

PROCEDURA

PER IL CORRETTO TRATTAMENTO DI DATI

CON STRUMENTI INFORMATICI

INFORMAZIONI DOCUMENTO:

Titolo	Procedura per il corretto trattamento di dati con strumenti informatici		
Data di emissione	26/06/2025	Versione	1.0

INDICE

1. SCOPO, ENTRATA IN VIGORE E AMBITO DI APPLICAZIONE
 - Scopo della procedura
 - Entrata in vigore e pubblicità
 - Campo di applicazione
2. PROCEDURE DISCIPLINARI
3. COMUNICAZIONI IN FORMATO ELETTRONICO
 - Linee Guida per le comunicazioni su formato elettronico.
 - Comunicazioni in formato elettronico e responsabilità ai sensi di legge.
 - Contenuto o utilizzo inappropriato.
 - Divieto di uso personale dell'e-mail dell'Ordine.
 - Monitoraggio delle comunicazioni su formato elettronico.
 - Disattivazione account dell'Ordine.
4. UTILIZZO DELLE APPARECCHIATURE INFORMATICHE IN GENERALE
 - Sicurezza.
 - Password.
 - Uso personale.
 - Protezione delle apparecchiature.
 - Protezione antivirus.
 - Copyright.
 - Apparecchiature dell'Ordine.
 - Utilizzatori di dispositivi mobili.
 - Dispositivi di archiviazione dati removibili.
 - Furto, smarrimento, accesso non autorizzato.
5. UTILIZZO SOFTWARE
 - Verifiche software.
6. DIVIETO DI UTILIZZO DI STRUMENTI PERSONALI PER SCOPI LAVORATIVI (BYOD)
7. SOCIAL MEDIA
8. ATTIVITA' DI FORMAZIONE
9. CONTATTI E RIFERIMENTI

Sezione 1 – Scopo, entrata in vigore e ambito di applicazione

Scopo.

Lo scopo della presente Procedura è di assicurare che tutti i dipendenti e il personale esterno siano a conoscenza delle regole che l'Ordine applica relativamente a quanto segue:

- utilizzo della tecnologia e dei servizi informatici forniti dall'Ordine;
- utilizzo della comunicazione in formato elettronico, come l'e-mail;
- utilizzo di piattaforme di Social Media, come ad esempio LinkedIn, siano esse interne o esterne all'Ordine.

Entrata in vigore e pubblicità.

Il presente regolamento entrerà in vigore successivamente alla delibera di approvazione del Consiglio dell'Ordine. Con la sua entrata in vigore tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Copia del presente regolamento viene consegnata con la "lettera di nomina autorizzato".

Campo di applicazione.

Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e fornitori dell'Ordine a prescindere dal rapporto contrattuale con la stessa intrattenuto. Pertanto laddove la Procedura si riferisca ai dipendenti è sottinteso che si riferisce anche ai collaboratori e al personale esterno. La Vostra firma posta in calce alla "lettera di nomina autorizzato" indica che avete letto, compreso e accettato di attenervi alle regole ivi previste.

Sezione 2 – Procedure disciplinari

La Procedura sull'utilizzo della tecnologia e dei servizi informatici forniti dall'Ordine è stata implementata al fine di salvaguardare la reputazione dell'Ordine e dei suoi dipendenti, di tutelare la privacy di questi ultimi e dei terzi e di garantire un ambiente informatico fidato e sicuro a tutti gli utenti.

I dipendenti che si ritiene agiscano in violazione della Procedura potranno essere soggetti a procedure disciplinari, salve le responsabilità civili e penali previste dalla legislazione in vigore.

Sezione 3 – Comunicazioni in formato elettronico

Questa sezione della Procedura delinea le regole dell'Ordine in merito all'uso consentito delle comunicazioni in formato elettronico.

Le seguenti regole sono valide per tutte le comunicazioni in formato elettronico ivi comprese, a titolo esemplificativo e non esaustivo, quelle tramite e-mail, Instant Messaging e messaggistica di testo che sono:

- accessibili nella o dalla sede dell'Ordine;
- accessibili utilizzando le apparecchiature informatiche dell'Ordine o attraverso modalità di accesso offerte dall'Ordine;
- utilizzate in un modo tale da identificare l'individuo all'interno dell'Ordine.

Eventuali terzi quali Consiglieri, iscritti all'Ordine, visitatori o consulenti che siano autorizzati ad utilizzare la rete e i servizi informatici dell'Ordine sono tenuti a rispettare questa Procedura.

È responsabilità del dipendente, che ne autorizza l'uso da parte di terzi, assicurare che detti terzi rispettino la presente Procedura e che accettino i vincoli in essa contenuti.

Linee Guida per le comunicazioni su formato elettronico.

Una buona comunicazione implica parlare con iscritti, colleghi, fornitori e cittadini. Spesso, in questo modo, le questioni possono essere risolte più velocemente e con minor rischio di fraintendimento.

Tuttavia, laddove un'e-mail risulti essere la forma di comunicazione più idonea, sia internamente che esternamente all'Ordine, per esempio nel caso in cui venga richiesta della documentazione di supporto o una spiegazione, ci si dovrà attenere alle linee guida di seguito descritte.

Le comunicazioni via e-mail, in particolare, vengono spesso percepite come più vicine a un modo di scrivere informale piuttosto che formale.

Inoltre, le e-mail e l'instant messaging stanno diventando sempre più i mezzi principali di contatto tra l'Ordine e i propri iscritti, cittadini, fornitori, terzi in generale e, di conseguenza, questi hanno un impatto fondamentale sulla percezione dei servizi offerti dall'Ordine.

Al fine di ridurre il più possibile la possibilità di comunicazioni inopportune o offensive e di salvaguardare la reputazione dell'Ordine, si richiede di attenersi alle seguenti linee guida:

- l'uso inappropriato delle maiuscole nelle comunicazioni elettroniche viene generalmente interpretato come un GRIDO e dovrebbe essere evitato;
- il campo dell'oggetto nelle e-mail deve contenere una descrizione chiara del contenuto della e-mail stessa;
- le e-mail devono essere inviate solamente alle persone che necessitano effettivamente di vederle/riceverle;
- le comunicazioni elettroniche devono essere scritte in un tono adeguato e semplice, utilizzando il normale linguaggio che riflette gli standard comunicativi di solito adottati per la corrispondenza a mezzo lettera su carta intestata;
- i dipendenti non devono insultare altri anche in risposta ad insulti a loro diretti;
- se un dipendente dovesse ricevere un'e-mail o una comunicazione in formato elettronico per errore, lo stesso è tenuto a informare il mittente immediatamente e a cancellare il messaggio dalla propria casella di posta e dallo storico delle conversazioni;
- le e-mail devono contenere le necessarie informazioni per identificare Ordine, Ufficio, Mansioni;
- si raccomanda in ogni caso la massima attenzione nell'aprire e-mail o allegati di cui non conoscete la fonte dal computer aziendale in quanto potrebbero contenere virus che possono mettere a rischio la rete IT aziendale: per ridurre al minimo il rischio di virus, le e-mail di natura sospetta dovrebbero essere inoltrate all'Amministratore di sistema, senza aprire gli allegati.

Comunicazioni in formato elettronico e responsabilità ai sensi di legge.

I dipendenti dovrebbero essere a conoscenza che la responsabilità legale per le e-mail e per qualsiasi uso improprio di internet da parte di un dipendente ricade sull'Ordine e sul dipendente stesso.

Le comunicazioni in formato elettronico sono equivalenti alla scrittura di una lettera con intestazione dell'Ordine e, a scanso di equivoci, i dipendenti dovrebbero sapere che questo tipo di comunicazione può costituire e modificare, ad esempio, un contratto.

Pertanto, i dipendenti dovrebbero essere consapevoli che le comunicazioni elettroniche sono legalmente vincolanti per l'Ordine e dovrebbero porre la stessa cura e attenzione su questo tipo di corrispondenza (sia esterna che interna) di quella che porrebbero sulla corrispondenza formale fatta attraverso carta intestata dell'Ordine.

Nessun dipendente dovrebbe siglare alcun tipo di documento a nome dell'Ordine, a meno che e fino a quando tutte le necessarie procedure di autorizzazione non siano state rispettate.

Contenuto o utilizzo inappropriato.

L'elenco di seguito fornito è puramente indicativo e non esaustivo delle condotte che possono portare a procedimenti disciplinari.

Ordine dei Medici Chirurghi e Odontoiatri di Como

I dipendenti dovrebbero essere consapevoli del fatto che l'Ordine deve informare le autorità competenti se, per esempio, è stato commesso un illecito civile o penale o una violazione della normativa sulla protezione dei dati o se l'Ordine ritiene che ci sia la probabilità che un reato possa essere commesso.

I mezzi elettronici non possono essere utilizzati per trasmettere o archiviare intenzionalmente comunicazioni o informazioni che sono:

- di natura discriminatoria o molesta;
- dispregiative di un individuo o di un gruppo o che possono in altro modo screditare l'Ordine o i suoi dipendenti;
- oscene o censurate o che rischiano di far considerare l'Ordine come tale e, in particolare, alcun materiale pornografico deve essere ricevuto, archiviato o divulgato né internamente, né esternamente all'Ordine;
- di natura diffamatoria o intimidatoria;
- parte di una "catena di Sant'Antonio" o pubblicità non richiesta o messaggi di spam;
- dati personali di terzi che un dipendente, intenzionalmente o incautamente, rivela ad altri senza consenso.

Divieto di uso personale dell'e-mail dell'Ordine.

La rete e i servizi dell'Ordine vengono forniti per attività legate al lavoro e non è consentito l'utilizzo per finalità personali. Ogni messaggio e-mail in uscita dovrà contenere l'indicazione della natura non personale dello stesso e della possibilità che le risposte possano in astratto essere visionate dall'Ordine.

Monitoraggio delle comunicazioni su formato elettronico.

In caso di assenze programmate, se disponibile la funzionalità di risposta automatica, il dipendente è tenuto ad attivarla indicando nel messaggio automatico il periodo di assenza e i contatti di altro dipendente e/o indirizzo e-mail comune a cui indirizzare le comunicazioni urgenti. In caso di assenze non programmate, per esigenze tecniche e/o organizzative, la casella e-mail sarà resa accessibile da parte dell'Amministratore di sistema a personale autorizzato dal Direttore o dal Presidente dell'Ordine. In caso di anomalie rilevate quali, ad esempio, flussi anomali di scambio di dati (ad esempio scambi di dati in quantità molto superiore rispetto alla normale operatività dei sistemi che possano indicare il download dalla rete di file non autorizzati ovvero l'invio non autorizzato verso l'esterno di dati) ovvero rilevazione di malware o altro software che possa avere ripercussioni negative sulla rete ovvero di violazioni del diritto d'autore, l'Amministratore di sistema può effettuare dei controlli saltuari e non sistematici sulle informazioni elettroniche create, archiviate e/o scambiate da un dipendente nel rispetto della normativa vigente. I controlli avverranno secondo un principio di gradualità. Nello specifico verranno in prima battuta effettuati controlli in forma aggregata circoscrivendoli al reparto o segmento in cui si siano rilevate anomalie; all'esito verranno dati avvisi generalizzati agli utenti potenzialmente coinvolti in quanto operanti all'interno dell'area oggetto del controllo al fine di far cessare i comportamenti sospetti. Solo in caso di persistenza dell'anomalia riscontrata saranno possibili controlli mirati ed individuali. In tale evenienza l'Amministratore di sistema, previo ordine scritto del Presidente dell'Ordine o del Direttore, potrà accedere alle e-mail con proprie credenziali. A tutela dei lavoratori ed al fine di verificare che non vi siano accessi ingiustificati, gli accessi da parte dell'Amministratore di sistema sono registrati mediante file di log. Le comunicazioni che sono chiaramente di carattere personale (sebbene vietate dalla presente policy) non verranno aperte o rivelate.

Disattivazione account dell'Ordine.

In caso di cessazione del rapporto di lavoro in essere con l'Ordine, gli account attribuiti al dipendente cessato (se assegnati individualmente) verranno immediatamente disattivati e successivamente rimossi dopo 30 giorni dalla disattivazione. L'account verrà definitivamente cancellato decorsi i 30 giorni dalla disattivazione salvo che ricorrano obblighi legali di conservazione per un periodo più lungo. Il termine di 30 giorni di cui

Ordine dei Medici Chirurghi e Odontoiatri di Como

sopra costituisce pertanto anche il termine entro il quale il lavoratore cessato può esercitare i diritti riconosciutigli dalla normativa sulla protezione dei dati personali (Artt. 12 - 23 Reg. UE 2016/679).

Sezione 4 – Utilizzo delle apparecchiature informatiche in generale.

Oltre alle regole sopra specificate relative all'uso delle comunicazioni elettroniche, i dipendenti dovrebbero essere a conoscenza delle regole da seguire nell'utilizzo di qualsiasi servizio informatico fornito dall'Ordine. I dipendenti dovrebbero essere consapevoli che l'accesso non autorizzato o il tentativo di accesso a un sistema informatico di terzi costituisce reato e determina obblighi risarcitori sul piano civilistico.

Pertanto sono attività proibite:

- tentare di ottenere un accesso non autorizzato a:
 - a) qualsiasi area della rete o di intranet o di qualsiasi file ivi archiviato al quale non si ha l'autorità o il permesso di accedere e/o
 - b) a qualsiasi altra apparecchiatura informatica o servizio;
- il caricamento/scaricamento non autorizzato di file e/o la modifica o la rimozione di file su qualsiasi server della rete ad eccezione dei file creati dal dipendente che siano diventati obsoleti o che siano stati sostituiti da versioni più recenti;
- tutte quelle che possono disturbare l'uso designato del sistema informatico o delle risorse della rete;
- l'utilizzo o la riproduzione non autorizzati del software di proprietà o di materiale soggetto a copyright - diritti di autore - (si veda la sezione sull'utilizzo del software);
- l'upload o il download di software gratuiti se non autorizzati e strettamente attinenti;
- l'utilizzo di documenti provenienti da siti web se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a forum, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books non attinenti l'attività dell'Ordine e/o lavorativa se non espressamente autorizzati;
- accedere o tentare di accedere a siti web che:
 - o sono osceni/offensivi;
 - o contengono materiale di carattere razzista, sessuale, politico o altro materiale di istigazione all'odio che possa facilmente provocare delle offese;
 - o mostrano immagini pornografiche;
 - o contengono un linguaggio ingiurioso;
 - o per qualsiasi motivo sono illegali.

Sicurezza.

I dipendenti sono tenuti a rispettare la riservatezza delle informazioni archiviate nei sistemi dell'Ordine e l'integrità dell'intero ambiente informatico, garantendo che non faranno mai nulla che possa danneggiare o potenzialmente danneggiare l'integrità dei sistemi.

I dipendenti non devono:

- tentare di accedere a informazioni se non per fini lavorativi;
- "violare" i sistemi (accedervi senza autorizzazione) o i login di altre persone o "craccare" (decriptare) le password;
- violare o tentare di violare la presente Procedura;
- infrangere le misure di sicurezza del computer o della rete.

I dipendenti devono tener presente che i sistemi dell'Ordine contengono informazioni confidenziali e che terzi potrebbero tentare di contattarli per accedere a tali informazioni ("phishing"). I dipendenti devono porre molta attenzione quando rispondono al telefono o a e-mail e non devono divulgare informazioni a meno che non siano sicuri dell'affidabilità e della liceità di chi le riceve.

Password.

Nell'accettare le credenziali di accesso personale il dipendente, collaboratore e personale esterno accetta la responsabilità di esserne diligente custode. Nel caso in cui si ritenga che qualcuno possa conoscere o aver utilizzato la propria password, bisogna cambiarla immediatamente e informare l'Amministratore di sistema. Tutti gli utenti che si connettono alla rete dell'Ordine sono pregati di cambiare le loro password al primo utilizzo e, successivamente, secondo quanto impostato dall'Amministratore di sistema. L'Amministratore di sistema dispone di proprie credenziali per accedere ai computer come "amministratore" nel caso in cui ciò sia necessario per improrogabili esigenze (organizzative o di sicurezza) in caso di assenza del lavoratore ovvero nel caso in cui il lavoratore cessi il proprio rapporto di lavoro.

Uso Personale.

Non è consentito fare un uso personale dei computer (anche portatili), dei dispositivi e dei servizi informatici in genere.

Protezione delle apparecchiature.

Ricordiamo, inoltre, a tutti coloro che utilizzano computer, portatili e tablet, che sono tenuti a proteggere i loro sistemi, "bloccando" i loro desktop (con una password) quando si allontanano dalla scrivania e/o dal dispositivo. Questo vale indipendentemente dal tempo per il quale ci si assenta dalla propria postazione di lavoro (o ci si allontana dal dispositivo). All'uscita dall'ufficio, ogni giorno, i computer dovranno essere spenti e non lasciati in "stand-by" per tutta la notte.

Protezione antivirus.

Il sistema informatico è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto all'Amministratore di sistema.

Copyright (diritti di autore).

Tutti coloro che hanno ottenuto accesso elettronico a materiali di terzi devono rispettare i diritti d'autore e non possono copiare, scaricare, consultare, modificare o inoltrare materiale soggetto a copyright, a eccezione di quanto consentito dal possessore del copyright stesso.

Utilizzatori di dispositivi mobili.

Particolare attenzione dovrebbe essere prestata quando si è in possesso di un dispositivo mobile dell'Ordine. I dispositivi non dovrebbero essere lasciati incustoditi (ad esempio non abbandonati in automobile né altrove e dovrebbero essere tenuti sempre con sé quando si è in viaggio). I dati presenti nei dispositivi mobili sono una copia di quelli presenti sui server. Se vengono modificati nel dispositivo mobile poi questi dati devono essere riversati nuovamente sul server nelle cartelle appropriate.

Dispositivi di archiviazione dati rimovibili.

I dispositivi di archiviazione dati rimovibili come chiavette USB, hard disk esterni e CD sono mezzi di trasferimento e archiviazione di molti dati efficienti e usuali. I dipendenti non devono usare i dispositivi di archiviazione dati rimovibili per salvare informazioni dell'Ordine per proprio utilizzo o per eventuali profitti commerciali. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.),

Ordine dei Medici Chirurghi e Odontoiatri di Como

contenenti dati personali nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, smarrito, alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Si consiglia di utilizzare sistemi di crittografia. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun utente dovrà rivolgersi all'Amministratore di sistema e seguire le istruzioni da esso impartite. In ogni caso, i supporti magnetici o ottici contenenti dati personali devono essere adeguatamente custoditi dagli utenti in luogo idoneo. Il dipendente è responsabile della custodia dei suddetti supporti e, conseguentemente, dei dati in essi contenuti.

Furto, smarrimento, accesso non autorizzato.

In caso di smarrimento, furto, accesso non autorizzato a qualunque dispositivo assegnatogli il dipendente deve segnalare immediatamente il fatto (entro 2 ore da quando ne ha contezza) all'Amministratore di sistema, utilizzando i canali che seguono, per consentire l'adozione tempestiva delle contromisure previste dalla normativa e di minimizzare il danno. La informiamo che il ritardo (anche minimo) nella segnalazione può causare gravi danni.

Sezione 5 – Utilizzo di software.

È consentito l'utilizzo del software indicato nell'elenco dei software autorizzati. Non sono consentite installazioni di altro software o installazioni non eseguite dall'Amministratore di sistema.

Verifiche software.

Al fine di assicurare che l'Ordine sia in regola con tutte le concessioni di licenza d'uso software, l'Amministratore di sistema condurrà delle verifiche periodiche a campione sugli strumenti informatici che includono, ma non si limitano a, PC, portatili, tablet e telefoni. Le verifiche possono essere condotte in qualsiasi momento dall'Amministratore di sistema, senza darne informazione preventiva. I dipendenti devono assecondare tutte le richieste di informazioni e di accesso che verranno loro sottoposte nel corso di queste ispezioni. Le verifiche potranno essere condotte utilizzando un prodotto di verifica del software. I software per i quali non vi sono registrazioni di supporto, licenze d'uso e/o gli strumenti di installazione originali saranno rimossi dal dispositivo dell'utente senza necessità di comunicazione né preavviso.

Sezione 6 - Divieto di utilizzo di strumenti personali per scopi lavorativi (BYOD).

Per garantire l'integrità dei dati e la sicurezza del sistema informatico, l'utilizzo di apparecchiature elettroniche personali per scopi lavorativi non è permesso. Le apparecchiature elettroniche includono ma non si limitano a, computer PC, laptop, tablet e smartphones.

Sezione 7 - Social Media.

L'uso di siti web e di applicazioni Social Media si è estremamente diffuso nel corso degli ultimi anni. Questa forma di comunicazione elettronica può rappresentare un problema giacché:

- può potenzialmente essere istantaneamente e universalmente pubblicizzata e diffusa;
- può potenzialmente essere comunicata a un pubblico molto più vasto di quello che si sarebbe voluto;
- può essere irrevocabile.

L'Ordine non vuole in alcun modo imporre il suo punto di vista in merito all'utilizzo "appropriato" di queste forme di comunicazione a nessuno dei propri dipendenti ma il fatto è che laddove i dipendenti parlino di argomenti che riguardano la loro attività lavorativa o vengano identificati come rappresentanti dell'Ordine,

Ordine dei Medici Chirurghi e Odontoiatri di Como

è facile per chi legge Facebook o un tweet di Twitter o il profilo LinkedIn o un'e-mail, prendere quanto viene da noi detto come affermazione dell'Ordine.

Pertanto, riteniamo che, quale necessario segno di responsabilità, i dipendenti debbano attenersi a quanto indicato di seguito:

- i dipendenti devono comprendere che ciascuno è personalmente responsabile di quanto viene pubblicato on-line (che sia su Twitter, Facebook, LinkedIn o qualsiasi altro forum/social media);
- ciò che si pubblica sul web rimarrà pubblico per lungo tempo - dovrete proteggere la vostra privacy e la privacy e gli interessi dell'Ordine e dei vostri colleghi;
- non fornite informazioni confidenziali su altri o altre informazioni proprietarie dell'Ordine in nessuna dichiarazione;
- se vi siete identificati come dipendenti dell'Ordine, assicuratevi che il vostro profilo e i suoi contenuti siano in linea con le regole dell'Ordine.

Quando scrivete dei post, comunicate tramite Twitter o commentate argomenti relativi alla vostra attività lavorativa, dovete seguire le regole di cui sotto:

- affermazioni in cui si cita qualcun altro (anche in parafrasi), e senza uno specifico accordo scritto da parte di questi che ne verifichi la citazione e la pubblicazione, non sono accettabili;
- affermazioni atte a denigrare qualsiasi altro servizio, altre persone o terzi non sono accettabili;
- affermazioni immorali, volgari, oscene o in altro modo sgradevoli non sono accettabili;
- affermazioni che riportano informazioni sensibili non autorizzate non sono accettabili;
- senza specifica approvazione scritta da parte della Direzione non possono essere fatte affermazioni riguardanti, ma non limitate a: iscritti, dipendenti, politiche interne, cambiamenti, piani o progetti.

Sezione 8 - Attività di formazione.

L'Ordine predispone momenti formativi ed informativi per garantire a tutti i lavoratori incaricati il massimo aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati. Potrà comunque rivolgersi in qualsiasi momento al Titolare del trattamento per ogni chiarimento utilizzando i canali di cui al punto successivo.

Sezione 9 – Contatti e Riferimenti.

Eventuali domande relative alla Procedura dovranno essere indirizzate a all'Amministratore di sistema.

Ordine dei Medici Chirurghi e Odontoiatri di Como