Nomina del soggetto "Autorizzato" al trattamento dei dati personali dello Studio osservazionale no profit sull'impatto della vaccinazione anti Covid-19 dal titolo "Efficacia e sicurezza della vaccinazioni anti covid-19 nei pazienti in dialisi: studio di coorte e caso-controllo nested" (di seguito "Studio"), ai sensi del Reg. UE 2016/679 (RGPD) e del D. Lgs. 30 giugno 2003, n. 196, come modificato dal D. Lgs. 10 agosto 2018, n. 101.

PREMESSO CHE

- la Società Italiana di Nefrologia ("SIN") e l'Istituto Superiore di Sanità ("ISS"), con il supporto dell'Agenzia Italiana del Farmaco ("AIFA"), per finalità di ricerca scientifica, hanno promosso lo Studio osservazionale no profit sull'impatto della vaccinazione anti Covid-19 dal titolo "Efficacia e sicurezza della vaccinazioni anti covid-19 nei pazienti in dialisi: studio di coorte e caso-controllo nested";
- nell'ambito dello stesso Studio è previsto il trattamento dei dati personali dei pazienti coinvolti, del quale la SIN è Titolare;
- il Suo Centro di appartenenza, che ha la possibilità di definire il numero di utenze attivabili presso le proprie sedi, abilitando e disabilitando gli "account" dei medici che danno esecuzione allo Studio, ha comunicato alla SIN il suo nominativo;
- in adesione all'art. 29, Reg. UE 2016/679, e alle disposizioni contenute nell'art. 2–quaterdecies del D.lgs. 30 giugno 2003, n. 196, come modificato dal D.lgs. 10 agosto 2018, n. 101, tutti i soggetti del Centro che contribuiscano all'esecuzione dello Studio, per le finalità di ricerca scientifica, vengono nominati dalla SIN soggetti "Autorizzati" al trattamento dei dati personali;

in relazione all'ambito di trattamento consentito, la SIN, in qualità di Titolare del trattamento dei dati relativi ai pazienti inseriti nello Studio, per le finalità di ricerca scientifica, La nomina

AUTORIZZATO AL TRATTAMENTO

Nell'effettuare il trattamento dei dati Lei avrà accesso ai dati personali gestiti pertanto dovrà scrupolosamente attenersi alle norme di legge emanate in materia, e, in particolare, alle seguenti istruzioni di carattere generale:

1. prima di iniziare il trattamento, consegnare l'informativa al paziente e raccogliere il suo consenso al trattamento dei dati personali; tale documentazione deve essere conservata in armadio chiuso a chiave al quale possono aver accesso soltanto i soggetti Autorizzati (o, se raccolto in modalità elettroniche, su database con password) e non deve essere messa a disposizione di alcuno al di fuori dei soggetti Promotori;
2. informare immediatamente la SIN di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati personali (anomalie, furti, perdite accidentali di dati) al fine di attivare, nel caso sia riscontrato un rischio grave per i diritti e le libertà delle persone fisiche, la procedura di gestione del Data Breach (violazione dei dati);
3. controllare e custodire gli strumenti elettronici utilizzati per il trattamento dei dati e i documenti contenenti dati personali, di cui si è a conoscenza o in possesso per lo svolgimento delle attività e dei compiti assegnati, in modo tale da impedire l'accesso a persone non autorizzate o trattamenti non consentiti;
4. non lasciare i documenti incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri autorizzati addetti al medesimo trattamento, poiché tali documenti non

devono esser consultati da altri soggetti non autorizzati al trattamento e non possono esser riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento;
5. utilizzare il codice identificativo (user-id) e la password assegnati per l'accesso ai dati trattati mediante strumenti elettronici e custodirli garantendone la segretezza;
6. effettuare operazioni di trattamento di dati personali soltanto per le finalità dello Studio e con le modalità strettamente correlate allo svolgimento delle attività affidate e secondo le metodologie seguite dal Centro e dalla SIN in ambito scientifico ed epidemiologico;
7. accedere solo ai dati strettamente necessari all'esecuzione delle predette attività;
8. verificare che i dati siano esatti (e, se necessario, aggiornarli), completi ed utilizzati in modo pertinente e non eccedente rispetto alle attività svolte e ai compiti assegnati;
9. trattare i dati personali in modo lecito e secondo correttezza;
10. raccogliere e registrare i dati personali per gli scopi strettamente legati allo Studio;
11. non affidare ad altri specifiche attività di trattamento senza la preventiva autorizzazione della SIN e del Centro;
12. evitare di creare nuove banche dati senza espressa autorizzazione del Titolare;
13. mantenere la riservatezza sui dati di cui venga a conoscenza od in possesso per le attività svolte, senza divulgarli a terzi al di fuori dei casi connessi allo svolgimento delle stesse attività, secondo le indicazioni fornite;
14. conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e trattati;
15. astenersi, in caso di cessazione dell'attività, dall'effettuare operazioni di trattamento dei dati di cui sia venuto a conoscenza durante lo svolgimento dell'incarico e, in particolare, dal conservarli, duplicarli, comunicarli, o cederli a terzi;
16. osservare tutte le misure di protezione e sicurezza, già in atto o successivamente disposte, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei dati personali, attenendosi inoltre, nel trattamento dei dati con o senza l'ausilio di strumenti elettronici, alle ulteriori particolareggiate istruzioni a tal fine impartite dal Titolare;
17. consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit), realizzate dalla SIN, nonché mettere a disposizione della SIN tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del RGPD;
18. restituire ovvero distruggere i dati di cui è in possesso, in caso di revoca della presente nomina da parte della SIN.

La S.V., comunque, effettuerà i trattamenti attenendosi alle "Buone pratiche" per i soggetti Autorizzati (Allegato 1), e alle ulteriori istruzioni che potranno essere impartite, anche successivamente.

La presente nomina di Autorizzato al trattamento dei dati personali può essere revocata in qualsiasi momento, anche senza preavviso; inoltre, essa si intende automaticamente revocata alla cessazione dello Studio; successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto del Titolare.

La preghiamo di comunicare senza ritardo al Suo Centro l'eventuale volontà di non contribuire allo Studio.

Allegato 1

BUONE PRATICHE RELATIVE ALL'UTILIZZO DEI DATI

PREMESSA

Per **dato personale** si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Per **trattamento di dati personali** si intende, invece, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

La progressiva diffusione delle tecnologie informatiche espone a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio di diligenza e correttezza, tuttavia si vuole evitare che condotte inconsapevoli possano innescare minacce alla sicurezza dei dati quali accessi illegittimi ai dati, perdita di dati, modifiche indesiderate ai dati nonché danneggiamenti o malfunzionamenti del sistema informatico.

1. POSTAZIONE DI LAVORO E PERSONAL COMPUTER

Il "Login" è l'operazione con la quale ci si connette al sistema informativo o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account) e aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, rete, ecc.) che richiedono un username e una password.

In alcuni casi può essere assegnato un univoco username e password per gruppi di Autorizzati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci username e password per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro.

Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa in quanto la non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

È sempre opportuno eseguire le operazioni seguenti.

1. Se ci si allontana dalla propria postazione, mettere in protezione il pc affinché persone non autorizzate non abbiano accesso ai dati protetti.
2. Chiudere la sessione (Logout) a fine giornata.
3. Spegnere il PC dopo il Logout.
4. Controllare sempre che non vi siano persone non autorizzate alle spalle che possano prendere visione delle schermate del pc.
5. Non lasciare la postazione informatica incustodita lasciando accessibili i dati; tutti i supporti magnetici utilizzati devono essere riposti negli archivi.

Mediante lo scambio di file via internet, via mail, lo scambio di supporti removibili, il file sharing, le chat, ecc. possono essere trasmessi virus informatici in grado di danneggiare le attrezzature informatiche e "rubare" i dati ivi contenuti.

Alla luce di tutto ciò, non si dovrebbero eseguire le seguenti operazioni.

1. Gestire, memorizzare (anche temporaneamente) o trattare file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative nella rete locale, nel disco fisso o in altre memorie di massa e negli strumenti informatici in genere.
2. Modificare le configurazioni già impostate sul pc.
3. Utilizzare programmi e/o sistemi di criptazione senza preventiva autorizzazione scritta.
4. Installare software senza licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul pc, senza espressa autorizzazione.
5. Fare copia del software installato al fine di farne un uso personale.
6. Caricare sul disco fisso del pc o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
7. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.), senza autorizzazione.
8. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico, quali per esempio virus, trojan horses ecc.
9. Effettuare in proprio attività manutentive o permettere attività manutentive da parte di soggetti non autorizzati.
10. Utilizzare aree di memoria diverse o creare altri files fuori dalle unità di rete locale.
11. Utilizzare i pc e accedere alla rete locale senza sistemi antivirus, antimalware e firewall attivi.
12. Utilizzare i pc senza periodicamente aggiornare i sistemi antivirus, antimalware e firewall.
13. Disattivare l'antivirus, anche temporaneamente.
14. Cliccare su allegati di messaggi di posta elettronica, certificata e non, provenienti da mittenti sconosciuti o di dubbia provenienza.
15. Cliccare su allegati di messaggi di posta elettronica, certificata e non, provenienti da persone conosciute ma con testi inspiegabili o in qualche modo strani.
16. Omettere di comunicare ogni anomalia o malfunzionamento dei sistemi antivirus, antimalware e firewall, nonché la presenza di virus o file sospetti.
17. Omettere di comunicare ogni attività sospetta.

2. PASSWORD

Le password costituiscono un metodo di autenticazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

Per una corretta e sicura gestione delle proprie password, è opportuno attuare le seguenti pratiche.

1. Le password sono segrete e non devono essere svelate ad altri soggetti per evitare danni al proprio lavoro e a quello dei colleghi.
2. Nel tempo anche la password più sicura perde la sua segretezza, perciò è buona norma cambiarle con una certa frequenza, preferibilmente ogni 90 giorni.
3. È buona norma non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.
4. Le password sono assolutamente personali e non vanno mai comunicate ad altri.

5. Occorre cambiare una password non appena si abbia alcun dubbio che sia diventata poco "sicura".
6. Le password dovrebbero essere lunghe almeno 8 caratteri e contenere anche lettere maiuscole, numeri e caratteri speciali quali { } [ ] , . < > ; : ! ” £ $ % & / ( ) = ? ^ \ | ’ * - + _..
7. Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, cellulare).
8. Bisogna evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se autorizzati.

La password ideale è complessa, senza alcun riferimento.
Di seguito, alcuni esempi di password da evitare.

1. Nome, cognome e loro parti.
2. Username assegnato.
3. Indirizzo di posta elettronica (e-mail).
4. Parole comuni (in Inglese e in Italiano).
5. Date, mesi dell'anno e giorni della settimana, anche in lingua straniera.
6. Parole banali e/o di facile intuizione e palindromi.
7. Ripetizioni di sequenze di caratteri (es. abcdabcd).
8. Password già impiegate in precedenza.
9. Se Username = "marioverdi", password = "mario", o ancora peggio, password = "marioverdi".
10. Il nome della moglie/marito, fidanzato/a, figli, ecc. anche a rovescio.
11. La propria data di nascita, quella del coniuge, ecc.
12. Targa della propria auto.
13. Numero di telefono proprio, del coniuge, ecc.
14. Il nome di login (o codice di identificazione personale) in qualsiasi forma (ad esempio: invertito, in maiuscole, duplicato, ecc.).
15. Il nome del sistema operativo che si sta usando.
16. Il numero di telefono.
17. Altre informazioni facilmente ricavabili dall’indirizzo, o parti del codice fiscale.
18. Nomi di città, nomi propri.
19. Semplici composizioni quali ad esempio “qwerty”.
20. Caratteri sequenziali ripetuti (ad esempio 1111, aaaa, ecc.).
21. Cifre in progressivo ordine crescente o decrescente.
22. Informazioni legate al lavoro quali nomi di software, hardware, nomi di prodotti o servizi.

3. DATI RACCOLTI MEDIANTE SUPPORTI CARTACEI - CLEAR DESK POLICY

È opportuno adottare una “politica della scrivania pulita” ovvero trattare dati raccolti mediante supporti cartacei solo se necessario, privilegiando, ove possibile, l’utilizzo degli strumenti digitali.
In particolare, si invita a non lasciare in vista sulla propria scrivania dati raccolti mediante supporti cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) è opportuno riporre in luogo sicuro (armadio, cassettiera, archivio, ecc.) i dati raccolti mediante supporti cartacei, affinché gli stessi non possano essere visti da terzi (es. addetti alle pulizie, visitatori, ecc.).
A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d’ufficio, in modo da lasciare la scrivania completamente sgombra, e, ove possibile, bisogna evitare la

stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.
È opportuno rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
Ove possibile, è buona norma eliminare i documenti attraverso apparecchiature trita documenti.
A seguito di una cessazione del rapporto lavorativo è necessario restituire immediatamente i dati raccolti mediante supporti cartacei in possesso.
L'eventuale accesso fuori dall'orario di lavoro impone la registrazione e identificazione delle persone ammesse ai locali e i documenti (o loro copia) non possono, senza autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi, previa autorizzazione.
Sarebbe opportuno conservare in armadi ben custoditi gli archivi relativi alle banche dati raccolti mediante supporti cartacei assicurandosi che gli uffici siano adeguatamente chiusi.
Qualora venga raccolto il consenso dell'interessato, il relativo documento deve essere custodito con la massima cura ed adeguate misure di sicurezza al fine di evitare che altri soggetti prendano visione dei dati riportati nel documento.

4. PROCEDURA IN CASO DI SOSPETTA VIOLAZIONE DEI DATI (DATA BREACH)

Con il termine data breach si intende la violazione dei dati personali dell'interessato, persona fisica, che può consistere, a titolo esemplificativo e non esaustivo, in:

- perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti;
- discriminazione, furto o usurpazione d'identità;
- perdite finanziarie, decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale;
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti;
- infedeltà (ad esempio: data breach causato da un autorizzato, il quale, dopo aver avuto accesso ai dati, ne produca una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo proprietario;
- virus o altri attacchi al sistema informatico o alla rete locale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche al cui interno sono contenuti dati personali "in chiaro" e non cifrati;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

In linea con la definizione di violazione di dati personali, ex art. 4 par. 12 Reg. UE 2016/679, possiamo distinguere tre tipi di violazione, che possono tuttavia combinarsi tra loro:
1) violazione di riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati;
2) violazione di integrità, in caso di alterazione di dati personali non autorizzata o accidentale;

3) violazione di disponibilità, quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.

La rilevazione di un evento di data breach può avvenire in maniera automatica (da sistemi di segnalazione automatica come, ad esempio, violazioni conseguenti al superamento del firewall); dall'interno (segnalazione ad opera di autorizzati, e/o amministratori di sistema, intrusioni fisiche di soggetti non autorizzati nei locali, furti, smarrimenti di fascicoli cartacei e/o di devices contenenti dati personali, blocco dei sistemi e/o malfunzionamenti degli stessi); dall'esterno (segnalazione durante le attività di monitoraggio, manutenzione e assistenza da parte di fornitori).

In caso di sospetto data breach viene attivata una procedura ad hoc, nella quale il Responsabile Protezione Dati assume il ruolo di responsabile del processo.

Lo scopo della procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali.

Ogni volta che vengono rilevate attività sospette per quanto riguarda la protezione dei dati, è opportuno avvisare il proprio Centro, il soggetto che le ha inviato le credenziali di accesso, il Responsabile della Protezione dei Dati della Società Italiana di Nefrologia, il Responsabile della Protezione dei Dati dell'Istituto Superiore di Sanità.

Il Presidente della Società Italiana di Nefrologia
(Titolare del trattamento)
Prof. Piergiorgio Messa

Il soggetto Autorizzato al trattamento

☐ Per presa visione ed accettazione