

 ASL TERAMO <small>www.aslteramo.it</small>	<i>Regione Abruzzo</i> Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)	Documento: Istruzione Dipendenti Revisione n.: 3.1 Data Emissione: 02.03.2022
	GDPR	pag. 1 di 9

Regione Abruzzo



**Istruzioni operative ai
DIPENDENTI e COLLABORATORI
in materia di protezione dati personali**

della ASL Teramo

in base a quanto previsto dal

**Artt. 29 e 32 del Regolamento UE 2016/679 e
2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018**

Redazione	Verifica	Parere favorevole	Approvazione
R.T.I.	UOSD Segreteria di Direzione	D.P.O.	Titoliare

 <p>ASL TERAMO www.aslteramo.it</p>	<p>Regione Abruzzo</p> <p>Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)</p>	<p>Documento: Istruzione Dipendenti</p> <p>Revisione n.: 3.1</p> <p>Data Emissione: 02.03.2022</p> <p style="text-align: right;">pag. 2 di 9</p>
GDPR		

Sommario

1. Introduzione.....	3
2. Trattamento di dati personali.....	3
3. Obblighi formali.....	3
4. Utilizzo e trasmissione dei dati.....	4
5. Strumenti informatici e telematici.....	4
6. Condivisione delle informazioni.....	4
7. Prontuario per lo scarto dei documenti.....	5
8. Regole per trattamenti senza strumenti informatici.....	5
9. Regole per trattamenti con strumenti informatici.....	6
10. Regole per le comunicazioni tramite posta elettronica c.d. email.....	6
11. FAQ del Garante con le risposte alle domande più frequenti in materia di protezione dei dati personali in ambito sanitario.....	6

 ASL TERAMO <small>www.aslteramo.it</small>	<i>Regione Abruzzo</i> Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)	Documento: Istruzione Dipendenti Revisione n.: 3.1 Data Emissione: 02.03.2022
	GDPR	pag. 3 di 9

1. Introduzione

In ottemperanza alle disposizioni del Regolamento Europeo per la protezione dei dati personali (GDPR 2016/679) e al Decreto Legislativo 196/2003 e successive modificazioni ed integrazioni (da ultimo D. Lgs. 101/2018), tutto il personale di questa ASL è nominato come "soggetto autorizzato al trattamento dei dati personali" e, nello svolgimento delle operazioni di trattamento dei dati, ha l'obbligo di attenersi con scrupolo e diligenza alle istruzioni e ad ogni ulteriore indicazione che potrà essere fornita dal Titolare del trattamento (Direttore Generale).

Presso la nostra azienda, i soggetti autorizzati al trattamento dei dati di I livello sono tutti i Direttori di Dipartimento/Coordinamento, di Unità Operativa Complessa (UOC), i Responsabili di Unità Operativa Semplice Dipartimentale (UOSD) nonché, per quanto riguarda le sole strutture "in staff" alla Direzione Aziendale, i Responsabili delle medesime strutture "di staff" (uffici o unità) ed i soggetti autorizzati al trattamento dei dati di II livello sono tutti i dipendenti e/o collaboratori delle ASL.

2. Trattamento di dati personali

L'art. 4 del GDPR 2016/679 definisce il trattamento di dati personali come "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Il trattamento dev'essere:

- effettuato secondo modalità tali da garantire la riservatezza, l'integrità e la disponibilità dei dati;
- effettuato in modo lecito, corretto e trasparente nei confronti dell'interessato;
- effettuato per scopi determinati, espliciti e legittimi;
- rispettoso dei principi di necessità, pertinenza e non eccedenza rispetto alle finalità per le quali il dato è raccolto;
- idoneo a garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale;
- effettuato per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono raccolti o successivamente trattati.

3. Obblighi formali

Ogni persona autorizzata al trattamento dati è tenuta a:

- adottare tutti gli accorgimenti possibili al fine di garantire sempre la dignità del paziente;

 www.aslteramo.it	Regione Abruzzo Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)	Documento: Istruzione Dipendenti Revisione n.: 3.1 Data Emissione: 02.03.2022
GDPR	pag. 4 di 9	

- rispettare i regolamenti interni e/o le disposizioni della direzione su chi possa fornire informazioni (sanitarie e non) verso l'esterno ed i casi in cui tale prassi è possibile;
- mantenere l'assoluto riserbo sulle informazioni trattate all'interno della struttura;
- attuare le misure necessarie per un corretto, lecito, sicuro trattamento, attenendosi alle istruzioni operative ed alle prescrizioni definite nell'atto di designazione di soggetto autorizzato al trattamento dei dati, di I o II livello, e nella regolamentazione aziendale;
- utilizzare le banche dati informatiche esclusivamente attraverso le proprie credenziali di autenticazione da tenere riservate;
- ottemperare agli obblighi di informazione ed eventuale acquisizione del consenso, quando necessario e quando non altrimenti eseguito dalla propria struttura nei confronti degli interessati;
- controllare e custodire, durante il compimento dell'intero trattamento e fino alla consegna, gli atti e i documenti contenenti dati, personali sensibili o giudiziari, in modo da impedirne l'accesso a persone non autorizzate;
- informare il proprio responsabile in merito ad eventuali richieste dell'interessato volte a far valere i propri diritti in materia di privacy o di accesso.

4. Utilizzo e trasmissione dei dati

I dati oggetto di trattamento non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative. Nessun dato personale può essere utilizzato o trasmesso all'esterno dell'Azienda, senza previa autorizzazione del Delegato alla gestione delle attività di trattamento dei dati o del Titolare.

5. Strumenti informatici e telematici

Al fine di garantire un corretto trattamento dei dati personali nel rispetto delle vigenti norme di legge nonché delle misure di sicurezza che l'Azienda ha ritenuto idoneo adottare, è opportuno impiegare gli strumenti informatici e telematici (internet, posta elettronica, strumenti di ultima generazione come computer portatili, tablets, telefoni cellulari, smartphone, etc....) con diligenza ed attenzione, attenendosi alle disposizioni contenute nel "Regolamento aziendale per l'utilizzo dei mezzi informatici e telematici", tempo per tempo vigente, consultabile nel sito internet aziendale all'interno della pagina web denominata "Area Protezione Dati Personali" raggiungibile all'indirizzo aslteramo.it/datipersonali.

Inoltre, a titolo esemplificativo e non esaustivo, si segnala che **non possono** essere utilizzati strumenti informatici personali (ad esempio i propri computer o dispositivi di memorizzazione non aziendali, quali memorie USB, dischi esterni, etc), e **non è consentito**: l'uso di applicazioni software non licenziate e non di proprietà dell'Azienda, l'uso di caselle di posta elettronica non aziendali (ad esempio: Gmail, Yahoo, Virgilio, Libero, etc), ed infine l'uso di piattaforme di social network (ad esempio: Facebook, Whatsapp, Instagram, Twitter, Telegram, etc.).

6. Condivisione delle informazioni

Laddove sia necessario condividere le informazioni contenute all'interno dei file, l'UOC Sistemi Informativi, mette a disposizione il servizio di cartella condivisa attivabile a partire dalla modulistica presente nel sito web aziendale <https://www.aslteramo.it/intranet/modulistica-personale/> (Personale ASL -> Modulistica ->

 ASL TERAMO <small>www.aslteramo.it</small>	<i>Regione Abruzzo</i> Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)	Documento: Istruzione Dipendenti Revisione n.: 3.1 Data Emissione: 02.03.2022
	GDPR	pag. 5 di 9

Sistemi Informativi). Si comunica altresì che per la condivisione di file **non è consentito** l'uso di sistemi di alternativi come ad esempio Dropbox, Google Drive, WeTransfer, ecc.ecc..

7. Prontuario per lo scarto dei documenti

Al fine di garantire un corretto trattamento dei dati personali anche nel rispetto del principio generale (citato in premessa) secondo il quale il trattamento dei dati deve essere effettuato "per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono raccolti o successivamente trattati", è altresì opportuno consultare, al bisogno, il "Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere" approvato con Deliberazione n° 128 del 3 marzo 2015 e pubblicato sul sito della ASL Teramo nella pagina dedicata <https://www.aslteramo.it/datipersonali/>

Per "Prontuario" aziendale di conservazione e scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permette di gestire in modo organizzato l'archivio aziendale, conservando solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria.

8. Regole per trattamenti senza strumenti informatici

Al fine di garantire un corretto trattamento dei dati personali anche nel caso non si usino strumenti elettronici o informatici, si riportano di seguito alcune corrette prassi da seguire:

- I dati presenti su documenti cartacei devono essere protetti mediante conservazione e gestione degli stessi in modo da evitarne la visibilità, la sottrazione, la riproduzione, l'alterazione o la distruzione abusiva.
- I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassette chiuse a chiave, uffici chiusi a chiave), evitando una indebita consultazione da parte di estranei o personale non autorizzato.
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti quando non più necessari o entro la fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie, stampanti, fotocopiatrici, fax o tavoli di lavoro.
- I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative
- Qualora un documento contenente dati personali e particolari non sia più necessario, esso deve essere distrutto utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili;
- I documenti che contengono dati particolari, sulla salute e/o giudiziari devono essere controllati e custoditi dagli autorizzati, i quali devono impedire l'accesso a persone prive di autorizzazione;
- L'archiviazione dei documenti cartacei contenenti dati particolari, sulla salute e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassette chiuse a chiave.

 <p>ASL TERAMO www.aslteramo.it</p>	<p>Regione Abruzzo</p> <p>Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)</p>	<p>Documento: Istruzione Dipendenti Revisione n.: 3.1 Data Emissione: 02.03.2022</p>
GDPR	pag. 6 di 9	

9. Regole per trattamenti con strumenti informatici

Al fine di garantire un corretto trattamento dei dati personali quando vengono utilizzati strumenti elettronici o informatici, si riportano di seguito alcune corrette prassi da seguire:

- Attuare una corretta gestione delle credenziali di autenticazione (Password) con cambiamento programmato delle medesime e relativa segretezza.
- Lavorare sul server aziendale ed effettuare il salvataggio dei dati in rete e non in locale (Desktop) attivando il servizio di cartella condivisa precedentemente illustrato.
- Non lasciare il personal computer incustodito e premere la combinazione di tasti "Windows + L"  +  ogni volta che ci si allontana dalla postazione dei lavoro in maniera tale da bloccare la sessione. Avere la massima cautela nell'utilizzo della stampante (non lasciare le stampe incustodite e prenderle al termine della stampa).
- Non creare banche dati autonome senza preventiva autorizzazione.

10. Regole per le comunicazioni tramite posta elettronica c.d. email

La Posta Elettronica Ordinaria, ovvero la classica email (anche chiamata con l'acronimo PEO) e la Posta Elettronica Certificata, meglio conosciuta con il relativo acronimo PEC, non possono essere considerati strumenti idonei a scambiare in modo sicuro dati personali in quanto per loro natura, non possono garantire la riservatezza delle informazioni contenute nel corpo dell'email e negli allegati. Per ovviare a tale inconveniente e consentire l'uso di tali strumenti è possibile proteggere con password gli allegati così che il ricevente possa accedere in modo riservato alle informazioni personali, particolari e sulla salute. **L'ASL di Teramo, grazie al supporto dell'UOC Sistemi Informativi, ha predisposto un servizio dedicato alla protezione delle email e dei relativi allegati, anche di grandi dimensioni, tramite password. In allegato sono disponibili semplici indicazioni su come utilizzare il servizio appena citato.**

Prima di procedere all'invio di una email, verificare l'effettiva correttezza degli indirizzi inseriti. Nel caso di destinatari multipli, soprattutto nel caso in cui si trasmettono dati sensibili, utilizzare in maniera appropriata i campi CC (copia conoscenza) e CCN (copia conoscenza nascosta). Nello specifico il campo CCN assicura che i destinatari della stessa email non possano venire a conoscenza dell'identità degli altri destinatari.

11. FAQ del Garante con le risposte alle domande più frequenti in materia di protezione dei dati personali in ambito sanitario.

La tutela della dignità della persona deve essere sempre garantita in modo particolare riguardo a fasce deboli (come ad es. disabili, minori, anziani). Particolare attenzione dovrà essere posta a coloro che sono sottoposti a trattamenti medici invasivi o per i quali è doverosa una particolare attenzione (per es. persone affette da HIV, che hanno subito abusi sessuali, interrotto gravidanze).

Questa guida raccoglie le risposte alle domande più frequenti che vengono poste all'attenzione dell'Autorità da pazienti e personale sanitario offrendo anche un quadro delle principali indicazioni fornite dal Garante nel

 www.aslteramo.it	Regione Abruzzo Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)	Documento: Istruzione Dipendenti Revisione n.: 3.1 Data Emissione: 02.03.2022
	GDPR	pag. 7 di 9

corso del tempo. L'intento è quello di agevolare le attività degli operatori del settore e di contribuire a migliorare le condizioni di vita quotidiana di chi accede alle cure.

SALE DI ATTESA

- IN ATTESA A CHE SERVE LA "DISTANZA DI CORTESIA"?

Per garantire la riservatezza dei colloqui. Presso gli sportelli pubblici di ospedali e dei distretti fare in modo che gli utenti e pazienti rispettino il proprio turno negli appositi spazi, spesso segnalati con una riga gialla.

- NELLE SALE D'ASPETTO IN CHE MODO IL PAZIENTE DEVE ESSERE AVVISATO DEL PROPRIO TURNO?

Nei locali di grandi strutture sanitarie i nomi dei pazienti in attesa di una prestazione o di documentazione (ad esempio delle analisi cliniche) non devono essere divulgati ad alta voce.

Occorre adottare soluzioni alternative: per esempio, attribuendo un codice alfanumerico al momento della prenotazione o dell'accettazione.

- ALL'INGRESSO DEI REPARTI POSSONO ESSERE AFFISSE LE LISTE DEI PAZIENTI IN ATTESA DI UN INTERVENTO?

No. Non è giustificata l'affissione di liste di pazienti in attesa di intervento in locali aperti al pubblico, con o senza la descrizione della patologia sofferta.

Non devono essere resi visibili ad estranei neanche documenti sulle condizioni cliniche del malato, come le cartelle infermieristiche poste vicino al letto di degenza.

INFORMAZIONI SULLA SALUTE

- QUALI PRECAUZIONI DEVE ADOTTARE IL PERSONALE SANITARIO PER TUTELARE LA PRIVACY DEI PAZIENTI?

Tutto il personale deve garantire la massima riservatezza durante lo svolgimento delle prestazioni mediche sanitarie ed assistenziali e più in generale su tutti i dati personali trattati all'interno della struttura, al di là di quanto già previsto dal segreto professionale. E' assolutamente vietato sfruttare tali dati personali per fini privati.

Il personale sanitario deve evitare che le informazioni sulla salute possano essere conosciute da soggetti non autorizzati, a causa di situazioni di promiscuità derivanti dall'organizzazione dello spazio dei locali o dalle modalità utilizzate. Il Garante ha prescritto a questo scopo specifici accorgimenti per garantire la riservatezza dei pazienti sia durante l'orario di visita, sia all'atto della prescrizione di ricette mediche o del rilascio di certificati. Tra questi accorgimenti va ricordato, ad esempio, l'uso di paraventi o simili nei reparti di rianimazione, volti a limitare la visibilità del malato ai soli familiari e conoscenti.

- SE UNA PERSONA VIENE PORTATA AL PRONTO SOCCORSO O RICOVERATA, CHI PUÒ AVERE NOTIZIE?

 www.aslteramo.it	Regione Abruzzo Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)	Documento: Istruzione Dipendenti Revisione n.: 3.1 Data Emissione: 02.03.2022
	GDPR	pag. 8 di 9

L'ASL, solo in alcuni casi, può dare informazioni, anche per telefono, sulla presenza di una persona al pronto soccorso o sui degenti presenti nei reparti solo ai terzi legittimati, come parenti, familiari, conviventi, conoscenti, personale volontario. L'interessato, se cosciente e capace, deve essere preventivamente informato (ad esempio al momento dell'accettazione) e poter decidere a chi possono essere comunicate notizie sulla propria salute. Occorre comunque rispettare l'eventuale richiesta della persona ricoverata a non rendere note neppure ai terzi legittimati la sua presenza nella struttura sanitaria o le informazioni sulle sue condizioni di salute.

- COME SI DEVONO SVOLGERE I COLLOQUI?

Quando si comunicano informazioni di natura sanitaria, il personale coinvolto, deve evitare che le informazioni sulla salute dell'interessato possano essere conosciute da terzi (a tal proposito non è ritenuto opportuno parlare lungo i corridoi). Stesso obbligo vale per la consegna di documentazione (cartella Sanitaria) quando questo avvenga in situazioni di promiscuità. Pertanto si consiglia di utilizzare gli uffici e se ciò non fosse possibile, assicurarsi che il colloquio o la consegna avvenga in aree in cui non vi siano terzi.

- SI POSSONO DARE NOTIZIE SUI RICOVERATI NEI REPARTI?

Solo in alcuni casi, si possono dare informazioni sulla presenza dei ricoverati nei reparti, ma solo ai terzi legittimati (familiari, conoscenti, personale volontario), previa acquisizione del consenso da parte dell'ospite e o di chi legittimato a tal proposito.

- PUÒ IL MEDICO INFORMARE ALTRE PERSONE SULLO STATO DI SALUTE DI UN SUO ASSISTITO?

In alcuni casi ciò è possibile, ma il paziente deve aver indicato a chi desidera che siano fornite tali informazioni.

Solo alcune figure (medici o altre eventuali figure individuate dal Titolare del trattamento) sono legittimate a fornire informazioni sullo stato di salute direttamente al ricoverato a soggetti diversi, in quest'ultimo caso purché in presenza di uno specifico consenso manifestato dallo stesso ospite o da un suo familiare. Tali informazioni non devono essere fornite in luoghi promiscui, ma necessariamente in luoghi idonei.

- E' POSSIBILE RILASCIARE ANCHE TELEFONICAMENTE INFORMAZIONI SUI DEGENTI RICOVERATI?

In alcuni casi si, ma limitatamente alla loro presenza e alla loro collocazione all'interno della struttura, solo previa autorizzazione scritta dell'interessato acquisita tramite il modulo di Consenso e purché si abbia verosimilmente cognizione dell'identità o della legittimazione ad ottenere i dati richiesti del soggetto chiamante.

INTERNET

- È POSSIBILE CARICARE FOTO O ALTRE INFORMAZIONI RELATIVE A DEGENTI SULLA PROPRIA PAGINA DI FACEBOOK O DI ALTRI SOCIAL NETWORK?

Assolutamente NO. Attenzione a non pubblicare dati personali, ad esempio nomi o fotografie, di pazienti sulle proprie pagine di social network. Anche se spesso si pensa di condividerle solo con amici, magari colleghi

 <p>ASL TERAMO www.aslteramo.it</p>	<p>Regione Abruzzo</p> <p>Istruzioni operative ai DIPENDENTI e COLLABORATORI in materia di protezione dati (Artt. 29 e 32 del GDPR e 2-quaterdecies comma 2 del D. Lgs. 196/2003 novellato dal D.Lgs. 101/2018) Regolamento UE 2016/679 (GDPR)</p>	<p>Documento: Istruzione Dipendenti</p> <p>Revisione n.: 3.1</p> <p>Data Emissione: 02.03.2022</p>
<p>GDPR</p>	<p>pag. 9 di 9</p>	

sanitari, si rischia invece di diffonderle a un numero imprecisato di utenti della rete, violando così la riservatezza delle persone coinvolte.

- LE GRADUATORIE DEI DISABILI BENEFICIARI DI UN CONTRIBUTO PUBBLICO POSSONO ESSERE DIVULGATE SU SITI INTERNET DELLA PUBBLICA AMMINISTRAZIONE?

È sempre vietato diffondere informazioni sulla salute di una persona. Senza venir meno al principio della trasparenza, la pubblica amministrazione deve evitare di pubblicare oltre alla lista dei beneficiari di contributi o di altre agevolazioni anche ulteriori informazioni delicate, quali il tipo di patologia associata al singolo individuo.

