Gent.mo Sig. / Gent.ma Sig.Ra

Ferrara, li

Oggetto: lettera di autorizzazione al trattamento dei dati personali nel contesto dell'attività di accesso, consultazione ed estrazione ed elaborazione di dati da parte di superiori, laureandi, studenti post laurea, assegnisti, dottorandi, specializzandi, ecc. operanti presso l'AZIENDA USL DI FERRARA e/o presso l'AZIENDA OSPEDALIERO UNIVERSITARIA DI FERRARA.

Gent.mo Studente/Frequentante /Tirocinante,

con la presente, a fronte della rilevata necessità di consentirLe l'acceso ai relativi documenti elettronici e cartacei contenenti dati personali e, comunque, in genere, ai dati personali, anche particolari, di titolarità delle intestate Aziende, Le si segnala che, come disposto dalla normativa in materia di trattamento di dati personali (Reg. UE 2016/679 e D.Lgs. 196/2003), possono accedere ed elaborare i dati personali solo soggetti all'uopo espressamente autorizzati dal Titolare, nel rispetto delle istruzioni impartite da quest'ultimo.

Con la presente, quindi, La si autorizza, con le modalità meglio descritte nell'allegato A alla presente, ad accedere, consultare, estrarre copia ed elaborare i dati coinvolti nelle attività di trattamento effettuati nell'ambito di questo Dipartimento, relativamente alle attività di trattamento in contitolarità alle intestate Aziende, con modalità elettroniche e cartacee e relativi, in particolare, alle normali attività oggetto del Suo rapporto in essere in qualità di studente, frequentante corso post-laurea, stagista, assegnista, dottorando, tirocinante, ecc., limitatamente ai dati relativi alla Struttura cui Lei afferisce, e alle operazioni indispensabili per l'espletamento delle incombenze necessarie all'adempimento degli obiettivi di ricerca, come definiti nei rispettivi programmi di corso o nel progetto formativo di orientamento, sottoscritto tanto dallo studente-frequentante quanto dal Dirigentecompetente.

La S.V. viene pertanto autorizzata ad accedere e a trattare i dati personali e particolari che sono contenuti nei documenti e negli atti aziendali contenenti dati personali (ivi comprese, laddove l'attività demandatale sia di tipo sanitario, il Dossier Sanitario, le cartelle cliniche, i referti, le lettere di dimissioni, ecc..), nonché negli archivi cartacei e/o automatizzati-informatici di pertinenza della Struttura cui Lei afferisce, ai fini dello svolgimento dell'attività di studio-ricerca nonché con le modalità enei limiti stabiliti nel programma di corso.

Il trattamento di dati relativi agli archivi dell'Azienda in rete potrà riguardare tanto quelli attualmente esistenti quanto quelli che potrebbero essere implementati in futuro.

Nel rammentarLe che, per lo specifico ruolo svolto all'interno della Struttura presso cui svolge la sua normale attività, Lei è tenuto ad osservare il maggior riserbo possibile in punto alle informazioni apprese nel corso delle operazioni di trattamento svolte, Le si segnala che è altresì tenuto a prendere visione e seguire le istruzioni che sono riportate *infra*, così come le altre eventuali che potranno essere fornite in seguito, con qualsiasi modalità, anche verbale, allo scopo di garantire chei trattamenti dei dati avvengano secondo le disposizioni di cui al Reg. UE 2016/679 e al D.Lgs. 196/03. In aggiunta alle istruzioni qui allegate,

inoltre, Lei è tenuto a prendere visione e rispettare, accedendovi dalla Sezione Privacy del sito istituzionale aziendale (www.ausl.fe.it e www.ospfe.it):

- il Regolamento per il Trattamento dei dati personali dell'Azienda;
- il Disciplinare sull'utilizzo dei Sistemi Informatici Aziendali;
- la Procedura per la gestione dei casi di violazione dei dati personali (c.d. Data Breach);

Ferme le istruzioni di cui all'all. A alla presente, e i Regolamenti e le Linee Guida sopra citati, Le si segnala, in ogni caso:

- che Le è fatto espresso divieto di salvare i dati di titolarità dell'Azienda in chiavette USB e/o in altri supporti elettronici senza specifica autorizzazione dello scrivente Titolare (che potrebbe fornirLa anche per il tramite del Servizio ICT);
- che Le è fatto espresso divieto di salvare i dati in servizi *cloud* non autorizzati dall'Azienda e/o dallo scrivente (si precisa che è consentito salvare i dati in rete soltanto attraverso il Suo account aziendale, specificamente attivato dallo scrivente Titolare e/o universitario);
- che Le è fatto espresso divieto di salvare in maniera permanente i dati aziendali in pc portatili, smartphone e/o pc desk diversi da quelli professionali o ai quali ha acceso nel corso della sua normale attività universitaria o postlaurea;
- che Le è fatto espresso divieto di sincronizzare in locale gli archivi cloud – o anche soltanto una porzione degli stessi – relativamente ai quali è possibile accedere da remoto;
- che Le è fatto espresso divieto di utilizzare, per la comunicazione di natura accademico-professionale tra Lei e i dipendenti e/o collaboratori dell'Azienda, nonché tra Lei e gli utenti dell'Azienda medesima, indirizzi di posta elettronica diversi da quelli messi a disposizione dall'Azienda: può quindi solo utilizzare, per le comunicazioni, l'indirizzo di sua pertinenza a Lei già noto o, comunque, quello accademico ma Le è espressamente e categoricamente vietato utilizzare indirizzo email personali (es. @gmail.com, @yahoo.it, @libero.it. ecc....);
- che Le è fatto espresso divieto di utilizzare i dati di soggetti facenti parte dell'organico dell'Azienda, dei pazienti e/o di soggetti comunque estranei all'organizzazione dell'intestato Titolare per finalità diverse daquelle strettamente attinenti alle attività della scrivente Azienda e per le quali è stata autorizzata;
- che Lei è tenuto – se non dotato di terminale aziendale – ad utilizzare solo pc o portatili personali sui quali siano state adottate le misure di cui all'art. 32 Reg. UE 2016/679 e, quindi, solo pc messi adisposizione dall'Azienda e/o autorizzati dall'Azienda e/o, comunque, ai quali possa accedere solo Lei, protetti da credenziali di accesso la cui password sia qualificabile come "sicura" (almeno 8 caratteri alfanumerici con almeno una maiuscola);
- che Lei è tenuto, nel caso di utilizzo del proprio pc personale per l'accesso ai dati di titolarità dell'Azienda, ad impedire l'accesso al suo pc o, comunque, al Suo account aziendale ad altri soggetti, ivi compresi i Suoi familiari, e quindi ad impostare il blocca schermo ogni qual volta si allontana dal pc, anche per mere esigenze igieniche;
- che Lei è tenuto, sul proprio pc personale e solo in quanto questo sia utilizzato per l'acceso a dati di titolarità dell'Azienda, a prevedere e installare un antivirus quanto più efficiente;
- che è tenuto a utilizzare, sul proprio pc personale e solo in quanto questo sia utilizzato per l'accesso a datidi titolarità dell'Azienda, solo connessioni di rete sicure e a prestare la massima attenzione anche nel contesto di eventuali attività personali – anche ludiche o di svago, specie se nel contesto della navigazione web – evitando di installare software malevoli, visitare pagine web non sicure e, in generale, a utilizzare applicativi suscettibili di provocare malfunzionamenti o rallentamenti del sistema;
- che Lei è tenuto a custodire con la massima diligenza le proprie credenziali di utente abilitato all'accesso alle cartelle cliniche digitalizzate, con l'assoluto divieto di rivelarle a terzi; per disservizi e malfunzionamenti ricollegabili al proprio utente può rivolgersi al servizio ICT della scrivente Azienda;
- che Lei è tenuto, in caso di perdita o furto del dispositivo personale sul quale erano (anche solo provvisoriamente) archiviati dati di titolarità dell'Azienda, a darne **immediata** (entro 2 ore da quando se ne rende conto) notizia, per le vie brevi, alla scrivente Amministrazione per le determinazioni più opportune.

Si segnala inoltre che, nello svolgimento dell'attività di ricerca, è necessario attenersi anche a quanto indicato nelle ***Linee guida per l'integrità nella ricerca, revisione dell'11 aprile 2019 (prot. n. 0067798/2019)*** della **Commissione per l'Etica e l'Integrità nella Ricerca del CNR**, e successive eventuali modifiche e integrazioni, reperibili alle seguenti coordinate:

https://www.cnr.it/sites/default/files/public/media/doc_istituzionali/linee-guida-integrita-nella-ricerca-cnr-commissione_etica.pdf?v=4

La presente autorizzazione ha validità fino a comunicazione di revoca e/o fino al termine dell'attività di studio e/oricerca, anche post-universitaria o nell'ambito di un tirocinio, svolta all'interno della scrivente Azienda, nel quale caso si intenderà automaticamente e tacitamente revocata.

Le si rammenta altresì la necessità di seguire scrupolosamente la regolamentazione aziendale in materia di trattamentodei dati personali e che, comunque, è tenuto a partecipare ai corsi formativi aziendali in materia di protezione dei dati personali che verranno organizzati dal Servizio Formazione.

Resta fermo, anche successivamente alla validità della presente autorizzazione, l'obbligo di mantenere la più assoluta riservatezza e/o segretezza sulle informazioni apprese nel corso dello svolgimento delle attività svolte.
Cordiali saluti,

Il Direttore Responsabile

per presa visione, in data _____

Firma Studente/tirocinante _____

Allegato A

Istruzioni per il trattamento dei Dati Personali

1. Dato personale

Per *dato personale* si intende 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. Sono quindi *dati personali*, per quanto interessa rispetto all'autorizzazione, tutte leinformazioni concernenti tanto gli operatori sanitari e amministrativi dell'Azienda, dai dati anagrafici, alla tipologia di pratica o attività svolta, passando per i dati contabili, ecc.

Sono definiti, si badi, *dati particolari*, quelle informazioni idonee a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti e sindacati, nonché i dati personali idonei a rilevare **lo stato di salute** (es. dati rinvenibili all'interno delle cartelle cliniche), la vita e l'orientamento sessuale, i dati genetici e idati biometrici.

2. Trattamento di dati personali

Per *trattamento* si intende qualunque operazione o complesso di operazioni, automatizzate o meno, concernente 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. In ogni caso l'elenco non è tassativo. Qualsiasi operazione venga svolta con i documenti, cartacei o elettronici, contenenti dati, costituisce *trattamento* e deve quindi essere svolta nel rispetto dellenorme di legge.

3. Consenso dell'interessato

Il *consenso* serve ogni qualvolta si raccolgano i dati dell'interessato per finalità di ricerca scientifica o per il trattamento dei suoi dati genetici, senza che il medesimo abbia già espresso un validoconsenso in precedenza. Alla raccolta del consenso, in ogni caso e solo ove necessario, procede l'Azienda. L'attività di raccolta del consenso non è demandata al soggetto autorizzato, salvo specifico incarico e/o istruzione in tal senso.

In ogni caso Le si segnala che, per lo specifico trattamento per il quale è autorizzato, non è necessario acquisire il consenso, essendo sufficiente l'informativa che l'interessato visiona prima di procedere all'attività oggetto del corso.

4. Diritti dell'interessato

Per *diritti dell'interessato* si intende la possibilità da parte dell'utente di richiedere informazioni circa i suoi dati trattati,le modalità e le finalità del trattamento, nonché ogni altro tipo di interazione rispetto ai propri dati trattati (cancellazione, blocco, opposizione, modifica, rettifica, integrazione, ecc.).

Nel caso in cui taluno, nel corso della Sua attività, chieda di sapere quali sono i suoi dati trattati, dovrà identificare ilrichiedente, raccogliere la richiesta mediante annotazione, riferire la richiesta al responsabile della struttura organizzativa ove presta la propria attività, evidenziando al richiedente che riceverà riscontro entro un mese.

5. Incarichi.

Il Suo Referente è il Direttore responsabile che ha sottoscritto l'autorizzazione alla quale le presenti istruzioni sono allegate.

L'amministratore di sistema, al quale può chiedere ogni delucidazione di carattere tecnico-informatico, è l'ICT dell'Azienda, che, per qualsiasi necessità, può contattare anche direttamente utilizzando i recapiti messi a Sua disposizione. In caso di disservizi o nell'impossibilità di mettersi in contatto con il Servizio Comune ICT potrà comunque fare riferimento al sottoscrittore della retroscritta nomina.

6. Misure di sicurezza e istruzioni specifiche per la gestione dei dati e dei supporti.

La normativa vigente (art. 32 Reg. UE 2016/679), prevede che nel trattamento dei dati sia indispensabile osservare misure di sicurezza organizzative e tecniche.

Fermo restando la formazione alla quale potrà essere invitato a partecipare, Le si segnala che è tenuto a rispettare leseguenti regole:

- utilizzare, nell'accesso alla rete, ai documenti e ai dati, il codice identificativo personale (CIP) e la parola chiave (PW), evitando di divulgarla. Il suo CIP e la PW iniziali Le sono già stati forniti dall'amministratore di sistema o dal Titolare stesso; si ricorda, comunque, che è obbligo modificare la parola chiave iniziale con una di Sua scelta all'atto del primo accesso; la PW dovrà essere di almeno otto caratteri possibilmente alfanumerici e non dovrà contenere riferimenti a Lei agevolmente riconducibili (es. iniziali del nome, data di nascita, ecc.). É inoltre fatto obbligo di modificare la PW ogni tre mesi, anche senza richiesta o sollecitazione; nel caso in cui la password venga, accidentalmente o meno, conosciuta da terzi, dovrà provvedere a cambiarla immediatamente;

- non dare alcuna comunicazione a soggetti terzi dei dati trattati, se non per ordine o istruzione del Titolare;
- in caso di abbandono, anche temporaneo, della Sua postazione, anche se domestica, deve provvedere allo spegnimento del pc o ad attivare un salvaschermo (screen saver) protetto da password;
- i supporti cartacei contenenti dati personali non possono essere gettati negli ordinari porta rifiuti ma devono essere distrutti attraverso modalità che non ne consentano la ricostruzione in modo agevole;
- informarsi sull'identità e sulle qualità personali di chiunque acceda agli archivi e, nel caso in cui l'accedente sia sconosciuto, dovrà informare immediatamente il Titolare;
- laddove sia necessario inviare a mezzo email documenti contenenti dati particolari è tenuto ad assicurarsi che i documenti inviati siano protetti da password (es. per inserire la password in documenti word è necessario seguire la seguente procedura: Accedere a File > info > proteggere il documento > crittografare con la password Verrà richiesto di creare una password e di confermarla. Dopo aver aggiunto una password al file, salvarlo per essere sicuri che la password venga applicata) oppure trasmetterli a mezzo cloud mediante l'apposita funziona di condivisione previa apposizione di password da comunicare al destinatario attraverso uno strumento diverso da quello attraverso il quale si comunica il link;
- Le è fatto espresso divieto di aprire file allegati ad email dei quali non abbia certezza della loro legittima provenienza (es. file excel o con estensione finale .xls contenute in email di persone sconosciute);
- prestare la massima attenzione in ogni fase di utilizzo e collocazione dei supporti cartacei, verificando che gli elementi di arredo ove vengono ubicati siano regolarmente chiusi, custodendo diligentemente i documenti contenenti dati personali di titolarità della scrivente Aziende, avendo cura che agli stessi non accedano soggetti non autorizzati e restituendoli al termine delle mansioni affidataLe;
- nel caso in cui intenda disfarsi di documenti cartacei contenenti dati personali di titolarità della scrivente Azienda, Lei è tenuta a gettarli solo dopo averli distrutti, ove necessario con l'ausilio di appositi strumenti, con modalità tali da renderne impossibile, o estremamente complessa, la ricostruzione;
- Le è fatto divieto di servirsi della documentazione cartacea che è messa a Sua disposizione in luoghi diversi da quelli di pertinenza della scrivente Azienda, salvo dietro specifica istruzione del Titolare e, in ogni caso, previa adozione di tutte le misure di sicurezza organizzative che si rendano necessarie;
- domandare, in fase di identificazione dell'interlocutore telefonico, informazioni personali che siano presumibilmente solo a sua conoscenza e/o nella sua disponibilità;
- evitare di trascrivere la password per l'accesso al sistema e/o agli applicativi in luogo ove la stessa sia facilmente reperibile.

7. Istruzioni e formazione del personale

Le presente istruzioni devono essere osservate in ogni fase di lavoro svolta durante il corso di studio o il periodo di tirocinio nonché durante tutto il rapporto che intercorre tra Lei e le intestate Azienda, e gli obblighi di riservatezza deidati devono essere rispettati anche dopo la cessazione del rapporto con il soggetto autorizzato, sotto pena di sanzioni penali e amministrative e/o di rivalsa civile per ogni danno del quale le Aziende siano chiamate a rispondere.

Le Aziende organizzeranno periodicamente dei corsi formativi in materia di protezione dei dati personali ai quali il soggetto autorizzato è tenuto a partecipare, in orario di servizio.