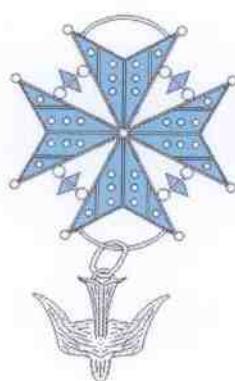


# **OSPEDALE EVANGELICO INTERNAZIONALE**

**Salita Sup. S. Rocchino, 31/A**

**GENOVA**



## **REGOLAMENTO AZIENDALE SULLA PRIVACY** di applicazione della normativa di cui al d. lgs. n. 196/03 e s.m.i.

**Ente Ecclesiastico Civilmente Riconosciuto**  
**Fondato nel 1857 da Chiese Evangeliche di Genova:**  
**Anglicana, Luterana, Presbiteriana Scozzese, Riformata Svizzera, Valdese**

## INDICE

▪	Introduzione	3
▪	Art.1 Oggetto e finalità	3
▪	Art.2 Definizioni	4
▪	Art.3 Titolare del trattamento dei dati personali	5
▪	Art.4 Responsabili del trattamento dei dati personali	5
▪	Art.5 Responsabile del trattamento dei dati personali del Sistema Informativo Aziendale	6
▪	Art.6 Incaricati del trattamento dei dati personali	6
▪	Art.7 Obblighi delle persone che operano all'interno dell'Ente	7
▪	Art.8 Attività formativa in materia di riservatezza dei dati	7
▪	Art.9 Referente per la Privacy	7
▪	Art.10 Amministratore di Sistema	8
▪	Art. 11 Documento Programmatico sulla Sicurezza	8
▪	Art. 12 Trattamento dei dati personali	8
▪	Art. 13 Trattamento dei dati personali da parte di soggetti esterni all'Ente	9
▪	Art. 14 Notificazioni e Comunicazioni al Garante	9
▪	Art. 15 Informazioni per la raccolta dei dati	9
▪	Art. 16 Consenso al trattamento dei dati	10
▪	Art. 17 Comunicazione e diffusione dei dati personali	10
▪	Art. 18 Comunicazione e notizie sullo stato di salute degli utenti	10
▪	Art. 19 Accesso alle liste di attesa	11
▪	Art. 20 Procedure organizzative a tutela della riservatezza in ambito sanitario	11
▪	Art. 21 Pubblicità degli atti e diritto alla riservatezza	11
▪	Art. 22 Esercizio dei diritti di cui all'articolo 7 del D. Lgs. n. 196/2003	11
▪	Art. 23 Diritto di accesso alla documentazione	12
▪	Art. 24 Misure di Sicurezza	12
▪	Art. 24.1 Criteri tecnici ed organizzativi per la protezione delle aree e dei locali	13
▪	Art. 24.2 Uso delle apparecchiature di video-sorveglianza	13
▪	Art. 24.3 Altre misure per il rispetto dei diritti degli interessati	13
▪	Art. 24.4 Istruzioni per il trattamento dei dati	13
▪	Art. 24.5 Istruzioni per il trattamento di dati sensibili e/o giudiziari	14
▪	Art. 24.6 Trattamenti senza l'ausilio di strumenti elettronici	14
▪	Art. 24.7 Archivi cartacei	14
▪	Art. 24.8 Custodia	14
▪	Art. 24.9 Selezione, scarto e distruzione	15
▪	Art. 24.10 Comunicazione	15
▪	Art. 24.11 Custodia delle stazioni di lavoro	15
▪	Art. 24.12 Credenziali delle stazioni di lavoro	15
▪	Art. 25 Procedura, criteri e modalità per il ripristino della disponibilità dei dati	16
▪	Art. 26 Procedura, istruzioni organizzative e tecniche per la custodia e l'uso dei supporti Rimovibili/distruzione supporti rimovibili	16
▪	Art. 27 Prevenzione dei virus informatici	16
▪	Art. 28 Politica di aggiornamento software	17
▪	Art. 29 Riferimenti normativi ed alle disposizioni aziendali e norme di rinvio	17

## Introduzione

Nel presentare questo Regolamento è bene chiarire che esso:

- Non è un'ulteriore normativa rispetto a quella nazionale;
- Non rappresenta una limitazione dell'autonomia gestionale dei singoli responsabili;

Il Regolamento aziendale sulla Privacy è uno strumento di applicazione del D. Lgs. 30 giugno 2003 n. 196 (c.d. Codice della Privacy da ora in avanti indicato come Codice) relativo alla tutela della riservatezza dei dati personali.

Tale decreto raccoglie le disposizioni già contenute nella legge n. 675/1996 e le successive modificazioni ed integrazioni emanate dalla sua pubblicazione fino al 2002. Il nuovo Codice della Privacy raccoglie 186 articoli, completati da diversi allegati tecnici e incorpora anche i precedenti regolamenti.

Un efficace rispetto delle regole in modo sostanziale e non solo formale che vengono dettate dalla normativa sulla Privacy prevede un impegno organizzativo all'interno di ogni struttura aziendale al fine di garantire il rispetto dei dati e della dignità della persona.

Questo è ancora più evidente se le regole sulla Privacy si applicano in una realtà particolare come quello di un Ente ospedaliero che utilizza e conserva dati molto delicati come quelli relativi alla salute della persona.

L'Ospedale Evangelico Internazionale ha cominciato a lavorare per il rispetto del diritto alla Privacy del cittadino e, attraverso l'elaborazione di un primo Regolamento aziendale, si è organizzato definendo le relazioni necessarie al suo interno per un corretto uso delle informazioni.

Tale Regolamento consente a tutti i dipendenti di prendere atto della necessità di un sistema aziendale che monitori e sviluppi la materia della Privacy.

Fondamentale a tal fine è anche la figura del Referente aziendale sulla Privacy che in questo Ente svolge la funzione di promuovere e garantire la riservatezza dei dati del cittadino e di raggiungere in maniera capillare tutti gli operatori aziendali anche attraverso la diffusione di lettere informative.

Altra figura introdotta dalla normativa è quella dell'Amministratore di Sistema.

Inoltre, per favorire il miglioramento della qualità del servizio offerto all'utenza, l'Ente si è attivato al fine di sensibilizzare tutti i Suoi operatori alla specifica problematica mediante appositi corsi di formazione.

Le istruzioni contenute nel presente Regolamento costituiscono una serie organica di prescrizioni, orientate a garantire la sicurezza dei dati e delle informazioni detenuti dagli uffici e dalle strutture dell'Ospedale Evangelico Internazionale. Tali prescrizioni devono intendersi come istruzioni impartite dal Titolare del trattamento ai sensi dell'art. 28 del d. lgs. n. 196/2003.

## Art. 1 Oggetto e finalità

Il presente Regolamento disciplina all'interno dell'Ente la tutela delle persone e degli altri soggetti in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali, emanato con D. lgs. n. 196/2003.

La normativa contenuta nel presente Regolamento è diretta a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche con particolare riferimento alla riservatezza e all'identità personale e al diritto della protezione dei dati personali degli utenti e di tutti coloro che hanno rapporti con l'Ente.

In ogni caso, il trattamento dei dati presso gli uffici e le strutture dell'Ente avviene:

- Nel rispetto del principio di riservatezza;
- Nel rispetto del principio di trasparenza;
- In modo lecito e secondo correttezza;
- Per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e, successivamente, trattati;
- Nel rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nello specifico si intende per:

- Tutela della riservatezza: l'attivazione di procedure di conoscenza delle informazioni detenute a qualsiasi titolo dall'Ente, tali da consentire l'accesso solo a soggetti identificati e dotati di un adeguato grado di autorizzazione;
- Integrità: l'aggiornamento dei dati e delle informazioni realizzato periodicamente da personale autorizzato;
- Disponibilità: l'attivazione di procedure che consentano ai soggetti autorizzati di accedere in tempi utili alle informazioni.

## Art. 2 Definizioni

Nel presente Regolamento e, comunque in sede di trattamento dei dati personali, l'Ente adotta le definizioni di cui all' art. 4 del Codice, secondo cui:

Si intende per:

- a) "*trattamento*", 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 di dati;
- b) "*dato personale*", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- c) "*dati identificativi*", i dati personali che permettono l'identificazione diretta dell'interessato;
- d) "*dati sensibili*", 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 lo stato di salute e la vita sessuale;
- e) "*dati giudiziari*", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- f) "*titolare*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- g) "*responsabile*", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- h) "*incaricati*", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- i) "*interessato*", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- l) "*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, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- m) "*diffusione*", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- n) "*dato anonimo*", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- o) "*blocco*", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- p) "*banca di dati*", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- q) "*Garante*", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Si intende, altresì, per:

- a) "*misure minime*", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- b) "*strumenti elettronici*", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- c) "*autenticazione informatica*", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- d) "*credenziali di autenticazione*", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- e) "*parola chiave*", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- f) "*profilo di autorizzazione*", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- g) "*sistema di autorizzazione*", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

