



## FRONTESPIZIO DELIBERAZIONE

AOO: DA  
REGISTRO: Deliberazione  
NUMERO: 0000225  
DATA: 27/10/2017 10:29  
OGGETTO: Approvazione del documento "Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli"

### SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Cavalli Mario in qualità di Direttore Generale  
Con il parere favorevole di Landini Maria Paola - Direttore Scientifico  
Con il parere favorevole di Bianciardi Luca - Direttore Sanitario  
Con il parere favorevole di Cilione Giampiero - Direttore Amministrativo

Su proposta di Beatrice Cavallucci - ICT che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

### CLASSIFICAZIONI:

- [06-01]

### DESTINATARI:

- Collegio sindacale
- Servizio Unico Metropolitan Amministrazione del Personale (SUMAP)
- Direzione Scientifica
- Dipartimento Patologie Complesse
- Dipartimento Patologie Specialistiche
- Dipartimento Rizzoli - Sicilia
- Struttura di Supporto Direzionale
- Affari Legali e Generali
- ICT

### DOCUMENTI:

File	Hash
DELI0000225_2017_delibera_firmata.pdf	BAA4C89FB79C058015180682B9DB56935DB45550B6D7C02288E3CDE0FF63B78D
DELI0000225_2017_Allegato1:	8CBEBF925BDB0F1BFB62D5D8B6D3B11A2112B5A242DAF9D9CC9583F7834F813D



L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.  
Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.



## **DELIBERAZIONE**

**OGGETTO:** Approvazione del documento "Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli"

### **IL DIRETTORE GENERALE**

Premesso che:

E' opportuno definire una regolamentazione aziendale, con lo scopo di disciplinare l'utilizzo dei servizi informatici aziendali dell'Istituto Ortopedico Rizzoli, al fine di assicurare la funzionalità e il corretto impiego delle risorse stesse tenendo conto della disciplina in tema di diritti e relazioni sindacali, conformemente alle Linee Guida emesse dal Garante per la protezione dei dati personali.

Considerato che:

La previsione di regole di utilizzo delle risorse informatiche chiare e puntuali ha inoltre lo scopo di tutelare il lavoratore, consentendo al medesimo di organizzare la propria attività e gli strumenti del proprio lavoro secondo criteri idonei a garantire la sicurezza e la funzionalità degli strumenti stessi.

Visti i rischi connessi alla crescente diffusione delle nuove tecnologie e l'impiego sempre più frequente di queste ultime all'interno della realtà aziendale di IOR, che impongono di informare e istruire adeguatamente gli utenti (dipendenti e collaboratori dell'Istituto) circa l'utilizzo dei sistemi informatici aziendali, al fine di scongiurare il più possibile rischi di natura patrimoniale ed eventuali responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (tra cui, in particolare, il d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e la l. 22 aprile 1941, n. 633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio").

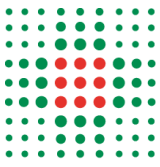
Tenuto conto che:

L'utilizzo delle risorse informatiche e telematiche deve ispirarsi al principio della diligenza e correttezza normalmente adottate nell'ambito dei rapporti di lavoro.

Dato atto pertanto:

Che si intende prevedere un regolamento avente ad oggetto, in particolare, le norme per l'accesso e l'utilizzo dei seguenti servizi: posta elettronica, rete di telecomunicazione (dati, voce, immagini), Internet e sistemi informativi aziendali, postazioni di lavoro aziendali fisse e mobili, firma digitale e carta nazionale dei servizi, attrezzature informatiche personali.

Precisato che:



Il percorso di informazione degli organi dell'Ente in ordine ai contenuti fondamentali del regolamento ha preso avvio in data 19 dicembre 2016 con la relazione al Collegio di Direzione della Dr.ssa Beatrice Cavallucci, Direttore della SC ICT (e successivo in data 22 maggio 2017) e si è concluso con l'intervento al CIV della Dr.ssa Beatrice Cavallucci, Direttore della SC ICT in data 19 luglio 2017, come da verbale pervenuto all'ufficio proponente.

Il contenuto del regolamento è stato inoltre oggetto di informativa e approfondimento con le OOSS di tutte le aree contrattuali ed RSU, contesto di una dialettica dipanatasi nel tempo ed in seguito alla quale si è pervenuti ad una formulazione definitiva che si va ad approvare.

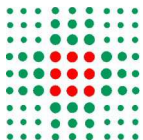
Nella formulazione definitiva che si va ad approvare, il regolamento è stato comunicato alle OO.SS. di tutte le aree in data 21 ottobre 2017 (come da mail dell'ufficio relazioni sindacali pervenuta all'ufficio proponente in data 21 ottobre 2017).

Considerato quindi che occorre adottare il testo del regolamento, così come risultato dopo i percorsi indicati;

### **Delibera**

1. Di approvare il documento denominato: Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli
2. Di precisare che modulistica e informativa allegati al regolamento potranno essere aggiornati nel tempo ad opera del Servizio ICT, con approvazione del responsabile del Servizio medesimo
3. Di demandare al Servizio ICT dell'Ente l'applicazione del medesimo e di diffonderlo alle strutture interessate.

Responsabile del procedimento ai sensi della L. 241/90:  
Beatrice Cavallucci



**SERVIZIO SANITARIO REGIONALE  
EMILIA - ROMAGNA**

Istituto Ortopedico Rizzoli di Bologna  
Istituto di Ricovero e Cura a Carattere Scientifico



**ICT**

# Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli

Ottobre 2017

**SC ICT**

Salita di San Benedetto, 1 - 40136 Bologna  
Tel. 051/6366302 - Fax 051/6366874  
ict@ior.it  
sistemi.informativi@pec.ior.it

**Istituto Ortopedico Rizzoli**

**Sede legale** Via Di Barbiano, 1/10 - 40136 Bologna  
**Ospedale** Via G. C. Pupilli, 1 - 40136 Bologna  
**Centro di Ricerca** Via Di Barbiano, 1/10 - 40136 Bologna  
Tel. 051/6366111 - Fax 051/580453 [www.ior.it](http://www.ior.it)  
Codice Fiscale e Partita IVA 00302030374

## *Indice*

Premessa .....	3
1. Entrata in vigore del regolamento .....	4
2. Oggetto e campo di applicazione del regolamento .....	4
3. Definizioni .....	5
4. Assegnazione e gestione delle credenziali di autenticazione .....	7
5. Richiesta di abilitazione ai servizi informatici .....	8
6. Utilizzo e gestione della postazione di lavoro .....	9
7. Navigazione in Internet .....	10
8. Utilizzo della rete wireless di IOR .....	11
9. Utilizzo e conservazione dei supporti rimovibili .....	11
10. Qualificazione della casella di posta elettronica .....	12
11. Gestione della casella di posta elettronica in caso di assenza del lavoratore .....	13
12. Accesso alla configurazione della casella di posta elettronica per ragioni di sicurezza o manutenzione .....	13
13. Modalità di prestazione del servizio di assistenza .....	15
14. Backup e archiviazione .....	16
15. Sistemi di controlli gradualmente .....	16
16. Osservanza delle disposizioni in materia di protezione dei dati personali .....	17
17. Cessazione della disponibilità dei servizi informatici aziendali e sanzioni .....	18
18. Aggiornamento e revisione del regolamento .....	18

## *Documenti collegati*

Informativa agli utenti che utilizzano i servizi informatici IOR;

ICT IOR 1 Richiesta di abilitazione ai servizi informatici;

ICT IOR 2 Richiesta di abilitazione ai servizi informatici IOR e alla teleassistenza per utenti esterni;

ICT IOR 3 Istruzioni per il primo accesso e per l'attivazione della casella di posta elettronica;

ICT IOR 4 Testo a piè di pagina di messaggi email;

ICT IOR 5 Consegna e custodia postazione mobile.

### *Premessa*

Il presente regolamento ha lo scopo di disciplinare l'utilizzo dei servizi informatici aziendali dell'Istituto Ortopedico Rizzoli (nel prosieguo, per brevità, "IOR"), come definiti al successivo paragrafo 3, 1° comma, lett. a), al fine di assicurare la funzionalità e il corretto impiego delle risorse stesse tenendo conto della disciplina in tema di diritti e relazioni sindacali, conformemente alle Linee Guida emesse dal Garante per la protezione dei dati personali.

La previsione di regole di utilizzo delle risorse informatiche chiare e puntuali ha inoltre lo scopo di tutelare il lavoratore, consentendo al medesimo di organizzare la propria attività e gli strumenti del proprio lavoro secondo criteri idonei a garantire la sicurezza e la funzionalità degli strumenti stessi.

I rischi connessi alla crescente diffusione delle nuove tecnologie e l'impiego sempre più frequente di queste ultime all'interno della realtà aziendale di IOR, impongono di informare e istruire adeguatamente gli utenti (dipendenti e collaboratori dell'Istituto) circa l'utilizzo dei sistemi informatici aziendali, al fine di scongiurare il più possibile rischi di natura patrimoniale ed eventuali responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (tra cui, in particolare, il d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e la l. 22 aprile 1941, n. 633 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio").

L'utilizzo delle risorse informatiche e telematiche deve ispirarsi al principio della diligenza e correttezza normalmente adottate nell'ambito dei rapporti di lavoro.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del d.lgs. 30 giugno 2003, n. 196 (nel prosieguo, per brevità, "Codice privacy") e del disciplinare tecnico di cui all'Allegato B del citato decreto legislativo, contenente le misure minime di sicurezza.

## 1. *Entrata in vigore del regolamento*

A partire dall'entrata in vigore del presente regolamento, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

## 2. *Oggetto e campo di applicazione del regolamento*

Il presente regolamento ha ad oggetto, in particolare, le norme per l'accesso e l'utilizzo dei seguenti servizi:

- a) posta elettronica
- b) rete di telecomunicazione (dati, voce, immagini)
- c) Internet
- d) sistemi informativi aziendali
- e) postazioni di lavoro aziendali fisse e mobili
- f) firma digitale e carta nazionale dei servizi
- g) attrezzature informatiche personali

di seguito indicati nel loro complesso come "servizi informatici".

Non costituiscono invece oggetto del presente regolamento i sistemi informativi strettamente collegati alle tecnologie sanitarie quali, a titolo esemplificativo e non esaustivo, i sistemi PACS ed i sistemi di elaborazione delle immagini ad esso relativi.

Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori (anche temporanei, interni o esterni) dell'azienda. Si applica altresì ai fornitori e ai terzi espressamente autorizzati a compiere operazioni di trattamento per conto dell'Istituto e costituisce parte integrante del relativo contratto.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente, collaboratore e ogni soggetto autorizzato comunque operante presso IOR, il quale, in qualità di incaricato del trattamento dei dati personali, deve attenersi alle istruzioni impartite con l'atto di designazione a incaricato, nonché alle istruzioni di seguito specificate.

### 3. Definizioni

Ai fini di una corretta comprensione delle disposizioni del regolamento, si ritiene opportuno indicare le seguenti definizioni:

- a) “servizi informatici aziendali”: posta elettronica, rete Internet, sistemi informativi aziendali e postazioni di lavoro aziendali fisse e mobili di proprietà dello IOR collegate alla rete dati aziendale cablata e *wireless*, fatto salvo quanto precisato sopra;
- b) “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;
- c) “dato personale”: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- 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) “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;
- f) “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;
- g) “incaricati”: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- h) “interessato”: la persona fisica cui si riferiscono i dati personali;
- i) “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;



- j) “parola chiave” (*password*): 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;
- k) “firma digitale”: un particolare tipo di firma elettronica qualificata, basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
- l) “CNS”: carta nazionale dei servizi;
- m) “LDAP” (*Lightweight Directory Access Protocol*): servizio per la gestione centralizzata delle credenziali di accesso degli utenti dei servizi informatici aziendali;
- n) “Babel”: sistema di gestione documentale di protocollo, determinazioni e deliberazioni dello IOR;
- o) “sistema applicativo dipartimentale verticale”: sistema applicativo contenente le sole informazioni relative all’episodio per il quale l’interessato si è rivolto presso quella struttura e alle altre informazioni relative alle eventuali prestazioni sanitarie erogate in passato a quel soggetto da quel reparto/ambulatorio;
- p) “Istituto”, “IOR”: Istituto Ortopedico Rizzoli;
- q) “SC”: Struttura Complessa;
- r) “SSD”: Struttura Semplice Dipartimentale;
- s) “PEC” (posta elettronica certificata): sistema di comunicazione in grado di attestare l’invio e l’avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;
- t) *file* “log”: *file* generato automaticamente da un sistema software, che registra alcune operazioni che avvengono in fase di avvio o di esecuzione. Le informazioni registrate nella navigazione in Internet sono: data e ora, utente, indirizzo IP del PC o dispositivo, indirizzo di destinazione;
- u) “utente”: ogni dipendente, collaboratore e ogni soggetto autorizzato comunque operante presso IOR, il quale, anche in qualità di incaricato del trattamento dei dati personali, deve attenersi alle istruzioni impartite con l’atto di designazione a incaricato, nonché alle istruzioni contenute nel presente regolamento.

#### 4. *Assegnazione e gestione delle credenziali di autenticazione*

L'accesso e l'utilizzo dei servizi informatici aziendali sono subordinati al possesso da parte degli utenti di credenziali di autenticazione, che vengono assegnate d'ufficio dal personale della struttura ICT nel momento dell'inserimento del nuovo utente nel sistema gestionale delle risorse umane.

Attraverso il modulo ICT IOR 3 il nuovo utente riceve le "Istruzioni per il primo accesso e per l'attivazione della casella di posta elettronica", le proprie credenziali di autenticazione che consistono in un codice per l'identificazione dell'utente (*user id*) associato ad una parola chiave segreta (*password*) ovvero in un dispositivo di firma digitale associato ad una chiave segreta (*pin*), il quale rimarrà in possesso ed uso esclusivo dell'utente<sup>1</sup>.

La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri, non deve essere banale e non deve contenere riferimenti agevolmente riconducibili all'utente.

È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo e, successivamente, almeno ogni tre mesi. La parola chiave dovrà essere altresì modificata, d'intesa con la struttura ICT, ove si abbia ragione di ritenere la sua diffusione non autorizzata.

Le credenziali di autenticazione, in qualunque forma assegnate, dovranno essere custodite dall'utente con la massima diligenza e riservatezza e non dovranno essere divulgate né cedute, neppure temporaneamente, a terzi. Al fine di evitarne usi illeciti, le credenziali non devono essere memorizzate all'interno degli applicativi.

Si presume che qualsiasi azione svolta utilizzando le credenziali di autenticazione sia riferibile e imputabile all'utente titolare di tali credenziali.

L'utente si impegna a comunicare immediatamente alla struttura ICT l'eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi della *password*, del dispositivo di firma digitale o della carta nazionale dei servizi. In quest'ultimo caso dovrà essere presentata denuncia all'Autorità giudiziaria e dovrà essere seguita la procedura dell'ente certificatore.

Nel caso in cui l'utente perda la qualità che gli consentiva di accedere ai servizi informatici aziendali (ad esempio, alla scadenza del contratto di lavoro o di collaborazione con lo IOR), le credenziali di autenticazione devono essere disattivate dalla struttura ICT con

---

<sup>1</sup> In questo caso si tratta della carta nazionale dei servizi.

effetto immediato. In tal caso, l'utente può richiedere per iscritto, attraverso il Responsabile dell'unità organizzativa di riferimento, che la struttura ICT attivi un messaggio di risposta automatico dalla casella di posta elettronica aziendale e inoltri i messaggi verso un altro indirizzo di posta elettronica interno o esterno, per un periodo massimo di tre mesi. I messaggi di posta elettronica in giacenza vengono eliminati completamente trascorsi sei mesi dalla scadenza o dall'interruzione del rapporto contrattuale o di collaborazione tra l'utente e IOR.

#### 5. *Richiesta di abilitazione ai servizi informatici*

Gli utenti possono richiedere l'abilitazione ai servizi informatici<sup>2</sup> attraverso il modulo ICT IOR 1 "Richiesta di abilitazione ai servizi informatici aziendali". La richiesta di abilitazione di un utente deve essere motivata, e il modulo di richiesta deve recare una sezione in cui sia esplicitata la ragione specifica dell'abilitazione (ad esempio rapporto di lavoro o di collaborazione con IOR, indicando i riferimenti dell'autorizzazione all'accesso e all'uso dei sistemi informatici).

Nel modulo deve essere prevista anche l'indicazione della durata del rapporto di lavoro o di collaborazione.

Una volta che l'utente ha debitamente compilato il modulo, questo dovrà essere firmato sia dal Responsabile della struttura organizzativa a cui l'utente appartiene sia dal Responsabile del servizio per l'accesso al quale si chiede l'abilitazione (se la fornitura del servizio richiesto non è di competenza del Responsabile dell'unità organizzativa cui appartiene l'utente). L'utente dovrà quindi consegnare, previa scansione, il modulo firmato, via *e-mail*, alla struttura ICT che dovrà compilare la parte di sua competenza e procedere all'abilitazione. Qualora la richiesta abbia ad oggetto il servizio PEC, il Responsabile organizzativo è individuato nella SSD Affari Legali e Generali che dovrà procedere in collaborazione con la struttura ICT.

Tra gli utenti<sup>3</sup> che possono richiedere l'abilitazione e l'accesso ai servizi informatici di IOR rientrano i medici frequentatori volontari e/o dipendenti di altro ente che operano presso

---

<sup>2</sup> La richiesta deve essere effettuata per quei servizi informatici ai quali l'utente non può accedere solo in virtù delle credenziali già in proprio possesso, ma che necessitano di un'apposita abilitazione. Il servizio di posta elettronica è pertanto escluso da tale richiesta.

<sup>3</sup> Si rinvia alla definizione di utente contenuta al precedente paragrafo 3, 1° comma, lett. u).

IOR per motivi di ricerca e/o studio, i quali possono richiedere l'abilitazione ai sistemi e ai servizi impiegando il modulo ICT IOR 1.

I fornitori o i terzi autorizzati devono invece impiegare il modulo ICT IOR 2 "Richiesta di abilitazione ai servizi informatici aziendali e alla teleassistenza per utenti esterni" per l'accesso ai sistemi e alla teleassistenza.

Infine, nel caso di incaricati dell'Università di Bologna, le abilitazioni ai sistemi applicativi dipartimentali verticali dell'area sanitaria, della ricerca e dell'amministrazione sono assegnate e revocate d'ufficio in base al piano formativo fornito dall'Università e in base all'oggetto dell'assegno, della ricerca o della convenzione di cui si è titolari.

## 6. *Utilizzo e gestione della postazione di lavoro*

L'utente è tenuto ad essere diligente nello svolgimento della propria attività lavorativa e nell'utilizzo dei servizi informatici aziendali.

Elemento essenziale della postazione è il *personal computer* che viene affidato all'utente e il cui utilizzo deve essere pertinente all'attività lavorativa, al fine di scongiurare eventuali rischi connessi a disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Il *personal computer* affidato all'utente permette l'accesso ai servizi e ai sistemi applicativi di IOR solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 8 del presente regolamento.

All'accensione di ogni singola postazione viene eseguito in automatico un inventario dell'*hardware* e del *software* presenti sui *personal computer*, il cui elenco è disponibile presso la struttura ICT.

Solo il personale della struttura ICT è abilitato ad eseguire aggiornamenti e installazioni di *software* sulle postazioni di lavoro tramite la rete aziendale. Non è consentito l'uso di programmi diversi da quelli installati dal personale ICT, né è consentito agli utenti installare autonomamente programmi provenienti da fonti esterne, poiché sussiste il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni *software* esistenti. Al fine di installare programmi informatici ulteriori, l'utente dovrà formulare specifica richiesta alla struttura ICT, che provvederà a valutarne la conformità agli standard aziendali ed eventualmente a consegnarli al richiedente.

L'utente non deve lasciare incustodita la propria postazione e deve effettuare il *logout* dalla sessione di lavoro qualora si debba allontanare dalla postazione. Il *personal computer* deve poi essere configurato in modo che, in caso di inattività, vada

automaticamente in sospensione (*stand-by*) dopo un periodo di tempo pari a quindici minuti. Inoltre, il *personal computer* deve essere spento prima di lasciare gli uffici.

Qualora all'utente venga assegnata una postazione mobile (ad esempio, *computer portatile*), l'utente si impegna a custodire con diligenza il relativo *device*, sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, e a mantenerne l'efficienza per il corretto utilizzo (ad esempio, ricarica della batteria), previa sottoscrizione del modulo ICT IOR 5 "Consegna e custodia postazione mobile".

Le regole di utilizzo previste dal presente regolamento si applicano anche alle postazioni mobili.

## 7. *Navigazione in Internet*

Il *personal computer* assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, nonché comportamenti non tollerati rispetto alla navigazione in Internet (ad esempio, il *download* di *software* o di *file* musicali), IOR adotta limitazioni d'uso automatiche (introdotte per mezzo di filtri sui contenuti) e specifiche politiche di sicurezza aziendale anche su indicazione della rete GARR.

Qualora le misure tecniche preventive non fossero sufficienti e su richiesta dell'*Internet Provider* di IOR, l'amministratore di sistema specificamente autorizzato per iscritto, anche con delega generale, può effettuare, in conformità alla legge e alle Linee Guida emesse dal Garante per la protezione dei dati personali, verifiche puntuali a posteriori sulle attività di navigazione degli utenti, per finalità di sicurezza e di manutenzione.

Ogni altro controllo o intervento da parte del datore di lavoro sulla navigazione in Internet potrà avvenire esclusivamente in conformità alle finalità e ai limiti previsti dalla legge, dalla giurisprudenza o dall'Autorità Garante per la protezione dei dati personali.

Il controllo sui *file* di log non è continuativo ed i *file* stessi vengono conservati non oltre sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

È vietato l'utilizzo di accessi Internet mediante *Internet Provider* diversi da quello scelto ufficialmente dallo IOR e la connessione di stazioni di lavoro aziendali alle reti di detti *Provider*, anche con abbonamenti privati.

## 8. *Utilizzo della rete wireless di IOR*

Ai fini dell'accesso alla rete *wireless* di IOR, ogni *device* mobile aziendale deve essere dotato di un certificato di autenticazione installato dal personale tecnico ICT; per i *device* personali ciascun utente deve essere in possesso della specifica credenziale di autenticazione assegnata dallo IOR via SMS, previa presentazione del modulo di richiesta ICT IOR 1 citato.

Il collegamento di dispositivi mobili personali dei dipendenti o collaboratori (ad esempio *laptop, tablet, smartphone*) è consentito solo in relazione alla rete *wireless* denominata "IOR" per i soli servizi Internet (ad es. posta elettronica via *web* e navigazione) ed esclusivamente per lo svolgimento di attività istituzionali.

Accedendo alla rete *wireless* "IOR" mediante le credenziali di autenticazione, l'utente si assicura che il dispositivo personale è regolarmente aggiornato dal punto di vista della sicurezza (ad es.: antivirus, *firewall* del sistema operativo) e solleva lo IOR da ogni responsabilità per qualsiasi evento subito in proprio o arrecato a terzi durante o a seguito dell'utilizzo del collegamento Internet a mezzo dell'accesso messo a disposizione. L'utente si assume in generale ogni responsabilità derivante dall'uso del servizio di navigazione in Internet tramite la rete *wireless* "IOR".

L'utente è informato che, utilizzando reti pubbliche quali la rete *wireless* "IOR" e la rete Internet, il traffico generato durante il loro utilizzo non è riservato e potrebbe essere oggetto di intercettazione.

Le credenziali di accesso alla rete *wireless* "IOR" sono revocate in automatico alla scadenza del contratto o della collaborazione; possono essere altresì revocate in qualsiasi momento in caso di anomalie rilevate attraverso i *report* di sicurezza di IOR e le segnalazioni dell'*Internet Provider*.

## 9. *Utilizzo e conservazione dei supporti rimovibili*

L'Istituto non fornisce di regola i supporti rimovibili (chiavi USB, masterizzatori e *hard disk* rimovibili) ma consente il loro impiego per la gestione di documenti quali presentazioni, elaborazioni statistiche o documentazione di progetti e procedure.

Ogni dispositivo rimovibile dovrà essere verificato mediante il programma antivirus prima del suo utilizzo, e nel caso siano rilevati uno o più *file* infetti dovrà darsi immediato avviso alla struttura ICT.

Qualora l'utente sia autorizzato al salvataggio o alla memorizzazione di informazioni di IOR ovvero di dati trattati da quest'ultimo su supporti rimovibili, i dispositivi utilizzati per la memorizzazione devono essere conservati e custoditi dall'utente con la massima diligenza in modo che non siano lasciati incustoditi o facilmente accessibili. L'utente risponde della perdita e/o del trattamento posto in essere da soggetti non autorizzati di informazioni o di dati di IOR salvati sui predetti dispositivi, e in generale di eventuali danni derivanti dall'utilizzo di supporti rimovibili.

L'utente si impegna a comunicare immediatamente al proprio Responsabile e a denunciare all'Autorità giudiziaria l'eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi dei supporti rimovibili. Copia della denuncia deve essere inviata alla struttura ICT.

#### 10. *Qualificazione della casella di posta elettronica*

La casella di posta elettronica assegnata all'utente è espressione dell'organizzazione datoriale e costituisce uno strumento di lavoro teso a favorire sia una forma di comunicazione agile, di carattere informale ed operativo, sia la comunicazione ufficiale di documenti per via telematica in sostituzione quanto più possibile della comunicazione formale cartacea.

È vietato utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. Pertanto, in linea con le raccomandazioni contenute nelle Linee Guida del Garante per la protezione dei dati personali, non può crearsi un'aspettativa di confidenzialità del contenuto, in capo all'utente o ai terzi, rispetto a tale forma di comunicazione, che potrà essere inoltrata e/o utilizzata per motivi attinenti all'attività lavorativa.

Al fine di rendere edotti i destinatari della natura esclusivamente aziendale della casella di posta elettronica, conformemente alle Linee Guida emesse dal Garante per la protezione dei dati personali, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi. A tal fine, nei messaggi di posta elettronica inviati a destinatari esterni il sistema inserirà in automatico il testo riportato nel modulo ICT IOR 4 "Testo a piè di pagina di messaggi e-mail".

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. La casella di posta deve essere mantenuta in ordine, cancellando

documenti inutili e soprattutto allegati ingombranti. Con i messaggi di posta elettronica si possono inviare file allegati di dimensione massima di 10 MB.

#### 11. *Gestione della casella di posta elettronica in caso di assenza del lavoratore*

In caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella), si raccomanda all'utente di attivare l'opzione di invio automatico di un messaggio di risposta contenente l'indicazione di un altro indirizzo di posta elettronica di IOR cui fare riferimento o al quale il messaggio sarà automaticamente inoltrato, indicando eventualmente altre utili modalità di contatto della struttura. La funzionalità di inoltro deve essere attivata dal personale ICT su richiesta dell'utente, esclusivamente su indirizzi di posta elettronica di IOR.

In caso di assenza non programmata (ad esempio, per malattia), la procedura di risposta automatica oppure di inoltro - qualora non sia attivata dall'utente, anche avvalendosi del servizio *webmail* - potrà essere attivata a cura della struttura ICT su richiesta dell'utente stesso.

In caso di assenza improvvisa o prolungata, di impedimento dell'utente di attivare la funzionalità di cui sopra ovvero in caso di improrogabili necessità legate all'attività lavorativa, l'utente, conformemente alle Linee Guida emesse dal Garante per la protezione dei dati personali, ha facoltà di delegare un altro utente (fiduciario) ai fini dell'inoltro e della verifica del contenuto dei messaggi, anche al fine di trasmettere al Responsabile della struttura organizzativa di appartenenza dell'utente assente quei messaggi ritenuti rilevanti per lo svolgimento dell'attività stessa, fermi restando la riservatezza e l'utilizzo strettamente personale delle credenziali di ciascuno, come precisato in precedenza. La delega di cui al periodo che precede dovrà essere esercitata per iscritto, senza particolari formalità, anche via *e-mail*. Il Responsabile di riferimento del delegante deve essere immediatamente notiziato dell'esistenza della delega.

#### 12. *Accesso alla configurazione della casella di posta elettronica per ragioni di sicurezza o manutenzione*

Quando motivi di sicurezza o di manutenzione lo richiedono, l'amministratore di sistema specificamente autorizzato per iscritto, anche con delega generale, previo avviso agli utenti interessati e anche in assenza di questi, può accedere alla configurazione delle



caselle di posta elettronica per le sole finalità di sicurezza e manutenzione, per esclusive finalità tecniche. L'accesso alla configurazione di posta non comporta la visualizzazione dei messaggi della casella, salvo il caso eccezionale in cui il problema di sicurezza o di manutenzione non possa essere risolto. In quest'ultimo caso, l'avviso all'interessato deve essere rinnovato prima dell'accesso ai messaggi contenuti nella casella, fermo restando che l'accesso dell'amministratore di sistema può avvenire esclusivamente per motivi di sicurezza o manutenzione come sopra precisato.

L'attività effettivamente eseguita sulle configurazioni (o sui messaggi di posta, nel caso eccezionale di cui al periodo che precede), deve essere in ogni caso comunicata all'utente interessato senza ingiustificato ritardo al termine dell'intervento.

La struttura ICT dovrà annotare, anche in modalità telematica, gli interventi svolti, specificando i motivi, la data e l'orario dell'intervento, dando atto degli avvisi intervenuti nei confronti del soggetto o dei soggetti interessati.

Conformemente alla struttura organizzativa aziendale e a lato delle caselle nominative personali, sono create caselle di posta elettronica di gruppo condivise da più dipendenti della medesima struttura, il cui accesso avverrà mediante l'utilizzo di credenziali personali di accesso, secondo quanto indicato dal relativo Responsabile mediante una lista di distribuzione dei messaggi a ciascuna casella nominativa personale. Una lista non può riferirsi a gruppi con più di 50 elementi.

L'invio di *e-mail* che abbiano destinatari gruppi o categorie di persone è consentito se effettuato dalle direzioni, da amministratori o dirigenti, oppure se autorizzato dai medesimi o dalle relative segreterie, nei limiti di cui al successivo periodo.

Ad eccezione delle comunicazioni provenienti dalla Direzione Generale e dalle strutture che utilizzano i servizi messi a disposizione dal sistema di gestione del protocollo informatico (Babel), è consentito l'invio di messaggi ad un massimo di 50 indirizzi di *e-mail*.

L'invio massivo di comunicazioni a tutti gli utenti dello IOR o ad altre liste di distribuzione aziendali può essere effettuato esclusivamente dal personale autorizzato dalla Direzione Generale, dalla Direzione Sanitaria, dalla Direzione Amministrativa e dalla Direzione Scientifica, per mezzo del sistema *software* per la gestione delle *mailing list* aziendali.

È vietato l'utilizzo di tecniche di "mail spamming" attraverso il *server* di posta aziendale: controlli in tal senso sono applicati sui *server* aziendali e sui dispositivi di protezione perimetrale della rete.

Non sono previste caselle di posta anonime e non sono previste *password* condivise per l'accesso alla posta.

### 13. *Modalità di prestazione del servizio di assistenza*

L'Istituto si impegna a fornire continuità ai servizi informatici attraverso l'attività della struttura ICT che, per finalità di assistenza tecnica, manutenzione e normale attività operativa, è autorizzata a collegarsi alle postazioni di lavoro tramite sistemi *software* di manutenzione remota, per mezzo dei quali può prendere via rete il controllo del *personal computer* ed operare come se fosse in loco.

L'intervento viene effettuato su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, ove possibile e sempre che non si pregiudichi la tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento e/o dell'interruzione ai servizi informatici.

I riferimenti della postazione di lavoro e l'indicazione dell'utente che la sta in quel momento utilizzando sono di norma visibili sul *monitor*. L'utente può verificare l'attività effettuata rimanendo presso la postazione; inoltre, alla fine dell'intervento, il tecnico, su richiesta dell'utente o se ritenuto necessario per il buon esito dell'intervento, può lasciare visibile sul *desktop* del *personal computer* un messaggio descrittivo dell'attività effettuata con identificativo del tecnico stesso.

Solo nel caso di mancata soluzione del problema in modalità remota, viene effettuato un intervento in loco.

Gli interventi di manutenzione sono eseguiti da personale tecnico identificato ed autorizzato dalla struttura ICT. I tecnici afferiscono direttamente o tramite contratti di fornitura di servizi alla struttura ICT oppure ad altre articolazioni aziendali o di Area Vasta Emilia Centro, con funzioni di supporto agli utenti per l'utilizzo di specifici sistemi *software* gestionali.

Nel primo caso l'elenco degli interventi effettuati sulle postazioni (numero di inventario, data e durata dell'intervento) con indicazione di chi ha eseguito l'intervento è disponibile presso la struttura ICT. Per migliorare la qualità o la sicurezza dei servizi e dei sistemi informatici attualmente predisposti, l'Istituto valuterà con attenzione eventuali osservazioni, suggerimenti ed indicazioni che gli utenti faranno pervenire via *e-mail* all'indirizzo [gradimento.assistenzainformatica@ior.it](mailto:gradimento.assistenzainformatica@ior.it).

#### 14. *Backup e archiviazione*

La struttura ICT provvede al salvataggio dei dati registrati tramite i sistemi informativi aziendali.

I documenti elaborati tramite strumenti di *office automation* e in generale tutti i documenti, *file* ed immagini che contengono dati personali e/o sensibili, devono essere ospitati sui *server* centrali e resi fruibili agli utenti autorizzati tramite meccanismi di condivisione anche di gruppo, con accessi basati su *user id* e *password* personali. È vietata la condivisione diretta fra *personal computer* di cartelle che contengano dati personali e/o sensibili.

Su queste unità non possono in alcun modo essere conservati *file* che non siano legati all'attività lavorativa, nemmeno per brevi periodi. Per tale ragione il personale della struttura ICT può in qualunque momento procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericolosi per la sicurezza sia sui *personal computer* degli utenti sia sulle unità di rete.

È fatto obbligo agli utenti di effettuare il salvataggio dei dati memorizzati sul *computer* aziendale utilizzato, con frequenza almeno settimanale. La struttura ICT a questo scopo fornisce l'infrastruttura *hardware* centralizzata per il salvataggio di tali dati. L'attivazione della cartella per l'archiviazione sui *server* centrali è conseguente alla compilazione e sottoscrizione del modulo ICT IOR 1.

Risulta opportuno infine che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei *file* obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

#### 15. *Sistemi di controlli gradual*

Oltre a quanto previsto nelle disposizioni precedenti del presente regolamento, il personale incaricato della struttura ICT effettuerà controlli anonimi, tramite l'analisi aggregata del traffico di rete riferito all'intera struttura lavorativa o a sue aree (reparto, servizio, ecc.) e la rilevazione della tipologia di utilizzo (*e-mail*, *file* audio e video, *file* archiviati su *server* centrale, ecc.). Deve, infatti, per quanto possibile, essere preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Ove sia rilevata un'anomalia o una situazione di rischio, la struttura ICT può inviare via *e-mail* un avviso generalizzato agli utenti dell'area o del settore interessati, evidenziando

l'utilizzo irregolare degli strumenti aziendali e invitando gli utenti ad attenersi scrupolosamente alle disposizioni impartite.

Nel caso in cui la situazione di rischio o l'anomalia nell'utilizzo degli strumenti aziendali non sia risolvibile da un controllo su dati aggregati come sopra precisato, l'amministratore di sistema specificamente autorizzato per iscritto, anche con delega generale, può effettuare controlli circoscritti su singole postazioni di lavoro, in conformità alle norme dell'ordinamento o alla giurisprudenza.

In quest'ultimo caso, previo avviso agli utenti interessati e anche in assenza di questi, l'amministratore di sistema può accedere alla postazione di lavoro, fermo restando che l'accesso può avvenire esclusivamente per motivi di sicurezza o manutenzione come sopra precisato.

L'attività effettivamente eseguita sulla postazione di lavoro deve essere in ogni caso comunicata all'utente interessato senza ingiustificato ritardo al termine dell'intervento. La struttura ICT dovrà annotare, anche in modalità telematica, gli interventi svolti, specificando i motivi, la data e l'orario dell'intervento, dando atto degli avvisi intervenuti nei confronti del soggetto o dei soggetti interessati.

#### 16. *Osservanza delle disposizioni in materia di protezione dei dati personali e a tutela dell'Istituto*

Tutti gli utenti devono attenersi alle disposizioni in materia di protezione dei dati personali, in particolare in relazione alle misure minime di sicurezza come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Codice in materia di protezione dei dati personali.

Non verrà fornita assistenza tecnica a fronte di problematiche di connessione imputabili al dispositivo personale.

L'utente si astiene dal diffondere e comunicare, anche mediante pubblicazione sui *social network*, immagini e/o video degli ambienti e dei locali di IOR (comprese le aree verdi esterne e i parcheggi), nonché informazioni relative alle attività di IOR, oltre che alle persone, senza apposita autorizzazione dell'Istituto.

Salvo autorizzazioni specifiche ed eccezionali, non è consentito l'utilizzo di attrezzatura informatica personale in ambienti sanitari protetti (ad esempio nelle sale operatorie).

#### 17. *Cessazione della disponibilità dei servizi informatici aziendali e sanzioni*

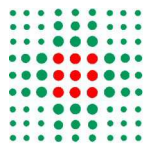
Ai sensi del presente regolamento, l'utente non avrà più accesso ai servizi informatici aziendali, oltre che nei casi eventualmente previsti nei precedenti paragrafi del presente regolamento, qualora:

- non sussistano più i requisiti soggettivi necessari per l'accesso ai servizi informatici;
- qualora non sia confermata l'autorizzazione all'uso fornita dal Responsabile;
- qualora vengano accertate manomissioni e/o interventi sul *hardware* e/o sul *software*; diffusione o comunicazione da parte dell'utente di *password*, procedure di connessione, indirizzo IP ed altre informazioni tecniche riservate;
- nel caso di accesso doloso dell'utente a *directory*, a siti e/o *file* e/o servizi dannosi, da chiunque resi disponibili;
- qualora l'attività dell'utente cagioni un danno, anche solo potenziale, al sito contattato.

Il mancato rispetto o la violazione del presente regolamento potranno, se accertati, essere sanzionati, a seconda della gravità, con provvedimenti disciplinari e risarcitori previsti dalla contrattazione collettiva, nonché con tutte le azioni civili e penali consentite.

#### 18. *Aggiornamento e revisione del regolamento*

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente regolamento. Le proposte verranno esaminate dalla Direzione Generale.



**ICT**

## INFORMATIVA AGLI UTENTI CHE UTILIZZANO I SERVIZI INFORMATICI IOR

Questa informativa è resa, ai sensi dell'art. 13 del d.lgs. 30 giugno 2003, n. 196 e s.m. ("Codice in materia di protezione dei dati personali"), agli utenti di Istituto Ortopedico Rizzoli ("IOR") al fine di fornire chiare e comprensibili indicazioni circa il trattamento dei rispettivi dati in relazione all'utilizzo dei servizi informatici di IOR.

Il trattamento da parte di IOR avviene nel rispetto della legge e degli obblighi di riservatezza, in particolare in osservanza dei principi di necessità e non eccedenza del trattamento previsti dal Codice.

### *Tipologia di dati e finalità del trattamento*

I dati degli utenti raccolti e trattati da IOR in relazione all'utilizzo dei servizi informatici aziendali comprendono i dati relativi alle operazioni effettuate servendosi delle credenziali di autenticazione, l'indirizzo IP della postazione di lavoro, data e ora, salvati nei file di log.

Si tratta di informazioni raccolte esclusivamente per garantire il corretto svolgimento del rapporto contrattuale, la sicurezza ed il funzionamento dei servizi informatici, nonché per finalità connesse alle esigenze organizzative, produttive e di sicurezza del lavoro nel rispetto di quanto previsto dall'art. 4, 2° comma, l. 20 maggio 1970, n. 300 così come modificato dal d.lgs. 14 settembre 2015, n. 151.

Tra i dati raccolti non sono compresi dati sensibili o comunque altri dati o informazioni di carattere personale dell'interessato, ad eccezione di quelli sopra riportati.

### *Modalità del trattamento*

Il trattamento dei dati personali dell'utente sarà effettuato attraverso strumenti automatizzati consistenti nella memorizzazione e nella registrazione dei *file* log di sistema a cura del personale incaricato della struttura ICT.

Tali dati saranno conservati dalla struttura ICT, per conto di IOR, per un periodo massimo di sei mesi, al termine del quale verranno cancellati. Durante tale periodo le registrazioni potranno essere utilizzate, su richiesta del Titolare o dei Responsabili del trattamento dei dati personali, esclusivamente in conformità alla legge, per finalità statistiche e di valutazione della qualità dei servizi erogati sulla rete.

I dati relativi all'utilizzo dei servizi informatici non sono oggetto di diffusione. Tuttavia, per le finalità indicate al punto precedente, potrebbero essere comunicati dagli operatori della struttura ICT al Responsabile dell'unità organizzativa di appartenenza dell'utente.

I log potranno poi essere oggetto di comunicazione nei confronti dell'Autorità giudiziaria e amministrativa quando risulti necessario per l'adozione di specifici provvedimenti, nonché ai soggetti incaricati delle funzioni ispettive e di controllo all'interno dello IOR.

#### *Natura obbligatoria del conferimento dei dati*

Il conferimento dei dati è obbligatorio in quanto necessario allo svolgimento stesso del rapporto contrattuale che lega l'utente a IOR, nonché per il perseguimento delle finalità di corretto funzionamento e utilizzo dei sistemi informatici e di tutela del patrimonio aziendale, come espressamente previsto dalla legge. Pertanto l'eventuale rifiuto al trattamento determina l'impossibilità di IOR di dar corso ai rapporti contrattuali con l'utente.

#### *Titolare del trattamento*

Il Titolare del trattamento dei dati è l'Istituto Ortopedico Rizzoli, legalmente rappresentato dal Direttore Generale, con sede legale in Bologna, Via di Barbiano, 1/10.

#### *Diritti dell'utente interessato*

Ciascun utente interessato ha il diritto, in qualunque momento, di ottenere la conferma dell'esistenza o meno dei propri dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione ai sensi dell'art. 7 del d.lgs. 196/2003. Ai sensi del medesimo articolo ciascun interessato ha altresì il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati che lo riguardano trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Per qualunque informazione in merito al trattamento dei dati, nonché per l'esercizio dei diritti ex art 7 del d.lgs. 196/2003, gli utenti possono avanzare richiesta al Titolare, rivolgendosi alla

segreteria della Direzione Generale, Via di Barbiano, 1/10 – Bologna, designata per il riscontro all'interessato oppure al Direttore della struttura ICT attraverso i seguenti canali:

Direzione Generale  
Istituto Ortopedico Rizzoli  
via di Barbiano, 1/10  
40136 Bologna  
direzione.generale@pec.ior.it

ICT  
Istituto Ortopedico Rizzoli  
salita di San Benedetto, 1  
40136 Bologna  
sistemi.informativi@pec.ior.it



SCANSIONARE E INVIARE VIA EMAIL A [abilitazioni.ict@ior.it](mailto:abilitazioni.ict@ior.it)

**Dati del Richiedente**

Cognome e Nome			
Codice Fiscale			
E-mail aziendale			
Struttura di appartenenza			
Codice Centro di Costo			
Durata rapporto di lavoro o collaborazione			
Matricola		Telefono	Cellulare
Profilo (medico, infermiere, amministrativo, ...)			
Data di decorrenza	___/___/___	Data fine	___/___/___

Servizi o Sistemi Informatici di cui si richiede:  attivazione  disattivazione  riattivazione

Motivazione della richiesta: \_\_\_\_\_

AREA GENERALE	AREA SANITARIA	AREA AMMINISTRATIVA	AREA RICERCA
<input type="checkbox"/> Posta elettronica	<input type="checkbox"/> SIR	<input type="checkbox"/> GRU	<input type="checkbox"/> PRWEB - progetti
<input type="checkbox"/> Accesso internet	<input type="checkbox"/> AREAS	<input type="checkbox"/> GE4	<input type="checkbox"/> CARDINIS
<input type="checkbox"/> Password aziendale	<input type="checkbox"/> DNWEB	<input type="checkbox"/> GE4 web richieste on line	
<input type="checkbox"/> Rete Wi-Fi "IOR"	<input type="checkbox"/> DNTER	<input type="checkbox"/> CE4	
<input type="checkbox"/> Firma digitale con CNS	<input type="checkbox"/> POLARIS	<input type="checkbox"/> CI4CI -inventario	
<input type="checkbox"/> Cartella per archiviazione	<input type="checkbox"/> ATHENA	<input type="checkbox"/> CASSA TICKET DRS	
<input type="checkbox"/> Posta Elettronica PEC	<input type="checkbox"/> DIGISTAT	<input type="checkbox"/> PRWEB - progetti	
	<input type="checkbox"/> LOG80	<input type="checkbox"/> BUSINESS OBJECT	
	<input type="checkbox"/> GARCIA	<input type="checkbox"/> OSLO	
	<input type="checkbox"/> BUSTERMED	<input type="checkbox"/> BABEL	
	<input type="checkbox"/> ELIOT	<input type="checkbox"/> SO4	
	<input type="checkbox"/> ELIOTWEB		
	<input type="checkbox"/> MYSANITA		

ALTRO (specificare) \_\_\_\_\_

<b>Reparti (REP), ambulatori (AMB), laboratori (L) ai quali si desidera essere abilitati</b> (E' possibile specificare un collega dal quale copiare le abilitazioni) Copia abilitazioni da utente (Nome, cognome, login) _____		
Tipologia (REP, AMB, L)	Descrizione	Codice CDC

L'utente richiedente dichiara di aver preso attenta visione del "Regolamento per l'utilizzo dei servizi informatici" e di accettare sotto la propria responsabilità tutte le condizioni ivi contenute.

Nel caso in cui dimentichi la password, per riottenere l'accesso ai servizi l'utente dovrà contattare il servizio di assistenza informatica per richiederne una nuova, che dovrà essere obbligatoriamente modificata al primo accesso.

Data, \_\_\_\_\_ In fede \_\_\_\_\_


**Il Responsabile della struttura dell'utente richiedente**

Cognome e Nome	Timbro e Firma
----------------	----------------

-----  
Da compilare solo in caso che il Responsabile della struttura dell'utente richiedente non sia responsabile dei servizi di cui si chiede l'abilitazione.

**Responsabile organizzativo dei servizi di cui si richiede l'abilitazione**

Cognome e Nome	Timbro e Firma
----------------	----------------

 <p>SERVIZIO SANITARIO REGIONALE EMILIA - ROMAGNA Istituto Ortopedico Rizzoli di Bologna Istituto di Ricovero e Cura a Carattere Scientifico</p> 	<b>MODULO</b> <b>RICHIESTA DI ABILITAZIONE</b> <b>AI SERVIZI INFORMATICI IOR E</b> <b>ALLA TELEASSISTENZA PER UTENTI</b> <b>ESTERNI</b>	<b>ICT/IOR/2</b> <b>Rev. 1.0</b> <b>Pag. 1/1</b> <b>1-10-2017</b>
---	---	--

SCANSIONARE E INVIARE VIA EMAIL A [abilitazioni.ict@ior.it](mailto:abilitazioni.ict@ior.it)

**Dati del Richiedente**

Cognome e Nome			
Codice Fiscale			
Ente/Ditta			
Convenzione/Contratto			
Durata Convenzione/Contratto			
Indirizzo sede di lavoro			
Telefono		Cellulare	
E-mail			
Data di decorrenza	___/___/___	Data fine	___/___/___

Servizi o Sistemi Informatici di cui si richiede:  attivazione  disattivazione  riattivazione

Motivazione della richiesta: \_\_\_\_\_

<p><b>Attivazione VPN per manutenzione sistemi (breve descrizione)</b></p> <p><b>Indirizzi IP postazioni da mantenere: .....</b></p> <p><b>Servizi/Sistemi da abilitare: (ad esempio: vnc, ssh, SIR, Digistat, Babel...)</b></p> <p>-----</p> <p>-----</p> <p>-----</p>
---

L'utente richiedente dichiara di aver preso attenta visione e di osservare le disposizioni contenute nel Codice di Comportamento IOR e nel "Regolamento per l'utilizzo dei servizi informatici" di IOR e di accettare sotto la propria responsabilità tutte le condizioni ivi contenute.

Nel caso in cui dimentichi la password, per riottenere l'accesso ai servizi l'utente dovrà contattare il servizio ICT IOR per richiederne una nuova, che dovrà essere obbligatoriamente modificata al primo accesso.

Data, \_\_\_\_\_ In fede \_\_\_\_\_



**Il Responsabile del Servizio/Ditta richiedente**

Cognome e Nome	Timbro e Firma
----------------	----------------

-----  
*Parte da compilare da parte del responsabile dei servizi di cui si chiede l'abilitazione*

**Responsabile organizzativo per IOR dei servizi di cui si richiede l'abilitazione**

Cognome e Nome	Timbro e Firma
----------------	----------------

 <p>SERVIZIO SANITARIO REGIONALE EMILIA - ROMAGNA Istituto Ortopedico Rizzoli di Bologna Istituto di Ricovero e Cura a Carattere Scientifico</p> 	<b>MODULO</b> <b>ISTRUZIONI PER IL PRIMO ACCESSO E</b> <b>PER L'ATTIVAZIONE DELLA CASELLA DI</b> <b>POSTA ELETTRONICA</b>	<b>ICT/IOR/3</b> <b>Rev. 1.0</b> <b>Pag. 1/1</b> <b>1-10-2017</b>
---	--	--

Di seguito vengono fornite le credenziali per l'accesso alle risorse informatiche IOR.

utente:

*password* di primo accesso:

indirizzo *e-mail*: @ior.it

La “password di primo accesso”, presente in questa comunicazione, deve essere obbligatoriamente cambiata in occasione del primo utilizzo. La nuova parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri, non deve essere banale e non deve contenere riferimenti agevolmente riconducibili all'utente.

Per procedere alla modifica della *password*, è necessario collegarsi, da qualsiasi computer in rete, all'indirizzo:

<https://areariservata.ior.it/password>

Solo dopo la modifica della *password* sarà possibile accedere e utilizzare le risorse informatiche dello IOR.

Dopo aver cambiato la *password*, per attivare la casella di posta elettronica, occorrerà collegarsi all'indirizzo: <https://webmail.ior.it> oppure dalla pagina <http://www.ior.it>, selezionare la voce “Area Riservata” situata in calce alla pagina e poi selezionare “Accedi alla Posta Elettronica Aziendale”.

Per accedere dall'esterno della struttura IOR, verranno richieste due autenticazioni:

- 1) una prima autenticazione prevede l'inserimento del proprio nome utente nella forma nome.cognome e come *password* il CODICE FISCALE in lettere MAIUSCOLE;
- 2) una seconda autenticazione prevede l'inserimento del proprio nome utente nella forma nome.cognome e come *password* la “password di primo accesso” indicata in questa comunicazione.

Si ricorda che è necessario procedere almeno con cadenza trimestrale alla modifica della *password*.

Si ricorda altresì che le credenziali di autenticazione dovranno essere custodite dall'utente con la massima diligenza e riservatezza e non dovranno essere divulgate né cedute, neppure temporaneamente, a terzi. Si presume che qualsiasi azione svolta sotto l'autorizzazione offerta dalle credenziali di autenticazione sia riferibile e imputabile all'utente titolare di tali credenziali.

Per qualsiasi problema è possibile rivolgersi all'*helpdesk* informatico via email a [helpdesk@ior.it](mailto:helpdesk@ior.it) oppure al n.051 636 6303 (dalle 8.00 alle 17.00 dal lunedì al venerdì).

Prima dell'utilizzo, l'utente deve prendere attenta visione del regolamento per l'utilizzo dei sistemi informatici al *link* <http://intranet.internal.ior.it/manuali/regolamentoICT>



I messaggi di posta elettronica inviati a destinatari esterni devono riportare in calce la seguente comunicazione:

Sostieni la ricerca dell'Istituto Ortopedico Rizzoli con il 5 per mille!  
Codice fiscale 00302030374, riquadro 'finanziamento della ricerca sanitaria.  
Per maggiori informazioni visita il sito [www.ior.it](http://www.ior.it)

Il presente messaggio non ha natura di comunicazione personale da parte del mittente.

**Ricorda di salvaguardare l'ambiente, stampa solo se è necessario.**

Formattazioni:

Helvetica nero 11

Arial Narrow nero 10

**Helvetica verde 11**

Il/La sottoscritto/a .....

in servizio presso .....

telefono .....

Dichiara

di aver ricevuto in data odierna il seguente materiale inventariabile:

.....  
(marca, modello, serial number, nome personal computer)

numero di inventario se già presente

.....

L'utente dichiara di aver preso attenta visione del "Regolamento per l'utilizzo dei servizi informatici" di IOR e di accettare sotto la propria responsabilità tutte le condizioni ivi contenute, in particolare quanto previsto al punto 6 relativo alla corretta gestione della postazione di lavoro.

Il ricevente (Nome Cognome in stampatello e firma)

.....

L'incaricato alla consegna (Nome Cognome in stampatello e firma)

.....

Data di consegna

.....