;
f. garantisca il rispetto degli obblighi di legge, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
g. al termine della prestazione cancelli o restituisca, come indicato dall'Azienda , i dati personali trattati ed elimini le copie esistenti;
h. fornisca all'azienda e, per essa, al RPD ogni dato ed informazione necessaria ad espletare gli adempimenti normativi previsti dal regolamento europeo e dalla vigente legislazione nazionale nonché quelle necessarie a dimostrare il rispetto degli obblighi di legge;
i. contribuisca alle attività di controllo e revisione, comprese le eventuali ispezioni e gli audit attivati da ASL 5 direttamente, ovvero tramite altro soggetto a ciò incaricato/autorizzato;
j. dimostri di possedere adeguate coperture assicurative volte a risarcire i terzi ovvero l' azienda da eventuali danni inerenti/derivanti dal trattamento dati affidato;
k. segnali all' azienda e per essa al RPD ogni non conformità riscontrata o verificatasi nel trattare i dati entro i termini di cui al successivo art. 33;
l. collabori con l'azienda ad attuare le misure di sicurezza e le previsioni di legge vigenti in materia di protezione dei dati e di amministrazione digitale con particolare riferimento alle misure standard;
m. non delocalizzi le banche dati ed i server deputati alle attività oggetto di affidamento né eluda le vigenti disposizioni in materia di trasferimento dati transfrontaliero;
n. non adotti modalità di conservazione dei dati su cloud senza l'autorizzazione dell'Azienda e la verifica di idoneità del provider;
o. non metta a disposizione i dati affidati a nessun terzo, con ciò intendendo anche gli appartenenti allo stesso gruppo commerciale/societario, posto che, di norma, i dati affidati hanno valenza sanitaria e, quindi, non possono né debbono essere soggetti a condivisione al pari di altre informazioni squisitamente commerciali.

Il Responsabile Esterno risponde dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi e per gli effetti di cui agli artt. 1218 e 1223 del Codice Civile.
Resta fermo che il Responsabile esterno del trattamento dati personali non può delegare il trattamento affidatogli, neppure in parte, ad altri soggetti, denominati Sub-Responsabili esterni, senza preventiva e specifica autorizzazione scritta di ASL 5. Nel caso in cui un Responsabile del trattamento ricorra, previa specifica autorizzazione, ad un Sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto dell'Azienda, al Sub-Responsabile sono imposti, mediante specifico atto , gli stessi obblighi a cui soggiace il Responsabile.

Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti di ASL 5 l'intera responsabilità per l'inadempimento.
Posto che la possibilità di verificare l'affidabilità del responsabile esterno muove dal necessario inserimento, negli atti prodromici[54], a disciplina dei rapporti con gli affidatari di beni e servizi , attività strumentali e di supporto, ivi incluse quelle manutentive, di clausole e requisiti specifici, le strutture aziendali provvedono a segnalare l'affidamento in itinere ed a stendere gli atti di competenza previo concerto con il RPD aziendale affinché questi possa integrare gli atti con clausole privacy e specifiche disposizioni operative a tutela dell'Azienda.
Qualora l'azienda non abbia gestito le procedure di affidamento, ed il contraente sia stato selezionato in esito a gare regionali[55]/nazionali, prima dell' adesione è onerata di verificare, qualora non risultino dagli atti di gara ovvero da contratti quadro, le implicazioni privacy che lo svolgimento del servizio comporta e ciò anche al fine di valutare l'affidabilità dell'aggiudicatario in punto protezione dati a norma del citato art. 28 del Regolamento Europeo.

Art. 26
Responsabili che effettuano operazioni di natura informatica

In particolare, i Responsabili interni, i Responsabili esterni ed i Sub-Responsabili del trattamento che effettuano operazioni di trattamento finalizzate alla gestione, protezione e manutenzione di sistemi informativi e programmi informatici e delle relative banche dati devono assicurare al Titolare del trattamento oltre agli adempimenti di legge almeno quanto sottoelencato a titolo esemplificativo e non esaustivo ossia che:

- i sistemi ed i programmi forniti/aggiornati siano conformi alla prescrizioni generali ed a quelle di settore vigenti in materia di privacy;
- i sistemi ed i programmi siano pre-configurati, in ossequio al già citato principio della "privacy per impostazione predefinita", riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, così da escluderne il trattamento quando le finalità perseguite possano essere realizzate mediante, rispettivamente, dati anonimi o modalità che permettano di identificare l'interessato solo in caso di necessità;
- essi posseggano acconce polizze assicurative con specifica estensione per il risarcimento danni inerenti / derivanti da eventuali violazioni in materia di privacy;
- garantiscano al proprio interno ogni adempimento previsto per legge;
- designino, al proprio interno, gli amministratori di sistema dandone comunicazione al Titolare e, per esso, al SIA ed al RPD aziendali;
- si impegnino a/e garantiscano di non comunicare i dati oggetto di trattamento a terzi salvo espressa autorizzazione dell'Azienda;
- rendano all' Azienda, al termine dell' attività, i dati trattati ovvero li distruggano senza conservarne copia;
- non trasferiscano i dati in paesi terzi senza l'autorizzazione dell' azienda e/o in violazione/elusione delle prescrizioni dettate al proposito dal regolamento europeo;
- avvisino il Titolare di eventuali inconferenze tra le richieste/procedure/sistemi gestiti e le disposizioni di legge vigenti, suggerendo correttivi idonei;
- non deleghino a terzi, anche in parte le attività oggetto dell'incarico senza previa autorizzazione dell'Azienda;
- non utilizzino le attività manutentive per acquisire dati di cui vengano a conoscenza per scopi/utilità finalità proprie differenti da quelle manutentive/conferite ancorché ad esse connesse;
- non utilizzino per la conservazione dei dati, qualora vi siano delegati, cloud ovvero server allocato al di fuori del territorio dello stato ovvero dell'UE senza autorizzazione dell'azienda;
- si rendano parti diligenti nel riscontrare le richieste comunque formalizzate dai servizi aziendali e dal RPD e durante gli audit da questi programmati a sensi di legge;
- adottino e collaborino ad adottare idonee misure di sicurezza.

Art. 27
Il Responsabile Aziendale per la protezione dei dati (RPD) ovvero Data Protection Officer

[54] contratti, convenzioni, scritture private, conferimenti, disciplinari ed atti di gara / selezione pubblica etc.,
[55] ad es gare gestite da Centrale acquisti Regione Liguria , Consip ,Liguria Digitale

Il RPD ovvero DPO aziendale è designato esclusivamente in funzione delle specifiche qualità professionali, della conoscenza specialistica della normativa e delle prassi aziendali in materia di protezione dei dati, nonché delle capacità di assolvere ai compiti individuati dalla normativa vigente.
I dati di contatto sono pubblicati sul sito e introdotti nelle informazioni, nonché comunicati all'Autorità Garante per la protezione dei dati a cura dell' azienda .
In conformità alle indicazioni ed alle disposizioni normative vigenti, l'Azienda e, per essa, i Direttori di SC/Responsabili SSD, garantiscono fattivamente che il RPD aziendale sia tempestivamente e adeguatamente coinvolto nelle questioni riguardanti la protezione dei dati personali, con particolare attenzione alle procedure informatizzate volte a gestire/condividere dati sanitari ovvero reti ingrate per dispensare l'attività sanitaria sul territorio.
A norma di legge la Direzione aziendale fornisce al RPD le risorse, umane, tecnologiche, strumentali ed economiche necessarie per assolvere ai propri compiti, accedere a dati, progetti, trattamenti ed a mantenere la propria conoscenza specialistica.
Il RPD possiede autonomia gestionale, attribuita per legge e garantita dall'azienda, agisce quindi in totale autonomia operativa e si avvale delle risorse umane assegnate, nonché dei Referenti Privacy individuati in ogni singola SC/Area/Dipartimento allo scopo di realizzare una "rete privacy" aziendale adeguatamente diffusa e capillare in tutte le articolazioni territoriali dell'azienda. La S.C. SIA assicura al RPD la massima collaborazione, sia in merito all'applicazione interna delle misure di sicurezza e di protezione dei dati personali per i trattamenti automatizzati, sia in merito agli audit di verifica di applicazione delle stesse misure da parte di Responsabili e Sub-Responsabili.
Il RPD mantiene totale indipendenza ed autonomia, anche ai fini della valutazione dell'adeguatezza delle misure di sicurezza e di protezione dei dati personali per i trattamenti automatizzati. Di concerto ed in stretta collaborazione con il SIA, egli attiva tutte le misure per favorire l'osservanza del presente Regolamento e delle altre disposizioni vigenti relative alla protezione dei dati.
Il RPD svolge di norma i seguenti compiti:

a) riferisce alla Direzione Aziendale le problematiche relative alla protezione dei dati personali proponendo adeguate soluzioni tecnico- giuridiche;
b) informa e fornisce consulenza alla Direzione Aziendale, ai direttori e responsabili di struttura ed agli incaricati/autorizzati del trattamento dati personali in merito agli obblighi derivanti dalla normativa vigente in materia di protezione dei dati;
c) sorveglia sull'osservanza del Regolamento Europeo e delle altre disposizioni vigenti relative alla protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione di Responsabili ed Incaricati/Autorizzati del trattamento e alle connesse attività di controllo;
d) fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento;
e) propone correttivi in merito alla gestione dei dati e collabora, nei limiti delle proprie competenze ad individuare / suggerire soluzioni / percorsi di adeguamento normativo;
f) predispone, anche su impulso della Direzione Aziendale e in stretto raccordo con i responsabili dei servizi interessati modulistica, linee guida, procedure, disposizioni tecnico- operative, registri e policy necessari a rendere operative le indicazioni di legge e del presente Regolamento;
g) coopera e funge da punto di contatto per l'Autorità di controllo per tutte le questioni connesse al trattamento dei dati personali, e ad adempimenti normativi consultandolo quando necessario.

Nell'eseguire i propri compiti il RPD considera debitamente i rischi inerenti al trattamento dei dati, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Art. 28
Accesso alle procedure informatiche aziendali

Fermo restando il crescente ricorso all'informatizzazione per gestire, anche in sanità, una serie di attività strettamente connesse ai dati di salute, anche al fine di evitare accessi non conformi a banche dati sanitarie o amministrative ed a strumenti quale il dossier sanitario elettronico, di cui l'azienda si è dotata, la disciplina degli accessi alle procedure informatizzate, da annoverarsi tra le misure organizzative e tecniche assunte dall'azienda a

tutela dei dati in esse contenuti, assume particolare rilievo.
L'accesso ad ogni procedura informatica è consentito solo se congruente con il trattamento di dati per il quale il collaboratore/operatore di ASL 5 è stato precedentemente designato Incaricato/Autorizzato del trattamento e soltanto utilizzando apposite credenziali di autorizzazione composte da un *user-id*. La richiesta è attivata inoltrando al SIA, almeno nei 7 giorni antecedenti la data di attivazione, il modulo compilato e firmato dal proprio Responsabile, all'indirizzo di posta elettronica: richiestaaccesso@asl5.liguria.it.
Il direttore della S.C. richiedente e, per esso, il coordinatore è tenuto a verificare, in via preliminare, che l'autorizzando risulti incaricato/autorizzato al trattamento dati con specifica abilitazione anche alla procedura informatica per cui è richiesto l'accesso.
Nel caso in cui la richiesta di credenziali riguardi una Struttura esterna ovvero, un Medico di medicina generale o Pediatra di libera scelta, il direttore di S.C. competente deve accertare che gli stessi siano già designati "responsabili esterni del trattamento dati" con specifica abilitazione alla procedura informatica per cui è richiesto l'accesso. In caso contrario, è tenuto ad attivarsi per effettuare designazione, in collaborazione con il RPD aziendale.
Si precisa, che, per obbligo normativo i soggetti carenti di autorizzazione non possono trattare i dati, né fruire delle credenziali che, se concesse, debbono essere sospese e/o disattivate.
Il RPD verifica la congruenza tra designazione ad incaricato-autorizzato/responsabile, ruolo e profilo ricoperto, e rilascio delle credenziali formulando le relative osservazioni e disponendo le misure necessarie a ricondurre le attività nell' alveo normativo di riferimento. La password ottenuta è strettamente personale e, a nessun titolo, può essere comunicata / ceduta a terzi ovvero a colleghi; della custodia e del corretto utilizzo risponde personalmente il singolo incaricato/autorizzato del trattamento dei dati personali.
Il Responsabile del trattamento dei dati è tenuto a comunicare agli Amministratori di Sistema ed al RPD la data di cessazione dell'incarico al trattamento dei dati da parte del suo collaboratore.
La S.C. Risorse Umane comunica al RPD e, per suo tramite, agli Amministratori di Sistema gli aggiornamenti e le variazioni relative al personale (assunzioni, cessazioni, sostituzioni, incarichi, aspettative, assenze prolungate per almeno 180 gg, trasferimenti, etc.) che comportano una modifica al sistema delle autorizzazioni al trattamento dei dati personali. ASL 5 effettua, a cadenza annuale, unitamente al registro dei trattamenti l'Analisi e la Valutazione Rischi con cui:

- ✓ individua le misure adeguate per elevare lo standard di sicurezza dei dati anche sulla base dell'analisi dei rischi;
- ✓ rappresenta la distribuzione dei compiti e delle responsabilità del trattamento dei dati;
- ✓ programma l'attività di formazione degli incaricati/autorizzati, dei Delegati del trattamento e Amministratori di Sistema al fine di un utilizzo consapevole delle informazioni;
- ✓ evidenzia le misure che l' azienda ha adottato nel tempo per proteggere i dati personali a sua disposizione e il piano delle azioni di miglioramento che intende adottare per l'anno in corso.

Tale documento è predisposto dal RPD di concerto con la S.C. SIA ed in collaborazione con la Direzione Sanitaria, sulla base delle informazioni trasmesse dai Responsabili del trattamento dei dati e dagli amministratori di sistema e di norma inserito nel registro dei trattamenti , poiché strettamente connesso con questi.
I Responsabili interni (Delegati) ed i Responsabili (esterni) del trattamento dati devono inviare al RPD una relazione annuale sul loro operato, che deve evidenziare:

- ✓ l'attività svolta e le misure di sicurezza adottate;
- ✓ le carenze strutturali e organizzative che possono influenzare la corretta applicazione etc.;
- ✓ le specifiche necessità formative per l'attuazione delle disposizioni sulla riservatezza;
- ✓ le criticità di sicurezza riscontrate;
- ✓ le eventuali contromisure di cui si propone l' attivazione.

Art. 29
Misure di sicurezza

ASL 5 ed i Responsabili del trattamento (interni ed esterni) dei dati sono tenuti ad adottare, come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, ogni misura di sicurezza organizzativa e tecnica necessaria per assicurare nell'immediato un sufficiente livello di sicurezza dei dati personali

trattati, attraverso, a titolo esemplificativo e non esaustivo : autenticazione informatica, adozione di procedure di gestione delle credenziali di autenticazione e dei profili di accesso ai dati, utilizzazione di un sistema di autorizzazioni, aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati/addetti alla gestione o alla manutenzione degli strumenti elettronici, protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti nonché l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.
Inoltre l'azienda, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio ad impatto differente, per probabilità e gravità, su diritti e libertà delle persone fisiche, del trattamento dati , propone e mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza idonea al relativo rischio.
Tali misure comprendono, tra le altre, se del caso e compatibilmente con le risorse a disposizione:

- la pseudonimizzazione[56] e/o la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati;
- la capacità di ripristinare tempestivamente disponibilità e accesso ai dati personali in caso di incidente;
- una procedura per testare, verificare e valutare con regolarità l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento in modalità analogica e digitale;
- le misure di minimizzazione nell' utilizzo/inserimento dei dati;
- le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati;
- le altre misure necessarie a garantire i diritti degli interessati;
- gli standard previsti dalle linee guida AGID sulle le misure di sicurezza delle pubbliche amministrazioni [57] ovvero dalle norme europee [58];
- soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominale;
- l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o barriere;
- soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
- cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
- il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dati;
- la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
- la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;
- la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
- la sottoposizione dei soggetti autorizzati al trattamento degli Incaricati/Autorizzati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

[56] «pseudonimizzazione»: il trattamento dei dati personali tale che i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, conservate separatamente e soggette a misure tecniche e organizzative volte a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
[57] linee guida Agid 26 aprile 2016 (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015) CIRCOLARE Agid 18 aprile 2017, n. 2/2017
[58] Regolamento (UE) n. 910 del 23 luglio 2014 (2014/910/UE) "eIDAS" i

Nel valutare l'adeguato livello di sicurezza si tiene conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare da distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Coloro che trattano dati per conto di ASL 5 possono trattare dati personali solo se autorizzati formalmente ed istruiti dall'Azienda stessa.

Art.30
Misure di sicurezza informatica a protezione dei dati

Fermo restando quanto sopra, le misure di sicurezza informatica a protezione dei dati prevedono l'adeguamento alle "misure minime di sicurezza ICT per le pubbliche amministrazioni" quali meglio puntualizzate nelle relative linee guida dettate da AGID, comprensive delle cosiddette misure standard.
In particolare, a cura dei Sistemi Informativi aziendali vengono censiti i dispositivi e i software autorizzati e non; vengono protette le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server; viene effettuata la verifica circa l'uso appropriato dei privilegi di amministratore di sistema; sono in atto misure che impediscono l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda. Sono previsti adeguamenti ulteriori quali: controlli per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive, valutazioni e correzioni continue della vulnerabilità.
Circa le copie di sicurezza queste vengono eseguite a cadenza settimanale, almeno per le informazioni strettamente necessarie per il completo ripristino del sistema, e la riservatezza delle informazioni contenute nelle copie di sicurezza viene garantita mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. Sono previsti adeguamenti ulteriori quali: verifiche periodiche sull'utilizzabilità delle copie mediante ripristini di prova, backup multipli con strumenti diversi per contrastare possibili malfunzionamenti e garantire la continuità operativa. Inoltre verrà effettuata un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica. Verranno inoltre utilizzati sistemi di cifratura per i dispositivi portatili ed i sistemi che contengono informazioni rilevanti. Sul perimetro della rete vengono utilizzati strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale l'accesso a siti di dubbia reputazione.
Sono previsti adeguamenti ulteriori, graduati in relazione alle risorse disponibili, in particolare : verrà monitorato l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni; verranno effettuate periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern" significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro. Verranno inoltre implementati gli strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi, qualsiasi anomalia rispetto al normale traffico di rete verrà registrata anche per consentirne l'analisi off line.

Art. 31
Misure di sicurezza per i trattamenti dati affidati a soggetti esterni

I Responsabili e gli eventuali Sub-Responsabili del trattamento sono tenuti a:

- ✓ assicurare e dimostrare ad ASL 5 di aver adottato, prima di effettuare attività di trattamento di dati, le misure di sicurezza minime ed idonee in tema di protezione di dati e amministrazione digitale.
- ✓ assicurare e dimostrare ad ASL 5 di aver adottato di aver ulteriormente attivato ogni altra misura idonea alla protezione dei dati loro affidati.
- ✓ a rispettare le specifiche istruzioni operative impartite dall'azienda per la tenuta in sicurezza dei dati conferiti
- ✓ ad inviare al RPD una relazione dettagliata nella quale siano evidenziate:
  a) l'attività svolta e le misure di sicurezza adottate;
  b) l'elenco degli Incaricati/Autorizzati del trattamento e l'indicazione della sede presso la quale i relativi atti di nomina sono custoditi;
  c) l'elenco delle risorse hardware e software;
  d) le procedure di continuità operativa ed emergenza adottate;
  e) le misure di eventuale recupero da disastro adottate;

f) le misure adottate di back-up degli specifici sistemi informativi aziendali utilizzati per i trattamenti autorizzati, di contenimento dei virus/malware informatici e altre misure, comprese quelle di eventuale conservazione sostitutiva;
g) le eventuali criticità che potrebbero costituire occasione di accesso non consentito o perdita/manomissione del patrimonio informativo gestito per conto dell'Azienda;
h) le misure adottate per la cifratura, o la separazione dei dati relativi alla salute;
i) le misure adottate per la gestione delle disposizioni in tema di Amministratori di Sistema, rimettendo al riguardo anche la relativa documentazione;
j) le verifiche periodiche sul mantenimento in sicurezza che sono state adottate, con la relativa documentazione.

Nel caso in cui il Responsabile, nell'esecuzione delle attività di trattamento, utilizzi strumenti informatici propri, è tenuto ad attestare con propria dichiarazione scritta di garantire la protezione dei dati affidati dal Titolare attraverso specifiche misure di sicurezza e di non aver affidato alcune fasi del trattamento a soggetti terzi, salvo che l'Azienda non ne abbia autorizzato in via preventiva la nomina a Sub-Responsabile del trattamento dei dati personali.
Qualora il Responsabile del trattamento utilizzi, al contrario, strumenti informatici forniti da ASL 5 è tenuto a fornire l'elenco degli atti di designazione degli incaricati/autorizzati al RPD aziendale e ad attivare le procedure necessarie al rilascio delle relative credenziali di accesso.
Il mancato rispetto da parte del Responsabile esterno del trattamento di misure di sicurezza adeguate a contenere o prevenire rischi che possono riguardare i dati affidati può costituire titolo di risoluzione del sotteso rapporto sostanziale per grave inadempimento e per il risarcimento dell' eventuale danno .

Art. 32
Sicurezza di documenti ed archivi [59]

Gli archivi che custodiscono i dati di cui è titolare l azienda, cartacei e digitali, devono essere collocati in locali non esposti a rischi ambientali in ossequio alle disposizioni generali in materia di sicurezza ed a quelle specifiche per la protezione del patrimonio informativo aziendale in tema di continuità operativa, conservazione sostitutiva e Disaster Recovery.
La documentazione archiviata, anche digitalmente, che riporta dati personali è conservata soltanto per il tempo previsto dalla legge e poi sottoposta a scarto di archivio o cancellata definitivamente.
Il Responsabile del Trattamento interno ovvero esterno, attiva, attenendosi alle indicazioni del Data Protection Officer ed alle disposizioni e Procedure Aziendali vigenti, i meccanismi necessari a garantire l'accesso selezionato ai dati e l'accesso controllato ai locali dove questi sono collocati mediante registrazione degli accessi ed esclusione degli stessi fuori dell'orario di servizio dell'Archivio medesimo.
I supporti contenenti dati personali diversi dal cartaceo (supporti informatici, magnetici, videoregistrazioni effettuate nell'ambito dell'attività clinica, bobine di microfilm, immagini iconografiche), debbono essere conservati e custoditi con le modalità indicate per gli archivi cartacei nei modi e termini previsti dalla normativa vigente.
Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Responsabile interno/ eterno di competenza, che deve assicurarne la riservatezza, la protezione e l'integrità per tutto il tempo in cui ne mantiene la disponibilità.
L'accesso agli archivi cartacei aziendali é formalmente autorizzato, da parte dei Responsabili del trattamento;
relativamente agli archivi digitali il rilascio di tale autorizzazione e di competenza dell'Amministratore di Sistema, previa indicazione del Responsabile del Trattamento e comunicazione al RPD.
Per quanto riguarda la documentazione cartacea facente parte dell'archivio aziendale corrente e/o di deposito, in conformità a quanto disposto dal Ministero per i beni Culturali ed Ambientali con l'apposito Massimario di scarto per gli archivi degli Enti Sanitari, ASL 5, tramite proprio personale, predispone periodicamente un piano di scarto d'archivio, approvato con apposita deliberazione ovvero può delegare a tale funzione soggetti esterni.
L'Azienda, relativamente agli archivi informatizzati di dati, adotta, in conformità alle disposizioni vigenti in tema di protezione dati e amministrazione digitale ed, avvalendosi del SIA in stretta collaborazione con il RPD Aziendale ,i Responsabili del trattamento dei dati e degli Amministratori di Sistema, idonee procedure di:

[59] per archivio si intende qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico

- ✓ salvataggio periodico degli archivi di dati personali;
- ✓ misure di contenimento dei virus/malware informatici e di protezione perimetrale da cyber-attacchi alle infrastrutture aziendali;
- ✓ Disaster Recovery e continuità operativa;
- ✓ conservazione sostitutiva.

Art. 33
Violazione di dati

Ogni Responsabile / Incaricato o Autorizzato del trattamento dei dati personali o Amministratore di Sistema è tenuto ad informare, senza ingiustificato ritardo, il Titolare ed il RPD circa i casi di possibile violazione dei dati personali (*Data Breach*), utilizzando l' indirizzo mail, pubblicato sulla Intranet aziendale .

L'Azienda, in tale ipotesi avvia le necessarie procedure e, avvalendosi della collaborazione dei Responsabili del trattamento, accerta l'effettivo stato dell'arte. Provvede quindi, sussistendone i requisiti, a notificare attraverso il RPD la violazione all'Autorità Garante Privacy senza ingiustificato ritardo e, ove possibile, entro 48 ore dal momento della conoscenza, fatta salva l'ipotesi che la violazione dei dati personali non presenti un rischio per i diritti e le libertà degli Interessati.
Se la notifica non è effettuata entro 48 ore, occorre porre a corredo i motivi del ritardo.
Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati viene loro inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente.
La notifica della violazione dei dati personali deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome ed i dati di contatto del RPD o altro punto di contatto presso cui ottenere maggiori informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali ed anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni nell' immediato queste possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Il Titolare del trattamento documenta qualsiasi violazione dei dati personali in un apposito Registro delle violazioni di dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio; tale documentazione consente all'autorità di controllo di verificare il rispetto delle indicazioni di legge.

Art. 34
Limiti alla conservazione dei dati

ASL 5 assicura l'adozione di apposite misure e procedure attraverso le quali:

- ✓ distruggere i dati personali, una volta terminato il limite di conservazione ovvero inerente o derivante da specifiche finalità/modalità di trattamento dei documenti analogici e digitali e dei dati personali in questi riportati;
- ✓ smaltire gli apparati hardware o i supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare l' azienda;
- ✓ riutilizzare apparati di memoria o hardware con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui e titolare ASL 5.

Quando sopra, fermo restando il rispetto dei termini derivanti dagli obblighi di conservazione legale e quanto previsto in tema di conservazione digitale[60] o a fini organizzativo- strumentale come nel caso del Dossier Sanitario Elettronico, i cui contenuti, di norma, seguono l'intera vita dell'assistito. Per quel che riguarda i termini temporali di conservazione dei dati, fermi i vincoli previsti per legge, l'azienda intende seguire il principio di indispensabilità e necessità dei dati in relazione al fine perseguito attraverso il loro utilizzo.

Art. 35
Controllo a distanza

Ad ogni sistema di controllo a distanza, che coinvolga interessati e/o lavoratori, ASL 5 applica il principio di proporzionalità tra mezzi impiegati e fini perseguiti, nel rispetto delle disposizioni vigenti e delle ulteriori direttive europee ovvero dell'Autorità Garante per la protezione dei dati personali.
L'azienda comunque garantisce il rispetto della disciplina del divieto di controllo a distanza del lavoratore, cosi come prevista dalla normativa di riferimento compreso il rispetto degli accordi con le rappresentanze sindacali aziendali.
Per i sistemi di controllo attivati, viene assicurata l'effettività delle misure di tutela degli interessati e dei lavoratori, con particolare riguardo all'erogazione di informativa specifica ed alla piena trasparenza di caratteristiche, finalità e modalità del controllo eseguito.

Art. 36
Attività di verifica e controllo

ASL 5 individua apposite modalità per svolgere verifiche e controlli, anche periodici e che, durante le operazioni di trattamento dati, da parte dei soggetti autorizzati , siano rispettate le misure di legge e le ulteriori disposizioni aziendali impartite. Controlli e verifiche sono effettuati e programmati periodicamente o, in caso di necessità, su sollecitazione degli interessati ovvero anche tramite audit da parte del RPD come da previsioni normative.

Art. 37
Videosorveglianza, riprese in sala operatoria, utilizzo telefonia e postazioni informatiche e posta aziendale

Per quel che attiene alla disciplina degli argomenti in parola si richiama e si rinvia in modo espresso al relativo Regolamento approvato dall'Azienda con deliberazione n. 111/2020 ed alle relative informazioni tutte pubblicate sul sito aziendale al link privacy.

Art. 38
Redazione degli atti

Ancorché, per prassi, alcuni atti vegano assunti con deliberazioni/determinazioni, soggetti a pubblicazione al fine di evitare problematiche ad essi riferite è opportuno utilizzare la forma della deliberazione/determinazione soltanto quando l'atto sia espressione della volontà dell'ente. Tale carattere è di norma connesso alla discrezionalità, carente laddove si tratti di accertamento di natura tecnica ossia si concretizzi nella stretta verifica della sussistenza del possesso, in capo il soggetto, dei requisiti previsti dalla legge[61].
Per quel che attiene alle modalità di redazione dell'oggetto qualora il nome e cognome del dipendente/paziente/utente/terzo siano correlabili ad una patologia che si evinca dall'oggetto stesso si consiglia, per la pubblicazione dell'atto all'albo on line, l'utilizzo delle sole iniziali.
Ai fini della redazione degli atti, fermo restando l'obbligo di citare sempre dati aggiornati, è necessario applicare i principi di pertinenza, non eccedenza e necessarietà dei dati inseriti nella deliberazione/determinazione. In altre parole i dati sono da selezionare in base ad una connessione logica stringente tra narrato e dispositivo valutando quando i dati comuni siano necessari o meno e quando la loro indicazione nell'atto sia prevista per legge.
A tal fine, si tenga presente che "i soggetti pubblici sono tenuti a ridurre al minimo l'utilizzazione di dati personali e

[60] Si citano, a titolo esemplificativo e non esaustivo, le linee guida AGID sulla conservazione dei documenti informatici del 2015 il Codice di Amministrazione Digitale, principi di cui al Regolamento Eidas 910/2014,le regole tecniche di conservazione di cui al DPCM del 3 dicembre del 2013 e del DPCM del 13 Novembre 2014 e modificazioni ed integra-zioni nonché il del D.lgs. 217/2017.

[61] A titolo esemplificativo e non esaustivo si cita l'esempio della L. 104/92. In tali ipotesi infatti non sussiste né il carattere di concessione di un beneficio/ vantaggio, né il carattere della discrezionalità . Il datore di lavoro infatti, acquisita la documentazione di rito, è normativamente vincolato a prendere atto di tale stato di fatto e di diritto , senza alcuna possibilità di scelta discrezionale.

di dati identificativi". Qualora il provvedimento trovi fondamento/motivazione in atti/fatti di natura sensibile (dati di salute, certificati medici, valutazioni inerenti le persone dei dipendenti, stato di indigenza, etc.) o a maggior tutela (HIV/dipendenze tutte/psichiatrici/trattamenti consultoriali, vittime di violenza , IVG, esiti disciplinari etc.), è richiamata la possibilità di motivare ob relationem ossia citando il relativo allegato contenente i dati fondanti il provvedimento, salvo che l' intero provvedimento non sia da secretarsi per legge/Regolamento.

Art. 39
Pubblicazione degli atti

Le norme in materia di privacy comportano il rispetto della dignità della persona, considerata nel suo insieme, pertanto anche la pubblicazione degli atti deve essere pensata ed attuata in modo da non violare il diritto all' integrità anche morale della persona. Non risultando possibile, a priori fornire un elenco dei provvedimenti soggetti a tutela, tale soggezione va valutata caso per caso in relazione ai contenuti ed alle connesse modalità espositive. Occorre tuttavia garantire l'oscuramento totale previsto per legge circa le delibere che abbiano ad oggetto provvedimenti disciplinari/ ed altre circostanze della vita lavorativa di particolare rilievo ancorché inerenti fatti riportati dalla stampa poiché l' azienda , come datore di lavoro è tenuta a gestire tali situazioni con totale riserbo a sensi della privatizzazione del rapporto di lavoro ex artt. 2 e 5 del d.lgs. 165/2001 e ss.mm.ii., nonché delle specifiche linee guida sulla gestione del rapporto di lavoro nel pubblico impiego dettate dal garante e del provvedimento n. 392 del 31.7.2014. La legge 33/2013 e ss.mm.ii. impone alle P.P.A.A. di pubblicare nell'apposita sezione trasparenza una serie di dati di cui sussiste un' elencazione puntuale . Ciò nondimeno occorre distinguere tra gli atti da pubblicare sull' albo on line e ciò che è soggetto a pubblicazione obbligatoria per trasparenza infatti è convinzione comune che ciò che sia pubblicato sull'albo vada trasfuso di default nella sezione trasparenza [62].
Al proposito sussistono precise linee guida offerte dal garante al link:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436, a cui si rinvia per brevità.

Art. 40
Regole di comportamento da adottare a tutela della privacy

a) Modalità di conservazione della documentazione cartacea.
Tutta la documentazione cartacea contenente dati personali e/o sensibili (soprattutto nel caso dei dati sensibili) con specifico riferimento a quelli appartenenti alle particolari categorie di dati di cui all'art. 9 del RGPD deve essere conservata dai responsabili Delegati e dai soggetti autorizzati al trattamento e dagli incaricati/autorizzati, alla fine del trattamento, in contenitori muniti di serratura. Se vi è la possibilità all'interno dei locali/uffici di utilizzare: schedari, armadi, cassetti e quant'altro chiudibile con serratura, si provvederà all'utilizzo dei medesimi. In caso contrario si considererà il locale come contenitore, pertanto quando sono terminate le operazioni di trattamento, e non vi è nessuno tra il personale autorizzato che possa vigilare sulla documentazione, il locale dovrà essere chiuso a chiave. In aggiunta a tale misura di sicurezza, è inoltre consigliabile collocare un cartello sulla porta che vieti l'ingresso ai soggetti non autorizzati al trattamento dei dati.
b) Modalità di trasporto interno della documentazione cartacea.
Quando le cartelle cliniche (ed altra documentazione sanitaria i dati sensibili) devono essere trasportate all'interno degli ospedali, è opportuno quando possibile necessario utilizzare delle buste al fine di impedire un accesso non autorizzato a tale documentazione; inoltre chi trasporta tale documentazione deve effettivamente custodirla con attenzione.
c) Modalità di conservazione della documentazione cartacea negli archivi.
Per i locali adibiti ad archivio, contenenti dati personali, è necessario che tali locali siano chiusi a chiave e che le chiavi siano in possesso del personale autorizzato (accesso selezionato); mentre per i locali adibiti ad archivio contenenti particolari categorie di dati ex art. 9 RGPD, in aggiunta alla misura di sicurezza sopra esposta, è necessario predisporre un foglio - registro cartaceo, ove vengono indicati i soggetti autorizzati che vi accedono dopo l'orario di chiusura dell'archivio, riportando "nominativo, data, ora di ingresso e uscita, il dato consultato e/o prelevato, firma" (accesso selezionato e controllato).
d) Modalità di distruzione di supporti cartacei riportanti dati personali.

[62] A titolo esemplificativo si richiama ad es. una deliberazione di cessazione dal servizio: questo atto è soggetto a pubblicazione sull'albo on line, ma non a trasparenza, potrebbe inoltre essere soggetto a privacy in relazione alla motivazione della cessazione.

Qualora sia necessaria l'eliminazione di supporti cartacei contenenti dati personali, ed in partico-lare dati sensibili quelli appartenenti alle particolari categorie di dati di cui all'art. 9 del RGPD è necessario distruggere i supporti in modo tale da non consentire la consultazione del documento. In particolare prima del conferimento nell'apposito contenitore dei rifiuti è necessario ridurre i fogli stracciandoli più volte o, ancora meglio, utilizzare, se disponibile, il macchinario trita documenti.

e) Modalità di esposizione delle tabelle presenza nei reparti di degenza.

Le tabelle presenza dei degenti, eventualmente esposte nei corridoi od in altri punti visibili a terzi, nelle strutture di degenza, devono essere collocate in locali od aree più riparate dove solo il personale autorizzato può consultarle (ad esempio nel box infermieristico).

f) Richiesta di informazioni sulla presenza di un paziente.

Nel caso venga chiesto se una persona è ricoverata o meno presso l'Ospedale, è possibile dare tale informazione se l'interessato (paziente) non abbia richiesto che la sua presenza sia mantenuta anonima.

g) Richiesta di informazioni sullo stato di salute di un paziente.

Nel caso invece si presentino, parenti, amici, conoscenti che chiedono informazioni inerenti lo stato di salute dell'interessato-paziente (patologia, diagnosi, terapia etc.), non è possibile fornire tali informazioni senza aver prima raccolto il consenso dell'interessato. Pertanto al momento del ricovero, dovrà essere fornita all'interessato l'informativa, tramite un modulo predisposto dalla Direzione (che può sia essere consegnato in copia all'interessato che affisso in un luogo del reparto, ben visibile dallo stesso).

Gli operatori possono rendere note all'interessato informazioni sul suo stato di salute solo tramite un medico designato dal Titolare o delegato del trattamento o dall'interessato. Questa regola non vale nei casi in cui le predette informazioni erano state originariamente fornite dallo stesso interessato. Il Titolare o il Responsabile Delegato al trattamento possono incaricare altri operatori sanitari a rendere note le predette informazioni all'interessato, specificando per iscritto appropriate modalità e cautele.

h) Richiesta di informazioni delle forze dell'ordine.

Fermo restando il rapporto di collaborazione tra pubbliche amministrazioni , le richieste di informazioni anche sensibili inoltrate da un rappresentante delle forze dell'ordine, nell'esercizio delle proprie funzioni istituzionali, sono evase esclusivamente dalle direzione mediche di presidio e nei soli casi in cui il rappresentante si qualifichi ed esibisca un mandato dell'autorità giudiziaria.

i) Distanze di cortesia.

Tutti i punti accettazione devono essere muniti di strumenti idonei a garantire la distanza di cortesia per gli utenti; tali strumenti possono essere ad esempio: una riga di segnalazione a terra ed un cartello che indichi il rispetto della distanza di cortesia; o qualunque altro sistema garantisca il medesimo risultato.

l) Utilizzo del telefono.

In via generale è preferibile non fornire indicazioni inerenti lo stato di salute degli interessati via telefono, se non si è certi dell'identità dell'interlocutore e del fatto che egli sia autorizzato ad acquisire tali informazioni. Un suggerimento potrebbe essere quello di farsi lasciare dal chiamante, nominativo e numero di telefono per poter provvedere a ricontattarlo, previa verifica dei dati forniti e dell'autorizzazione dello stesso soggetto ad acquisire tali informazioni.

m) Utilizzo del fax per comunicazioni interne.

Nel caso si debba procedere alla comunicazione di dati sensibili all'interno delle aree di pertinenza dell'A.S.L. tramite fax, è necessario che ogni Struttura /Servizio abbia predisposto uno specifico numero di fax adibito anche a questa funzione, che tale fax sia collocato in un'area protetta e presidiata, e che i responsabili delegati e i soggetti incaricati/autorizzati al trattamento prestino attenzione alle fasi di invio e di ricevimento della documentazione contenente dati personali sensibili appartenenti alle categorie particolari di dati ex art. 9 del RGPD.

n) Utilizzo del fax per comunicazioni esterne.

Nel caso si debba procedere alla comunicazione di dati sensibili sempre tramite fax con un soggetto esterno, autorizzato per legge all'acquisizione di tale documentazione, si dovrà comunque adottare un accorgimento. Ossia, la prima volta che si stabilisce un rapporto con tale soggetto, che prevede la comunicazione di dati sensibili tramite fax, si deve chiedere allo stesso, prima dell'invio della documentazione, di indicare qual è il numero di fax al quale d'ora in poi possiamo inviare tale documentazione, la risposta dovrà essere fornita via fax. Pertanto l'A.S.L. deve avere un documento cartaceo inviatogli dal soggetto, ove quest'ultimo indica il numero di fax presso il quale inviargli la documentazione contenente dati sensibili. È fatto salvo quanto previsto dall'art. 47 del Codice

dell'amministrazione digitale e s.m.i. in materia di trasmissione di documenti tra Pubbliche Amministrazioni. In particolare è esclusa la trasmissione degli stessi a mezzo fax.

o) Utilizzo della stampante.

La stampa di documentazione contenente dati personali e sensibili deve avvenire ad opera di personale autorizzato il quale deve provvedere altresì al ritiro tempestivo della documentazione dalle stampanti ed alla conservazione della stessa; non deve essere utilizzata carta riciclata che contiene già informazioni personali e sensibili sull'altro lato del foglio; nel caso le stampe contenenti dati appartenenti alle particolari categorie di cui all'art. 9 del RGPD sensibili debbano essere cestinate, si consiglia di strappare la documentazione in modo da non renderla facilmente accessibile a terzi non autorizzati. È cura dell'utilizzatore effettuare la stampa dei dati solo se strettamente necessaria, così come è buona regola evitare di stampare documenti o file non adatti (ad esempio documenti di lunghezza notevole).

p) Utilizzo della fotocopiatrice.

La fotocopiatura di documentazione cartacea contenente dati personali e sensibili deve avvenire ad opera di personale autorizzato, che deve altresì provvedere al ritiro tempestivo degli originali e delle copie dalla fotocopiatrice. Non deve essere utilizzata carta riciclata che contiene già informazioni personali e sensibili sull'altro lato del foglio.

q) Contatto con il pubblico.

Il dialogo-colloquio tra personale / operatori aziendali autorizzati (medici, infermieri etc.) e gli utenti, qualora abbia ad oggetto informazioni inerenti lo stato di salute dell'interessato, e qualora avvenga in spazi od in situazioni ove sono presenti altri soggetti oltre all' interessato, come ad esempio nelle stanze di degenza a più posti letto o nei punti ove vengono ritirati, esami, referti etc. o presso le accettazioni e le segreterie delle S.C., deve essere improntato ad un criterio di prudenza. A tale prudenza devono essere adeguate le condizioni usuali di colloquio tra operatori nell'esercizio della professione: discussione di casi clinici durante il giro-visita, supervisione di casi in luoghi aperti all'utenza, consulenze specialistiche effettuate al letto di degenza, passaggi di consegne tra personale, comunicazioni di servizio effettuate mediante apparecchi telefonici portatili o meno non posizionati in luoghi protetti, informazioni fornite a studenti o frequentatori.

r) Utilizzo di e-mail per riscontrare l' utenza ovvero evadere inoltro di documenti.

Fermo restando che per tali comunicazioni deve privilegiarsi la posta certificata, tuttavia è utilizzabile anche la email ordinaria se l'utente richiede tale modalità di inoltro ed indica il relativo recapito autorizzando e manlevando espressamente il personale aziendale.

Art. 41
Comportamenti individuali e sanzionabilità

Fermo restando che ai sensi dell'art. 12 del D.P.R. n. 62/2013 c. 5 "i dipendenti sono tenuti ad osservare il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali", per ogni ipotesi di comportamento individuale che possa integrare una sanzionabilità disciplinare si richiama e si rinvia al Regolamento Aziendale a disciplina delle regole di comportamento e dei principi etici costituenti obbligo contrattuale.

Art. 42
Norme transitorie e finali

Per quanto non espressamente previsto dal presente Regolamento si rinvia alla normativa vigente con particolare riferimento in materia di protezione dei dati personali ed amministrazione digitale. Le autorizzazioni a trattare i dati già conferite restano valide sino alla loro revisione, programmata con il RPD, per i necessari adeguamenti normativi.

L'Azienda si riserva, inoltre, di adeguare, modificare o integrare il testo del presente Regolamento qualora per motivi organizzativi e/o nel caso in cui la normativa e le direttive sopra citate lo rendano opportuno, dotandosi anche progressivamente di strumenti operativi quali ad es.: Linee guida, procedure, istruzioni, circolari, modulistica, etc. finalizzati alla piena effettività delle misure previste dal presente Regolamento.