**PARTE SPECIALE**

**REATI IN MATERIA DI**

**VIOLAZIONE DEL DIRITTO DI AUTORE**

**INDICE**

[1. LA TIPOLOGIA DEI REATI IN MATERIA DI REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE (ART. 25-novies D.Lgs. 231/2001) 3](#_Toc164323293)

[2. IL FRAMEWORK DI RIFERIMENTO 3](#_Toc164323294)

[3. PROCESSI AZIENDALI E ATTIVITÀ SENSIBILI 4](#_Toc164323295)

[4. SOGGETTI COINVOLTI 4](#_Toc164323296)

[5. DOCUMENTI AZIENDALI DI RIFERIMENTO 4](#_Toc164323297)

[6. DIVIETI, OBBLIGHI E PRINCIPI DI COMPORTAMENTO 4](#_Toc164323298)

[7. PROCEDURE, PRASSI E ISTRUZIONI OPERATIVE DEI PROTOCOLLI SPECIALI 12](#_Toc164323299)

## LA TIPOLOGIA DEI REATI IN MATERIA DI REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE (ART. 25-novies D.Lgs. 231/2001)

Nell’ambito delle Strutture sanitarie sono state individuate le seguenti fattispecie concrete:

|  |  |
| --- | --- |
| Protezione penale dei diritti di utilizzazione economica e morale (art. 171, co. 1, lett. a-bis e co. 3, l. 633/1941) | Tale fattispecie può realizzarsi quando, ad esempio, un soggetto della struttura sanitaria si appropria di ricerche concernenti i risultati di attività realizzate da altri soggetti e le pubblica sul sito Internet dell'Ente come se fossero proprie. |
| Tutela penale del software e delle banche dati (art. 171-bis l. 633/1941) | Tale fattispecie può realizzarsi quando, ad esempio, i dipendenti di una struttura sanitaria utilizzano sistematicamente copie di programmi software non autorizzate, violando il diritto d’autore. |
| Tutela penale delle opere audiovisive (art. 171-ter l. 633/1941) | Tale fattispecie può realizzarsi quando, ad esempio, i dipendenti di un ente utilizzano e distribuiscono materiale divulgativo, in particolare fotocopiando opere protette, per distribuirle ad altri, a pagamento, e non per scopo di lettura, studio, consultazione, in violazione delle regole e limiti stabiliti (es. limite massimo del 15% di ciascun volume). |
| Responsabilità penale relativa ai supporti (art. 171-septies l. 633/1941) | Tale fattispecie può realizzarsi quando un dipendente di una struttura sanitaria dichiara falsamente l’avvenuto assolvimento degli obblighi derivanti dalla normativa sul diritto d’autore e sui diritti connessi. |
| Responsabilità penale relativa a trasmissioni audiovisive ad accesso condizionato (art. 171- octies l. 633/1941 | Tale fattispecie può realizzarsi quando, ad esempio, i soggetti di una struttura sanitaria utilizzano un apparato atto alla decodificazione ad uso privato di trasmissioni audiovisive via satellite ad accesso condizionato, per uso personale nella struttura o messo a disposizione dei pazienti (con o senza il pagamento del servizio) in modo da eludere le misure tecnologiche di protezione poste in essere dall'emittente, con la finalità fraudolenta di sottrarsi al pagamento del canone dovuto per l'accesso ai programmi. |

## IL FRAMEWORK DI RIFERIMENTO

L’attività di mappatura del rischio ha seguito il seguente framework concettuale *[a titolo esemplificativo]* per cui ogni fattispecie concreta di reato analizzato nella parte speciale vede coinvolti uno o più processi aziendali i quali, a loro volta, comprendono una o più attività sensibili nell’ambito delle quali sono posti dei (i) divieti, (ii) degli obblighi e (iii) dei principi di comportamento (uno o più di uno per singola tipologia) che, rispettati e attuati, sono posti a presidio della responsabilità *ex* D.Lgs. 231/2001 dell’Ente al fine di evitare che tali reati possano essere compiuti nell’interesse o a vantaggio della Struttura Sanitaria stessa.

## PROCESSI AZIENDALI E ATTIVITÀ SENSIBILI

In riferimento al reato di cui alla presente parte speciale sono stati individuati i seguenti processi e attività sensibili:

*[Inserire i processi aziendali e le attività sensibili riguardanti la struttura sanitaria, collegandoli ai processi e alle attività descritti nel paragrafo 6]*

## SOGGETTI COINVOLTI

Tutti i soggetti Destinatari del presente modello organizzativo e coinvolti nei macro-processi e nelle attività sensibili, nell’ambito della propria attività, al rispetto dei divieti, dei principi e dei presidi posti in essere dall’Ente nell’ambito del proprio sistema regolatorio.

# DOCUMENTI AZIENDALI DI RIFERIMENTO

Tutti i soggetti Destinatari coinvolti nei macro-processi e nelle attività sensibili sono tenuti, nell’ambito della propria attività, al rispetto delle norme di comportamento di seguito indicate, conformi ai principi dettati dal Modello e dal Codice Etico.

In particolare, nell’espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, bisogna conoscere e rispettare anche tutte le regole e i principi contenuti nei seguenti documenti:

*[Elencare la normativa di riferimento nazionale e regionale o di settore nonché i documenti a cui fanno riferimento aziendale i destinatari del modello quali, ad esempio, certificazioni di qualità, mansionari, job descriptions, codice di corporate governance delle società quotate, regolamento parti correlate, codice di internal dealing, istruzioni operative per la redazione delle situazioni finanziarie annuali e periodiche, ecc.].*

# DIVIETI, OBBLIGHI E PRINCIPI DI COMPORTAMENTO

Mappati i processi e le attività sensibili sono stati individuati i seguenti divieti, obblighi e principi di comportamento:

|  |
| --- |
| **Processo/Attività/dovere-divieto-principio di comportamento** |
| **Processo di approvvigionamento** |
| **Attività di approvvigionamento di beni, servizi e appalti condotti dalla Società, comprensive delle attività di selezione, valutazione e gestione dei fornitori, della definizione delle vendor list** |
| **Divieto** |
| È vietato negoziare condizioni contrattuali occulte, che non risultino da idonea documentazione conservata unitamente a quella relativa all'acquisto |
| **Processo di gestione della comunicazione** |
| **Attività di Public Relation, partecipazione a convegni, meeting, tavoli di lavoro organizzati da enti pubblici e associazioni di categoria** |
| **Divieto** |
| È vietato porre in essere comportamenti in contrasto con leggi e regolamenti in materia di tutela del diritto d’autore |
| È vietato diffondere immagini, documenti o altro materiale tutelato dalla normativa in materia di diritto d’autore |
| **Dovere** |
| Devono essere verificate, prima della loro diffusione, tutte le informazioni/dati/documenti utilizzati per la promozione dell’immagine aziendale e dei prodotti, al fine di escludere che siano protetti dalla normativa in materia di diritto d’autore |
| **Principio di comportamento** |
| Sono posti in essere controlli sul materiale informativo e documentale utilizzato nel corso di convegni o eventi, al fine di escludere che sia protetto dalla normativa in materia di diritto d’autore |
| **Processo di gestione delle risorse umane** |
| **Selezione, assunzione e formazione del personale** |
| **Principio di comportamento** |
| Con riferimento alle risorse umane sono condotte specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza dei sistemi informativi per tutti i dipendenti e, dove rilevante, per i terzi |
| Con riferimento alle risorse umane vi è una valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso |
| **Processo Gestione Sistema Informativo** |
| **Duplicazione o riproduzione di opere protette dal diritto d’autore** |
| **Divieto** |
| La struttura informa gli utenti che è vietato detenere elementi di decodificazione speciale senza il pagamento del canone dovuto, nonché trasmettere o diffondere servizi criptati ad accesso condizionato |
| La struttura informa gli utenti che è vietato detenere, porre in commercio o cedere a qualsiasi titolo supporti privi del contrassegno SIAE laddove questo contrassegno sia previsto per legge |
| La struttura informa gli utenti che è vietato duplicare, eliminare, contraffare o alterare il contrassegno SIAE in relazione ai prodotti per i quali tale contrassegno sia prescritto |
| La struttura informa gli utenti che è vietato impiegare strumenti atti ad eludere le misure tecnologiche di protezione relative ad opere e materiale protetti |
| È vietato utilizzare, sfruttare, diffondere o riprodurre indebitamente a qualsiasi titolo, in qualsiasi forma, a scopo di lucro o a fini personali opere dell’ingegno di qualsiasi natura coperte dal diritto d’autore |
| **Dovere** |
| Nel caso in cui la società sia tenuta a comunicazioni obbligatorie nei confronti della SIAE, è individuato il soggetto deputato alle suddette comunicazioni, specificandone le relative competenze. I dati oggetto di comunicazione devono essere controllati prima del relativo invio da un soggetto diverso da quello individuato quale responsabile delle comunicazioni obbligatorie. Al soggetto deputato alle comunicazioni è fatto obbligo di provvedere anche alla loro archiviazione |
| **Principio di comportamento** |
| La Struttura informa gli utenti che non è possibile utilizzare il masterizzatore per usi diversi da quelli strettamente collegati all’attività aziendale |
| Viene effettuata la verifica annuale circa l’utilizzo, la detenzione, la commercializzazione, la duplicazione e la riproduzione di software e banche dati non contrassegnati SIAE |
| **Gestione dati e informazioni riservate** |
| **Principio di comportamento** |
| Con riferimento alla classificazione e controllo dei beni, i ruoli e le responsabilità per l’identificazione e la classificazione degli assets aziendali (ivi incluse le categorie di dati trattati) sono chiaramente e formalmente definiti |
| **Gestione dei programmi software per elaboratore** |
| **Divieto** |
| È vietato procedere ad installazione di prodotti software in violazione degli accordi contrattuali di licenza d’uso e, in generale, di tutte le leggi e i regolamenti che disciplinano e tutelano la licenza d’uso |
| È vietato utilizzare software/banca dati in assenza di valida licenza, o qualora la licenza sia scaduta |
| **Dovere** |
| Deve essere controllata periodicamente la regolarità delle licenze dei prodotti in uso e procedendo, ove necessario, ai dovuti rinnovi |
| **Principio di comportamento** |
| Vi sono revisioni periodiche, almeno annuali, dei contratti di licenza in essere |
| La struttura sanitaria informa gli utenti che non è possibile installare nessun software o hardware che non sia stato approvato dai sistemi informativi |
| Il download e l’installazione di software o file per uso esclusivamente professionale sono consentiti ai soli addetti del Sistema Informativo Aziendale |
| È individuata una diversa figura aziendale deputata a verificare la corrispondenza tra i programmi software e le banche dati – non contrassegnati SIAE – lecitamente detenute e quelle “in generale” utilizzate (Responsabile area tecnico-amministrativa) |
| È consentivo solo installare software/banche dati tutelati dal diritto d’autore |
| **Gestione dei sistemi hardware** |
| **Principio di comportamento** |
| Nel caso in cui si riscontri un possibile utilizzo improprio delle strumentazioni informatiche, il Sistema Informativo Aziendale associa il nominativo dell’utilizzatore all’indirizzo IP e dà informazione al lavoratore interessato, con possibilità di contraddittorio e, qualora necessario ai fini istruttori, al relativo Responsabile il quale, sentito il lavoratore, valuterà l’attinenza dei dati rispetto all’attività lavorativa. A seguito dell’avvenuto accertamento dell’utilizzo improprio delle attrezzature informatiche, il responsabile attiva le procedure disciplinari finalizzate, al primo comportamento accertato, all’applicazione del richiamo, salvo casi di particolare gravità. Delle sanzioni applicate viene data informazione anche al Direttore Generale |
| È prevista una mappatura dei dispositivi hardware dotati di masterizzatore |
| È prevista una mappatura dei dispositivi hardware e dei programmi software (Sistema Informativo Aziendale) |
| È prevista una mappatura di tutti gli apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato |
| È prevista una mappatura di tutti gli uffici che possono avere accesso ai sistemi informatici e audiovisivi criptati |
| È prevista una mappatura di tutti i soggetti che possono avere accesso agli apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato |
| È prevista una mappatura di tutti i supporti o altri strumenti informatici per il quale sia prescritto il contrassegno SIAE |
| È individuata una figura aziendale deputata a gestire l’aggiornamento della mappatura sia dei dispositivi hardware e software, sia delle licenze relative a software e banche dati (Amministratore di sistema; Referente dei Sistemi informativi) |
| La struttura, con riferimento alla sicurezza fisica e ambientale, adotta adeguati controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature |
| **Gestione dei sistemi informativi aziendali** |
| **Dovere** |
| Con riferimento alle risorse umane è previsto l’obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, ecc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto, con firma per ricevuta da parte della Struttura |
| **Principio di comportamento** |
| Al fine di garantire una adeguata gestione delle comunicazioni e dell’operatività per il corretto e sicuro funzionamento degli elaboratori di informazioni la struttura è dotata di una verifica di controllo sui cambiamenti agli elaboratori e ai sistemi |
| Esiste un inventario fisico dei beni informatici della Struttura e viene costantemente aggiornato |
| Sono formalmente definite le modalità di inventariazione dei beni aziendali (incluse le basi dati in essi contenute) utilizzati ai fini dell'operatività del sistema informatico e telematico |
| Sono formalmente definiti ruoli, responsabilità e modalità operative per la gestione del contenuto delle banche dati |
| **Gestione dei sistemi software** |
| **Dovere** |
| A tutti i Destinatari sono comunicate le modalità di comportamento che devono essere assunte per un corretto e lecito utilizzo dei software e banche dati in uso |
| **Principio di comportamento** |
| Sono gestite le policy aziendali per distribuzione software e accesso ai programmi |
| È effettuata la mappatura di tutti gli uffici che possono avere accesso a supporti o altri sistemi informatici per i quali sia prescritto il contrassegno SIAE |
| È effettuata la mappatura di tutti i sistemi informatici e audiovisivi criptati di decodificazione speciale |
| È effettuata la mappatura delle licenze software e delle banche dati (Sistema Informativo Aziendale) |
| **Gestione dell’utilizzo di strumenti elettronici nell’ambito del rapporto di lavoro; gestione di assegnazione e uso di apparecchiature di telefonia mobile al personale** |
| **Divieto** |
| La struttura informa gli utenti che sono vietate la diffusione e la distribuzione di opere o altri materiali protetti rispetto ai quali siano state rimosse le protezioni |
| La struttura informa gli utenti che è vietato utilizzare, per fini differenti rispetto a quelli propri leciti, gli apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato. |
| **Dovere** |
| Devono essere verificati i prodotti in uso su ciascuna postazione |
| **Principio di comportamento** |
| L’utilizzo improprio degli strumenti elettronici può essere oggetto delle sanzioni disciplinari; per le sanzioni, le procedure e le competenze, si rinvia al codice disciplinare aziendale |
| La struttura definisce chiaramente all’interno di apposito regolamento le modalità per l’assegnazione e l’uso degli strumenti elettronici da parte del personale dipendente per l’espletamento dell’attività di servizio |
| **Gestione delle attività relative alla sicurezza informatica** |
| **Principio di comportamento** |
| Al fine di garantire una adeguata gestione delle comunicazioni e dell’operatività per il corretto e sicuro funzionamento degli elaboratori di informazioni la struttura è dotata di una protezione da software pericoloso |
| Al fine di garantire una adeguata gestione delle comunicazioni e dell’operatività per il corretto e sicuro funzionamento degli elaboratori di informazioni la struttura è dotata di una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni è prevista la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuisce il diritto di accesso |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni, è prevista la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti |
| Con riferimento all’organizzazione della sicurezza per gli utenti esterni sono formalmente definiti i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all’azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l’elaborazione dei dati e informazioni da parte degli stessi terzi |
| Con riferimento all’organizzazione della sicurezza per gli utenti interni sono formalmente definiti i ruoli e la responsabilità nella gestione delle modalità di accesso di utenti interni all’azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici |
| Con riferimento alla crittografia vi è l’implementazione e lo sviluppo sull’uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche |
| Con riferimento alla gestione degli incidenti e dei problemi di sicurezza informatica sono poste in essere adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica e in particolare vi è attenzione per la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva |
| Con riferimento alla gestione degli incidenti e dei problemi di sicurezza informatica sono poste in essere adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica, e in particolare vi è una chiara identificazione di ruoli, responsabilità e modalità operative delle attività di verifica periodica dell’efficienza ed efficacia del sistema di gestione della sicurezza informatica |
| Con riferimento alla sicurezza nell’acquisizione, sviluppo e manutenzione dei sistemi informativi esistono procedure che garantiscono la confidenzialità, autenticità e integrità delle informazioni |
| Con riferimento alla sicurezza nell’acquisizione, sviluppo e manutenzione dei sistemi informativi vi è l’identificazione di requisiti di sicurezza in fase di progettazione o modifica dei sistemi informativi esistenti |
| Con riferimento alla sicurezza nell’acquisizione, sviluppo e manutenzione dei sistemi informativi vi è una chiara e formalizzata policy per la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni |
| Vengono effettuate periodiche verifiche di sicurezza, da parte del Sistema Informativo Aziendale, aventi ad oggetto dati generali, consistenti in: verifiche giornaliere sui log del sistema firewall; verifiche dei software installati sui sistemi server e client; verifiche sul traffico di rete; verifiche sull’efficienza dei sistemi Proxy; verifiche sui sistemi antivirus; verifiche sull’efficacia dei filtri antispam; inserimento nella black-list di siti palesemente a valenza non istituzionale da parte del Sistema Informativo Aziendale |
| **Gestione di accessi, account e profili** |
| **Principio di comportamento** |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni è prevista l’autenticazione individuale degli utenti tramite codice identificativo dell’utente e password o altro sistema di autenticazione sicura |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni è prevista la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni è prevista una lista di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni è prevista una procedura di registrazione e de-registrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni è previsto il blocco delle postazioni di lavoro dopo un periodo predefinito di inattività |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni è previsto l’accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete |
| Sono formalmente definite le modalità di monitoraggio delle banche dati al fine di prevenire accessi non autorizzati mediante un sistema che monitorizza gli accessi |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni sono previste regole per l’utilizzo e la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, ecc.) |
| Con riferimento al controllo degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni sono previsti piani e procedure operative per le attività di telelavoro |
| **Gestione di tutte le attività aziendali nelle quali è previsto l'utilizzo di servizi informatici** |
| **Principio di comportamento** |
| La struttura è dotata di una politica in materia di sicurezza del sistema informativo con l’indicazione: (i) delle modalità di comunicazione, (ii) delle modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi |
| **Utilizzo dei sistemi di navigazione Internet** |
| **Principio di comportamento** |
| È prevista: la conservazione dei dati inerenti al traffico internet (log di navigazione) per un periodo non superiore a un mese (tali dati non sono oggetto di archiviazione di backup); la conservazione dei messaggi di posta elettronica per un periodo non superiore a un mese (tali archivi sono oggetto di backup giornaliero ma non hanno archivio storico collegato). I periodi di conservazione possono essere superati in caso di richiesta dell’autorità giudiziaria o di polizia giudiziaria per indagini in corso, nonché, in via eccezionale, a fronte di fatti illeciti già accaduti |
| È individuata una specifica figura aziendale volta a verificare l’inserimento del materiale sul sito aziendale |
| I dati inerenti al traffico Internet e la posta elettronica non sono in alcun modo oggetto di diffusione; sono eventualmente oggetto di comunicazione su richiesta dell’autorità giudiziaria e/o qualora necessari a difesa dell’azienda in ambito giudiziale |
| La Struttura ha chiaramente informato gli utenti che non è possibile utilizzare la rete internet per usi diversi da quelli strettamente collegati all’attività aziendale |
| Viene condotta periodicamente una verifica circa l’utilizzo o la diffusione, sul sito, di opere dell’ingegno senza la necessaria autorizzazione e/o il pagamento dei dovuti compensi all’autore |
| **Predisposizione, modificazione, trasmissione, archiviazione e custodia di dati, informazioni o documenti per via o su supporto telematico o informatico** |
| **Principio di comportamento** |
| Al fine di garantire una adeguata gestione delle comunicazioni e dell’operatività per il corretto e sicuro funzionamento degli elaboratori di informazioni, la struttura è dotata di una procedura per la gestione di dispositivi rimovibili |
| La Struttura informa gli utenti che non è possibile utilizzare alcun supporto di memorizzazione di massa per usi diversi da quelli strettamente collegati all’attività aziendale |
| **Attività di backup e gestione in caso di disaster recovery** |
| **Principio di comportamento** |
| Al fine di garantire una adeguata gestione delle comunicazioni e dell’operatività per il corretto e sicuro funzionamento degli elaboratori di informazioni, la struttura è dotata di backup di informazioni e software |
| La struttura è dotata di backup di strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati |
| **Processo di gestione della cartella clinica e diagnosi** |
| **Gestione della cartella clinica e diagnosi** |
| **Dovere** |
| Deve essere condotta una attività di analisi e sviluppo dei modelli e contenuti per cartella clinica informatizzata, in collaborazione con il responsabile dell’area assistenziale; devono essere create scale di valutazione, di gestione della piattaforma e voci di database per quanto non presente nei moduli standard |
| **Processo di gestione delle pubblicazioni scientifiche** |
| **Gestione delle pubblicazioni scientifiche** |
| **Principio di comportamento** |
| Sono coinvolti professionisti qualificati del settore nella valutazione circa l’esistenza o meno dei requisiti che determinano le caratteristiche tipiche di “opera dell’ingegno” e/o di “opera altrui”. Almeno annualmente viene condotto un audit specifico sul tema |
| Viene definito un processo strutturato per l'attività di gestione delle pubblicazioni scientifiche, suddiviso per specifiche fasi rilevanti, per ognuna delle quali sia prevista la predisposizione di specifica documentazione, flussi informativi verso gli organi gerarchici superiori e l'autorizzazione degli stessi per il passaggio alla fase successiva |
| È implementato un sistema antiplagio, anche informatico, per la verifica dell'originalità delle ricerche prima della pubblicazione |
| Qualora siano identificati elementi tali da fare supporre una possibile violazione di proprietà industriale di terzi, vengono svolte analisi accurate, anche dando incarico a terzi specialisti e mantenendone traccia |

# PROCEDURE, PRASSI E ISTRUZIONI OPERATIVE DEI PROTOCOLLI SPECIALI

I principi di comportamento generali a presidio della fattispecie in esame, con quelli dei processi e delle aree individuate, trovano altresì dettaglio nelle seguenti procedure, prassi e istruzioni operative così codificate di cui, a titolo esemplificativo:

* *Regolamento aziendale per l’assunzione e il conferimento di incarichi libero professionali;*
* *Procedura determinazione fabbisogno di risorse umane e processo di selezione;*
* *Regolamento aziendale per l’assunzione e il conferimento di incarichi libero professionali;*
* *Regolamento Aziendale in materia di attività libero professionale del personale medico e delle professioni sanitarie operanti;*
* *Linee Guida per l’inserimento del personale sanitario non medico;*
* *Linee Guida per l’inserimento del personale amministrativo;*
* *Linee Guida per Inserimento personale sanitario medico;*
* *Procedura di gestione inserimento personale;*
* *Requisiti Profili Professionali;*
* *Regolamento per l’assegnazione e l’uso di apparecchiature di telefonia mobile;*
* *Procedura di gestione formazione del personale;*
* *Regolamento Cassa;*
* *Procedura per l’emissione e l’autorizzazione delle note di accredito;*
* *Procedura per la chiusura contabili;*
* *Struttura sistemi Informativi;*
* *Regolamento aziendale sull’utilizzo di strumenti elettronici nell’ambito del rapporto di lavoro;*
* *Regolamento su donazioni, acquisizioni in conto visione e in comodato;*
* *Prontuario farmaceutico;*
* *Piastra ambulatoriale;*
* *[…].*