

MANUALE OPERATIVO PER LA CONFORMITÀ AL GDPR

REGOLAMENTO UE679/2016

D.LGS. 101/2018



Versione del Documento

Redatto da	Data di Revisione	Motivo del Rilascio
Dott.ssa M. Galimberti	07/07/2020	1° Rilascio

Approvatori del Documento

Versione Documento	Funzione Aziendale	Data
V1	Direzione Aziendale	07/07/2020

Registro Modifiche di Versione

Versione Documento	Sezione Modificata	Descrizione della Modifica

Indice generale

1. Normative di riferimento.....	4
2. I soggetti	4
3. I principi del trattamento	5
4. Informativa e consenso	5
5. Dati, Trattamenti e basi giuridiche	6
6. Modalità di trattamento, conservazione e cancellazione	7
7. I Diritti dell'interessato	8
8. Le sanzioni	9
9. Gli adempimenti del Titolare di trattamento	9
10. Gli adempimenti degli incaricati.....	9
10.1 Area amministrativa Front Office.....	10
10.1.1 Inserimento dati	10
10.1.2 Informative e consensi	10
10.1.3 Elaborazione e consegna fatture.....	10
10.1.4 Consegna dei referti / risultati	10
10.1.5 Comportamento e riservatezza	10
10.2 Area amministrativa Back Office e contabilità	11
10.3 Area Operativa	11
10.3.1 Fase di erogazione della prestazione	11
10.3.2 Colloqui	11
10.3.3 Presenza di altre persone	12
10.3.4 Pazienti di minore età o interdetti	12
10.3.5 Gestione degli ambienti.....	12

1. Normative di riferimento

La normativa attualmente vigente in materia di trattamento dati è il Regolamento Europeo numero 679 del 2016, entrato in vigore in Italia nel maggio 2018. Il regolamento si è sovrapposto alla normativa nazionale (il vecchio Codice Privacy o Decreto Legislativo 196 del 2003) senza eliminarla del tutto, ma sostituendo la sua disciplina a quella precedente e lasciando vivere il vecchio decreto nelle materie che il regolamento non ha normato. Il nostro legislatore ha quindi emanato il decreto legislativo 181 del 2018 per modificare il codice privacy e identificare le parti eliminate e quelle che rimangono in vigore.

Altre norme sono valide e vanno rispettate anche se emanate prima del regolamento, come le seguenti:

- Legge 179/2107 (disciplina del Whistleblowing), pubblicata sul portale HR disponibile a tutti i dipendenti
- Cookie Law (Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 recepita tramite il provvedimento “Individuazione delle modalità semplificate per l’informativa e l’acquisizione del consenso per l’uso dei cookie, 8 maggio 2014”), disponibile sul sito www.bianalisi.it (sezione cookies - more details)
- Provvedimento del Garante sulla Videosorveglianza, 8 aprile 2010, disponibile sul sito www.garanteprivacy.it
- Linee Guida sul Dossier Sanitario (Allegate alla deliberazione del Garante del 4 giugno 2015) , disponibile sul sito www.garanteprivacy.it
- normativa della Pubblica Amministrazione per la definizione di interesse pubblico (molte norme nei più disparati settori), disponibile sul sito www.garanteprivacy.it
- dichiarazioni del Garante per la Protezione dei Dati (autorizzazioni generali, decisioni di adeguatezza, pareri, provvedimenti), disponibile sul sito www.garanteprivacy.it
- Decreto Legislativo 231 del 2001, ha come oggetto la responsabilità amministrativa delle aziende per reati commessi dal proprio personale e comprende anche il trattamento dati, disponibile sul sito www.camera.it/deleghe

2. I soggetti

Nella normativa e nei documenti necessari a rendere e mantenere l’azienda conforme, sono nominati diversi soggetti identificati come segue.

L’interessato

L’interessato è la persona fisica i cui dati vengono trattati.

Titolare di trattamento

Il Titolare responsabile verso gli interessati è Bianalisi Spa.

Referente interno

La normativa europea non prevede più un responsabile del trattamento dati interno quale “braccio operativo” del titolare di trattamento ma è utile che in azienda ci sia un referente per la materia in questione, che vigili sull’operato degli incaricati/autorizzati e tenga sotto controllo la documentazione. Il referente non va confuso con il responsabile individuato dal regolamento europeo, quest’ultimo infatti esegue trattamenti per conto del titolare e corrisponde al responsabile esterno già previsto in precedenza dalla normativa italiana. Il referente può appoggiarsi all’RPD per ogni questione e supportare l’RPD stesso nella diffusione di documenti o nella raccolta di informazioni. Il referente di Bianalisi Spa a supporto della figura nominata come RPD, Dott.ssa Serenella Saccon, è la Dott.ssa Marina Negri (funzione Dirigente) in collaborazione con la Dott.ssa Maddalena Galimberti (funzione Amministrativa).

Incaricati o autorizzati al trattamento

Tutto il personale interno (dipendenti, autonomi, professionisti, collaboratori, stagisti ecc.) che in ogni modo o per qualunque motivo debba trattare dati deve essere individuato come autorizzato al trattamento in forma scritta. La procedura per la conformità al GDPR e il relativo manuale operativo sono circolarizzati a tutto il personale dipendente affinché sia comunicata in maniera chiara e lineare la modalità del trattamento dei dati.

Responsabile esterno del trattamento

Bianalisi Spa nomina quali Responsabili esterni del trattamento i fornitori/consulenti che lavorano trattando i dati personali in nome e per conto della Società. A sua volta Bianalisi Spa è nominata come Responsabile esterno dai clienti per i quali gestisce i dati di categorie particolari.

Responsabile protezione dati

Bianalisi Spa ha nominato la Dott.ssa Serenella Saccon come RPD o DPO (Data protection officer) che fornisce consulenza e soluzioni a problematiche o dubbi in materia di trattamento dati, controlla la correttezza e completezza della documentazione, esegue le attività che ritiene utili per consentire al titolare la piena conformità e fa da contatto in caso di intervento del Garante per la protezione dei dati.

3. I principi del trattamento

La normativa europea afferma che i trattamenti di dati sono consentiti se effettuati secondo i seguenti principi.

Liceità e correttezza : i dati sono utilizzati per attività ed operazioni autorizzate dalle norme vigenti o effettuato comunque sulle basi giuridiche che li permettono (come indicato al punto 5).

Trasparenza : le informazioni inerenti i trattamenti devono essere accessibili e facilmente comprensibili.

Limitazione delle finalità : i dati devono essere raccolti per finalità determinate, esplicite e legittime e trattati in una modalità che sia compatibile con tali finalità.

Minimizzazione : i dati raccolti e trattati devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità.

Esattezza : i dati devono essere esatti e aggiornati.

Integrità e riservatezza: i dati devono infatti essere sempre trattati in maniera da garantire una sicurezza adeguata, adottando misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

Privacy by design e privacy by default: la protezione dei dati deve essere prevista dal titolare fin dalla progettazione dei sistemi di trattamento dati e, per impostazione predefinita, devono essere trattati solo i dati personali necessari per ogni specifica finalità del trattamento.

Responsabilità del titolare del trattamento: tenuto conto dei dati, dei trattamenti, dei rischi e delle misure adottate, il titolare del trattamento deve garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento stesso.

4. Informativa e consenso

Tutti gli interessati, prima di fornire i propri dati, devono ricevere informazioni complete e chiare tramite un'informativa (scritta ed eventualmente anche spiegata oralmente) che deve contenere :

Chi è il titolare di trattamento

Quali dati raccoglie, tratta e conserva

Per quali scopi (finalità) principali (motivo del consenso principale)

Per quali finalità aggiuntive (che richiedono consensi separati)

Chi avrà accesso ai dati o a chi verranno comunicati

*Dove e per quanto tempo saranno conservati (potrebbe richiedere un consenso aggiuntivo)
Quali sono i suoi diritti e come esercitarli*

Soltanto avendo tali informazioni, l'interessato può dare il proprio consenso al trattamento dei dati. Il consenso, per essere valido, deve essere informato (quindi preceduto dall'informativa completa), libero e specifico (legato alla finalità).

Per i trattamenti a fini di cura il consenso non viene più considerato obbligatorio (se chiedo una prestazione sanitaria so che i miei dati saranno trattati) ma quando un paziente accede ad una struttura sanitaria in realtà fornisce dati anche per altri fini relativi alla contabilità, alla gestione interna, all'organizzazione del lavoro del personale, alle modalità di contatto ecc. perciò è consigliabile continuare a far firmare il consenso generale.

5. Dati, Trattamenti e basi giuridiche

Il regolamento europeo riformula le definizioni dei dati suggerendo anche una scala di "importanza" e necessità di protezione :

- dati personali (qualsiasi dato relativo ad una persona che possa contribuire a identificarla)
- dati di particolari categorie (inerenti la salute, la situazione giudiziaria)
- dati genetici e biometrici (caratteristiche specifiche di una persona)

Le tipologie di trattamento sono identificate in base alla modalità (che ormai è sempre sia in cartaceo che con strumenti elettronici/informatici) e in base alla finalità.

a) La finalità principale per la quale vengono raccolti e trattati dati da un titolare di trattamento è l'esecuzione delle richieste dell'interessato. Per raggiungere lo scopo (o finalità), i dati raccolti sono necessari e quindi l'interessato deve obbligatoriamente fornire questo consenso altrimenti il titolare non potrà soddisfare le sue richieste.

b) Perché il titolare possa operare come azienda, deve adempiere ad obblighi che la normativa gli impone, in ambito contabile, fiscale, organizzativo ecc. Questo scopo viene collegato alla finalità principale come adempimenti connessi e il consenso obbligatorio li comprende.

c) E' invece necessario un consenso separato ed autonomo per la finalità di marketing, cioè per poter utilizzare i dati dell'interessato per inviare messaggi pubblicitari generici in qualsiasi forma (cartaceo, mail, telefono, sms).

d) E' necessario un consenso separato ed autonomo anche per la finalità di profilazione, cioè per poter utilizzare i dati dell'interessato per esaminare le sue preferenze d'acquisto e formulare ed inviare proposte pubblicitarie personalizzate.

e) E' necessario un consenso separato ed autonomo per trasferire i dati degli interessati al di fuori dell'Unione Europea.

f) Non serve un consenso per eseguire analisi dei dati dopo che sono stati resi anonimi oppure se il trattamento è necessario per salvaguardare interessi vitali dell'interessato o di un'altra persona fisica.

Le basi giuridiche che rendono lecito il trattamento sono:

- il consenso espresso dell'interessato (informato e libero)
- l'esecuzione di un contratto (e di eventuali necessarie misure precontrattuali)
- adempiere un obbligo legale o ad ordini di autorità
- salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica
- compito di interesse pubblico o connesso all'esercizio di pubblici poteri (Pubbliche Amministrazioni)

- legittimo interesse del titolare del trattamento (purché di importanza pari al diritto alla riservatezza dell'interessato)

6. Modalità di trattamento, conservazione e cancellazione

I trattamenti devono essere eseguiti avendo come primo obiettivo il mantenimento dell'integrità e della riservatezza dei dati.

Ciò implica che :

a) Gli strumenti elettronici / informatici utilizzati devono garantire tali caratteristiche ed essere dotati delle misure di sicurezza necessarie. Ad esempio, misure hardware sono il firewall (protegge la rete da intrusioni), i gruppi di continuità (proteggono i computer da sbalzi o mancanze di alimentazione), armadi dedicati per la collocazione sicura di server e apparati, sale chiuse e con condizionamento ambientale per la collocazione di server e apparati. Misure software sono ad esempio il software antivirus, il software antimalware, i servizi antivirus e antimalware associati a caselle email, i software di verifica del backup. Misure organizzative sono ad esempio l'utilizzo corretto di credenziali di autenticazione, il rispetto delle procedure aziendali di utilizzo degli strumenti, la periodica manutenzione, i servizi di assistenza.

b) Il materiale cartaceo che contiene dati deve essere correttamente gestito e conservato, è considerato sempre sotto la custodia della persona che lo produce o preleva dall'archivio, non deve essere lasciato incustodito o a vista in aree ad accesso del pubblico, deve sempre essere riposto al termine dell'utilizzo, deve essere conservato in armadi o locali chiusi a chiave fuori dagli orari lavorativi.

La normativa richiede ai titolari di trattamento di conservare i dati soltanto per il tempo necessario al perseguimento delle finalità per le quali sono stati raccolti. Nell'ambito dei servizi di carattere sanitario il tempo di conservazione è determinato anche da obblighi normativi diversi, infatti la conservazione di documenti, referti e reperti è soggetta alle regole del Titolario e Massimario di Scarto della Regione Lombardia mentre le norme in materia di contabilità e fisco impongono tempi minimi di conservazione dei documenti contabili. Non è quindi possibile comunicare all'interessato un limite temporale preciso, si farà genericamente riferimento al tempo per il quale i dati saranno considerati utili.

Anche dopo l'eventuale scadenza dei tempi dettati dalle diverse normative, l'azienda dovrà considerare se distruggere o conservare documenti che in un futuro possano servire in caso di contestazioni, reclami, giudizi civili e richieste di risarcimento.

Ne consegue che la tendenza è di conservare i dati molto a lungo, questo implica la necessità di proteggere i dati conservati evitando che vengano distrutti, comunicati a persone non autorizzate, lasciati a disposizione di persone non autorizzate, diffusi, erroneamente modificati. Per garantire l'ottimale conservazione l'azienda deve implementare sistemi di backup ridondanti e sottoposti a verifiche periodiche e attuare tutte le misure idonee a rendere sicuro il sistema informatico e l'archivio cartaceo. Infine, ove il dato si consideri non più utile o necessario, sorge l'obbligo di cancellarlo (art. 5, par.1 lett. e GDPR). Allo stesso modo, se l'azienda dismette supporti (ad esempio hard disk) è necessario che i dati su di essi siano cancellati e non recuperabili, perciò si consiglia sempre di rendere i supporti fisicamente inutilizzabili prima di consegnarli a terzi per lo smaltimento.

Bianalisi Spa in collaborazione con l'RPD ha preparato un elenco con le seguenti caratteristiche:

- aree aziendali
- tipologie di documenti da conservare all'interno di ogni area
- modalità di conservazione e tempistica

Tale report è stato circolarizzato ad ogni funzione aziendale al fine di regolamentare le modalità del trattamento, conservazione e cancellazione.

7. I Diritti dell'interessato

Tutti gli incaricati di trattamento devono conoscere i concetti relativi ai diritti degli interessati per poter dare immediate informazioni ove richiesto dai clienti/utenti/pazienti. I diritti degli interessati si possono riassumere come segue :

Il Diritto di Informativa art 13 GDPR

Ogni persona che fornisce propri dati deve essere adeguatamente informata, deve poter leggere l'informativa prima di fornire il consenso al trattamento dati.

Il Diritto di Accesso, Rettifica e Cancellazione

Ogni persona ha diritto di sapere se i propri dati sono stati raccolti e vengono trattati, di quali dati si tratta e per quali fini. Ha diritto anche di chiederne la correzione se errati o la cancellazione se non sono utili per il trattamento identificato o se sono stati raccolti senza il suo consenso.

Il Diritto all'Oblio

Il diritto all'oblio è il diritto di ognuno di noi a mantenere riservate informazioni che, seppur correttamente rese pubbliche in passato, non vogliamo siano ripubblicate senza un motivo valido (un motivo che sia più importante della nostra riservatezza e dignità morale). Le informazioni pubblicate in rete sono difficili da eliminare, perciò possono essere ritrovate anche dopo molto tempo dall'originale pubblicazione. Per consentire alle persone di far cadere alcune informazioni nell'oblio, l'Unione Europea ha imposto ai maggiori motori di ricerca di mettere a disposizione degli utenti dei moduli di richiesta tramite i quali ognuno può chiedere che determinate informazioni non vengano mostrate come risultato delle ricerche effettuate dagli utenti.

Nell'ambito di un'attività aziendale e soprattutto quando l'attività consiste nell'erogazione di servizi per la salute delle persone, il diritto all'oblio si traduce nel diritto di richiedere la cancellazione oppure l'oscuramento di informazioni, nei limiti di quanto la normativa ci consente.

Il Diritto alle Portabilità dei Dati Personali

Ogni interessato può chiedere che i propri dati vengano consegnati ad un altro fornitore di servizi, restando comunque limitata la possibilità di cancellazione a causa della normativa vigente nel settore di attività aziendale.

Il Diritto di Opposizione

Gli interessati hanno diritto di opporsi al trattamento se questo esula dalle finalità per le quali hanno dato consenso o se desiderano che il trattamento abbia termine (sempre nei limiti che la normativa consente).

Il Diritto di Limitazione

Gli interessati, nei limiti della normativa, possono chiedere che i dati siano conservati ma usati solo su esplicito consenso, per difesa giudiziale o per tutelare diritti di pari grado di altre persone o interessi pubblici

Il Diritto di presentare Reclamo o Ricorso

Ogni interessato può rivolgersi anche al Garante in caso ritenga che i propri diritti siano stati violati.

8. Le sanzioni

Il Titolare di trattamento è responsabile verso l'interessato per ogni danno egli subisca in relazione al trattamento dei suoi dati effettuato in modalità non sicura, per finalità diverse da quelle dichiarate al momento della raccolta, o se non gli permette di esercitare i suoi diritti. L'interessato può rivolgersi al Garante tramite un reclamo o può ricorrere alla tutela giudiziaria e chiedere un risarcimento danni.

Il Garante, oltre che in caso di richieste da parte di interessati, può agire anche di iniziativa e sanzionare il titolare per violazioni della normativa.

Il Garante interviene tramite:

- sanzioni amministrative pecuniarie
le sanzioni pecuniarie sono molto pesanti, si arriva a milioni di euro o percentuali di fatturato
- poteri correttivi
può essere richiesto all'azienda di modificare le sue modalità di lavoro o interrompere operazioni in corso ma si arriva anche al ritiro di autorizzazioni, accreditamenti o certificazioni e limitazioni nei rapporti con enti dello Stato

9. Gli adempimenti del Titolare di trattamento

Il titolare di trattamento è responsabile per l'attuazione di tutti gli adempimenti richiesti dalla normativa vigente:

- effettuare un'analisi dei rischi che incombono sui dati
- selezionare e realizzare le misure di Sicurezza
- effettuare gli incarichi e le nomine
- fornire agli incaricati istruzioni e regole operative
- realizzare il Registro delle Attività di Trattamento
- mantenere una procedura per la violazione dei dati personali (Data Breach)
- eseguire la valutazione d'impatto dei trattamenti sui dati
- mantenere la documentazione di accountability (evidenze della realizzazione delle misure)

Per poter adempiere alla normativa, il titolare deve affidarsi all'impegno e alla professionalità del personale che lavora presso la sua struttura, che permette all'azienda di restare conforme attenendosi alle istruzioni ricevute e svolgendo con cura e attenzione il proprio lavoro in ogni aspetto.

10. Gli adempimenti degli incaricati

Bianalisi Spa stà provvedendo a circolarizzare, attraverso procedure scritte, tutti i principali processi aziendali al fine di fornire linee guida/istruzioni operative/regole che permettano la compliance aziendale.

Alcune regole di riservatezza valgono per tutti e in qualsiasi ambito operativo:

- qualsiasi informazione di cui si venga a conoscenza in relazione ad un paziente, che sia inerente il servizio erogato oppure no, è un dato riservato sul quale mantenere il più assoluto riserbo
- i doveri di riservatezza rimangono validi anche se il rapporto di lavoro cessa o si modifica
- i doveri di riservatezza sono validi anche nei confronti dei colleghi, ai quali si potranno e dovranno comunicare solo le informazioni necessarie perché svolgano consapevolmente e in modo ottimale il

proprio lavoro mentre non si dovranno comunicare le informazioni non inerenti di cui il paziente ci ha messo a conoscenza (o i famigliari o altri)

10.1 Area amministrativa Front Office

Nell'ambito del trattamento dati, il personale con mansioni relative all'accettazione ha contatto con pazienti (e accompagnatori) e ha diversi compiti e responsabilità come di seguito descritto.

10.1.1 Inserimento dati

Il personale deve raccogliere i dati necessari (parlando con i pazienti e tramite documenti) ed inserirli in database assicurandosi di non registrare dati non utili, di controllare l'esattezza dei dati (per evitare che dati inerenti la salute di un paziente vengano associati ad altri), di colloquiare in modo da non portare a conoscenza altre persone di dati riservati.

10.1.2 Informativa e consensi

Il personale di accettazione deve consegnare le informative all'utenza e raccogliere il consenso al trattamento, spiegando che l'informativa è disponibile, mostrandola e accertandosi di far apporre le firme al soggetto interessato o a chi ne ha la responsabilità genitoriale (per i pazienti minorenni) o la tutela (per pazienti interdetti o privi di capacità di intendere e volere). Ove i moduli richiedano una compilazione, si deve verificare che tutto sia stato correttamente indicato. Persone che non hanno la responsabilità genitoriale o la tutela non possono firmare (fratelli, nonni ecc.). Chi ha la responsabilità genitoriale può delegare altri tramite una delega formale accompagnata dalla copia della carta di identità del delegante.

In caso di pazienti di minore età è compito dell'operatore di accettazione informare l'accompagnatore delle regole di accesso:

- l'accompagnatore deve essere presente durante le prestazioni se il paziente è minorenne
- il paziente di 14 anni o più può chiedere che l'accompagnatore non sia presente durante la prestazione ma sia l'accompagnatore che il professionista che eroga la prestazione devono essere d'accordo
- in caso di terapie che richiedono più prestazioni, chi ha la responsabilità genitoriale deve accompagnare il minore alla prima seduta, per le sedute successive è possibile che il minore che ha già compiuto 14 anni acceda da solo se chi ha la responsabilità genitoriale acconsente (dichiarandolo in forma scritta al momento dell'accettazione)

10.1.3 Elaborazione e consegna fatture

La fase di elaborazione e consegna della fattura richiede la verifica dei dati del destinatario.

10.1.4 Consegna dei referti / risultati

Ogni documento che contenga dati inerenti la salute deve essere consegnato in busta chiusa. Il momento della consegna di referti e risultati è molto delicata, richiede una verifica attenta del destinatario per non incorrere in gravi errori consegnando referti di una persona ad un'altra. Ove accada, bisogna cercare di recuperare il referto al più presto.

10.1.5 Comportamento e riservatezza

All'accettazione si presentano a volte più persone contemporaneamente, perché sono attivi più "sportelli" o perché il pubblico non rispetta le distanze di attesa o perché persone si avvicinano per chiedere informazioni. Consapevoli di questo, gli operatori devono ricordare di mantenere un tono di voce normale/basso, non ripetere informazioni non necessarie, non lasciare documenti a vista.

Non è consentito fornire informazioni relative a referti e risultati (dati inerenti la salute di persone fisiche) al telefono e, durante i colloqui telefonici, è necessario mantenere un tono di voce medio/basso.

10.2 Area amministrativa Back Office e contabilità

Nell'ambito del trattamento dati, il personale con mansioni di back office ha il compito di:

- elaborare dati ed informazioni trattando dati dell'utenza
- seguire le procedure e le istruzioni ricevute

Nell'ambito del trattamento dati, il personale con mansioni amministrative di contabilità ha il compito di:

- elaborare dati ed informazioni trattando dati dell'utenza
- elaborare dati ed informazioni trattando dati di clienti, fornitori, personale interno
- elaborare dati ed informazioni trattando dati del titolare di trattamento di natura economico finanziaria
- seguire le procedure e le istruzioni ricevute

Le mansioni d'ufficio consistono essenzialmente nel trattamento di dati, perciò i doveri di riservatezza e corretta gestione dei dati fanno parte del lavoro quotidiano. E' necessario prestare particolare attenzione alle modalità di comunicazione delle informazioni, che fornitori e aziende clienti a volte cercano di condizionare.

10.3 Area Operativa

Nell'ambito del trattamento dati, il personale operativo ha contatto diretto con pazienti e personale interno. Nei confronti di colleghi e collaboratori si richiama il generale dovere di mantenere rapporti caratterizzati da cortesia, correttezza e collaborazione allo scopo di rendere il luogo di lavoro un ambiente positivo e produttivo per tutti.

Nei confronti dell'utenza (pazienti, clienti, famigliari, accompagnatori ecc.), ogni operatore ha il compito di svolgere le proprie mansioni seguendo le istruzioni ricevute, ricordando che la riservatezza delle informazioni di cui si viene a conoscenza è parte essenziale della professionalità di chi opera nel settore sanitario. Le principali regole da seguire si possono brevemente riassumere come segue.

10.3.1 Fase di erogazione della prestazione

I doveri di riservatezza sono validi soprattutto durante l'erogazione delle prestazioni, momento nel quale il paziente è più vulnerabile, può lasciarsi andare in conversazioni e racconti e parlare di sé e della propria salute o della famiglia. L'operatore deve mantenere toni neutri e ricordare che ogni informazione ricevuta è da ritenersi assolutamente riservata (anche in caso di pazienti che parlano tra loro). Il paziente non deve essere lasciato solo in ambulatorio e, comunque, in ambulatorio non devono essere lasciati a vista documenti che riportino dati relativi a pazienti. Non è consentito far fotografare i contenuti visualizzati a monitor, o documenti di qualsiasi genere.

Ove un collega debba comunicare informazioni urgenti, è necessario spostarsi almeno all'ingresso, parlando a bassa voce ed evitando di nominare altri pazienti.

Le porte degli ambulatori devono essere chiuse.

10.3.2 Colloqui

Ogni colloquio, tra colleghi o tra operatore e paziente, deve essere svolto in area riservata, ad esempio all'interno di un ambulatorio. Si deve evitare il colloquio in aree di passaggio o di attesa.

10.3.3 Presenza di altre persone

Anche se il paziente è accompagnato, è sempre necessario valutare la situazione ed eventualmente (se il paziente appare lucido e consapevole ed è maggiorenne) chiedere al paziente se desidera essere da solo durante il colloquio con l'operatore che comunica diagnosi, terapie o altre informazioni relative alla salute.

10.3.4 Pazienti di minore età o interdetti

Per i pazienti di minore età (o interdetti), la fase di accettazione viene svolta da chi ne esercita la responsabilità genitoriale o la tutela. Ciò significa che quando il paziente viene chiamato per la prestazione sono stati già correttamente forniti i consensi. Durante la prestazione, per soggetti interdetti o minori di anni 18 deve essere presente l'accompagnatore. L'operatore potrà valutare eventuali richieste dell'accompagnatore che desidera far accedere il paziente da solo se quest'ultimo ha almeno 14 anni, ricordando che si tratta di un'eccezione alla procedura.

10.3.5 Gestione degli ambienti

In generale gli operatori devono rispettare le regole stabilite dall'azienda per quanto riguarda le aree da mantenere chiuse, le aree dove possono o non possono sostare i pazienti, l'utilizzo di strumenti e materiali, le modalità di accesso ai locali, le modalità di smaltimento dei rifiuti ecc.

In particolare, nel caso si debba distruggere un documento cartaceo, si dovrà utilizzare un distruggi-documenti.

Come regola generale, i pazienti o le persone che non lavorano presso la sede devono avere accesso autonomo soltanto alle aree comuni (di passaggio e di attesa), essere accompagnate dal personale nelle aree di erogazione dei servizi e non avere accesso alle aree di conservazione del cartaceo, sale server, uffici, back office di accettazione.

In collaborazione con l'RSPP aziendale, Bialisi Spa regolerà gli accessi in entrata e in uscita e le relative norme di sicurezza.