Intesi Group Spa

Via Torino 48
20123 Milano (MI)
Tel: 026760641
P.IVA 02780480964
PEC: intesigroup@ig-trustmail.com

ELENCO DELLE MISURE DI SICUREZZA ADOTTATE PER TRATTAMENTI CONTO TERZI

Sono sotto riportate le misure di sicurezza implementate ai sensi dell'art.32 del Reg.to UE 2016/679.

Misure di sicurezza adottate a livello logico ed organizzativo

Redazione di un piano di formazione per gli addetti	È previsto un piano di formazione degli addetti, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevedere eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure adottate. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali.
Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione.	Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti del trattamento consentito agli addetti ed ai responsabili della gestione o manutenzione dei sistemi elettronici.
Verifica dei Back-up.	È stato predisposto un piano di verifica periodica del corretto funzionamento delle copie di Back-Up.
Consegna istruzioni dettagliate agli addetti.	Ad ogni addetto sono state consegnate istruzioni dettagliate e complete riguardanti il trattamento dei dati personali, a seconda dei suoi compiti e dei dati trattati. ► Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei. Gli incaricati hanno ricevuto istruzioni scritte sul comportamento da tenere per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento. ► Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari. In caso di dati sensibili o giudiziari, sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. ► Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento. Sono impartite istruzioni agli incaricati per non lasciare incostudito e accessibile lo strumento elettronico durante una sessione di trattamento. ► Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali. Istruzioni per assicurare la segretezza della componente riservata della credenziale (es. password) e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
Procedure per ripristino dei dati.	Sono state adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori ai 7 giorni.

È stato redatto e viene annualmente aggiornato il Manuale Organizzativo Privacy.	Il Manuale Organizzativo Privacy contiene i documenti e le procedure organizzative ed operative da effettuarsi da parte degli operatori durante un trattamento di dati personali.
Distruzione dei supporti removibili.	Nel caso di dati particolari o giudiziari, i supporti rimuovibili che contengono tali dati se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere usati da personale non autorizzato solo dopo che i dati in essi contenuti sono resi non intelleggibili e tecnicamente in alcun modo recuperabili.
Descrizione scritta degli interventi effettuati da terzi.	Quando ci si avvale di soggetti esterni per l'adozione pratica delle misure di sicurezza, viene richiesta la descrizione scritta dell'intervento effettuato che ne attesta la conformità a norma di legge.
Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna.	Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna.
Verifica annuale operato Amministratori di Sistema.	L'operato degli amministratori di sistema è verificato con cadenza almeno annuale da parte del Titolare al trattamento.
Redazione del Registro dei Trattamenti sia in qualità di Titolare sia se necessario in qualità di Responsabile	Il Registro dei Trattamenti e documento cogente e contiene la lista dei trattamenti effettuati eventuali comunicazioni degli stessi all'esterno e relative misure di sicurezza attuate.
Redazione documento Privacy by Design e By Default	Redazione Piano di Privacy by Design e By Default per documentare per tutti i trattamenti l'attuazione delle necessarie misure di sicurezza ex. Art. 32 in grado di garantire un rischio residuale basso
Nomina del DPO	Nomina del Data Protection Officer
Procedure Gestione Data Breach	Redazione ed Implementazione Procedure strutturale ed organizzative per la gestione di eventuali Data Breach
Implementazione Procedura di Nomina a Responsabile del trattamento	Implementazione Procedura di Nomina a Responsabile del trattamento per tutte le strutture esterne che trattano dati per conto del Titolare
Implementazione procedura di verifica per i Responsabile del trattamento	Implementazione procedura di verifica affinché i trattamenti effettuati da esterni abbiano adeguate garanzie di rischio residuale basso
Verifica delle valutazioni preventive ai sensi dell'art. 5 paragrafo 1 del GDPR.	Ogni Titolare ai sensi dell'articolo 5 paragrafo 2 deve essere in grado di dare evidenza della valutazione effettuata prima e durante il trattamento dei dati. Il Titolare del trattamento deve essere in grado di dimostrare la conformità delle attività dello stesso compresa l'efficacia delle misure di sicurezza ai sensi dell'articolo 32 e della Privacy by Design e by Default ai sensi dell'articolo 25 del GDPR.

Misure di sicurezza adottate per trattamento

- **Gestione e conservazione di documenti digitali**

Gestione e conservazione di documenti digitali

Tipi di Dati trattati:	• Tipi di dati definiti all'interno del DPA.
Archivi utilizzati per il trattamento	• Backup Archivi di Conservazione (fino al 2022) ; • Deleghe Digitali eW ; • Gestione e Conservazione Digitale ; • PEC Organizer per clienti eWitness .

Misure Adottate

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato. ► Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali.
Cifratura dei dati memorizzati.	I dati salvati su sistemi di archiviazione digitale vengono cifrati attraverso sistemi di protezione in ssl, PGP, o altri sistemi di cifratura proprietari
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ► Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione.

Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazioni nel caso di dati affidati all'esterno.
Verifica ed eventuale nomina degli amministratori di sistema se presenti	Verifica ed eventuale nomina degli amministratori di sistema se presenti
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Trattamento dei dati con protocolli criptati.	Trattamento dei dati con protocolli criptati ad es. SSL o criptazione dei dati tramite PGP
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.
Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda	Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda

• Manutenzione Applicativo presso il cliente

Manutenzione di un sistema applicativo installato presso il cliente

Dati Comuni trattati:	• Dati personali comuni se previsti dal cliente.
Tipi di Dati trattati:	• Dati personali particolari se previsti dal cliente.
Dati Particolari Giudiziari trattati:	• Dati personali giudiziari se previsti dal cliente.
Archivi utilizzati per il trattamento	• Applicativo installato presso cliente .

Misure Adottate

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password.
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ► Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione.

Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazioni nel caso di dati affidati all'esterno.

- **Servizio di firma elettronica non qualificata**

Servizio di firma elettronica non qualificata (ACS, FEA e altre firme elettroniche)

Dati Comuni trattati:	• codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale; • attività economiche, commerciali, finanziarie e assicurative; • dati personali come indirizzo IP ed altri dati comuni gestiti in cookie essenziali (strictly necessary); • cookie di tipo funzionale alla navigazione (functionality cookie); • Numero di telefono; • Videoregistrazioni; • Foto o fotocopie di documenti di identità.
Archivi utilizzati per il trattamento	• Armadio Erogazione (Sede: Sede principale azienda); • Data Center Equinix .

Misure Adottate

Copertura Assicurativa	Stipula adeguata copertura assicurativa per eventi inerenti ai trattamenti dati relativi al GDPR
Installazione Allarme	Installazione Allarme
Estintori	Installazione Estintori e verifica periodica degli stessi.
Custodia in classificatori o armadi non accessibili	I dati cartacei sono archiviati in modo da permettere l'accesso esclusivamente agli addetti al trattamento degli stessi e di non essere accessibili a persone non autorizzate.
Dotazione serrature archivio	Se sono presenti dati particolari o giudiziari in archivi cartacei, è utilizzata una chiusura a chiave dell'archivio.
Archivio ad accesso controllato.	L'accesso all'archivio è controllato dagli incaricati al trattamento o dalla sorveglianza. Dopo l'orario di chiusura possono accedere all'archivio solo le persone preventivamente autorizzate od identificate e registrate.
Controllo dei documenti con dati particolari o giudiziari da parte degli addetti.	Quando i documenti contenenti dati particolari o giudiziari sono affidati agli addetti del trattamento, sono controllati e custoditi dagli stessi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Sospensione manuale delle sessioni di Lavoro.	Sospensione manuale delle sessioni di Lavoro.
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ► Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione.
Verifica ed eventuale nomina degli amministratori di sistema se presenti	Verifica ed eventuale nomina degli amministratori di sistema se presenti

- **Servizio di Hosting**

Tipi di Dati trattati:	• Tipi di dati definiti all'interno del DPA.
Archivi utilizzati per il trattamento	• Gestionale eWitness .

Misure Adottate

Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disattivazione delle vecchie credenziali. Le credenziali di identificazione sono disattivate se non vengono usate da almeno sei mesi (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica), oppure non appena l'incaricato perde la qualità di accedere ai dati personali.
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento.
Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazioni nel caso di dati affidati all'esterno.
Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda	Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda
Verifica ed eventuale nomina degli amministratori di sistema se presenti	Verifica ed eventuale nomina degli amministratori di sistema se presenti

- **Servizio di invio SMS come Responsabile**

Servizio di invio SMS come secondo fattore di autenticazione

Dati Comuni trattati:	• Numero di telefono; • Dati relativi al contenuto delle comunicazioni e dati di traffico.
Archivi utilizzati per il trattamento	• SMS di Commify (ex Mobyt) ; • SMS e messaggistica .

Misure Adottate

Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.

- **Servizio IG Sign**

Servizio in cloud per il workflow di approvazione e firma di documenti, utilizzato dai clienti di Intesi Group in qualità di Titolari

Dati Comuni trattati:	• nominativo, indirizzo o altri elementi di identificazione personale; • Numero di telefono.
Tipi di Dati trattati:	• Tipi di dati definiti all'interno del DPA.
Archivi utilizzati per il trattamento	• IG Sign ; • Mandrill ; • Data Center Equinix .

Misure Adottate

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Autenticazione mediante user-id e password. ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ► È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ► Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione.

Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazioni nel caso di dati affidati all'esterno.
Verifica ed eventuale nomina degli amministratori di sistema se presenti	Verifica ed eventuale nomina degli amministratori di sistema se presenti
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Sospensione manuale delle sessioni di Lavoro.	Sospensione manuale delle sessioni di Lavoro.
Separazione dei dati sulla salute dagli altri dati personali su sistemi elettronici	I dati sulla salute sono separati in visualizzazione ed archiviazione dagli altri dati personali. Negli archivi elettronici basta che ad nella prima schermata non siano visibili i dati sulla salute. Gli enti sanitari hanno l'obbligo di separazione dei dati sulla salute dagli altri dati personali
Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda	Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda
Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.

- **Servizio SPID come Aggregatore**

Dati Comuni trattati:	• codice fiscale ed altri numeri di identificazione personale; • nominativo, indirizzo o altri elementi di identificazione personale; • cookie di tipo funzionale alla navigazione (functionality cookie); • Numero di telefono.
Archivi utilizzati per il trattamento	• Data Center Equinix .

Misure Adottate

Copie di Back-up.	Sono impartite istruzioni organizzative e tecniche e sono predisposte attrezzature elettroniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. ► Back-Up giornaliero.

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni). ► Disposizioni scritte per la disponibilità dei dati. Quando l'accesso ai dati è consentito solo mediante l'uso della componente riservata della credenziale, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con il quale si può assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato.
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Sospensione manuale delle sessioni di Lavoro.	Sospensione manuale delle sessioni di Lavoro.
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ► Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione.
Verifica ed eventuale nomina degli amministratori di sistema se presenti	Verifica ed eventuale nomina degli amministratori di sistema se presenti

- **Test Factory**

Test di prodotti software per conto dei clienti

Dati Comuni trattati:	• nominativo, indirizzo o altri elementi di identificazione personale.
Tipi di Dati trattati:	• Tipi di dati definiti all'interno del DPA.
Archivi utilizzati per il trattamento	• Google Suite ; • MS Office 365 & Teams .

Misure Adottate

Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni).
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Sospensione manuale delle sessioni di Lavoro.	Sospensione manuale delle sessioni di Lavoro.
Trattamento dei dati con protocolli criptati.	Trattamento dei dati con protocolli criptati ad es. SSL o criptazione dei dati tramite PGP
Profili di autorizzazione di ambito diverso per diversi incaricati.	Nel caso in cui gli incaricati possano accedere solo a certi tipi di dato, od effettuare solo alcuni trattamenti, i profili di autorizzazione devono essere diversificati per ciascun incaricato. ► È utilizzato un sistema di autorizzazione. Sono definiti od utilizzati procedure e strumenti che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione. ► I profili di autorizzazione vengono specificati prima di ogni trattamento. A ciascun incaricato viene assegnato il proprio profilo di autorizzazione prima dell'inizio del trattamento. ► Verifica periodica del profilo di autorizzazione. Periodicamente, ed almeno annualmente, sono verificati i profili di autorizzazione.
Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.	Nel caso di archivio gestito in modalità ISP, è necessario che il gestore dell'archivio attui adeguate misure di sicurezza in modo da garantire rischi residuali bassi sui trattamenti. Vedere la sezione sul Registro dei Trattamenti per ulteriori informazioni nel caso di dati affidati all'esterno.
Verifica ed eventuale nomina degli amministratori di sistema se presenti	Verifica ed eventuale nomina degli amministratori di sistema se presenti

- **Trattamento per conto terzi in Area Solutions**

Trattamento di dati personali di cui è titolare un cliente, effettuato dall' Area Solutions.

Tipi di Dati trattati:	• Tipi di dati definiti all'interno del DPA.
Archivi utilizzati per il trattamento	• Dispositivo individuale (Sede: Smart Working).

Misure Adottate

Installazione di un Firewall.	Nel caso di trattamento di dati personali con strumenti elettronici connessi con l'esterno, anche in maniere indiretta o solo saltuariamente, è necessario installare un firewall software od hardware per evitare l'accesso abusivo ad essi. ► Firewall software. Firewall Software
Antivirus.	Sono installati sugli elaboratori elettronici che contengono dati personali, programmi antivirus, aggiornati almeno semestralmente. ► Aggiornamento ogni mese.
Credenziali di autentificazione, assegnate individualmente ad ogni addetto.	Il trattamento dei dati è consentito solo dopo il superamento di una procedura di autentificazione univocamente associata all'addetto e relativa ad uno specifico trattamento o ad un insieme di trattamenti. Inoltre il codice di identificazione, quando utilizzato, non viene mai assegnato ad altri addetti, nemmeno in tempi diversi. ► Autenticazione mediante user-id e password. ► Parola chiave di almeno 8 caratteri. Le parole chiave sono di 8 caratteri od il massimo consentito dal sistema, non devono essere riconducibili all'incaricato e vengono modificate almeno ogni 3 mesi (6 se vi sono solo dati comuni).
Aggiornamento Software.	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità o a correggere difetti, sono effettuati tenendo conto di avere installato almeno la versione precedente all'ultima disponibile.
Cifratura dei dati trasmessi.	Quando vengono trasmessi da un sistema digitale ad un altro i dati prima della trasmissione vengono cifrati co sistemi di protezione come SSL, PGP, ZIP con password o altri Sistemi proprietari. Gli enti sanitari e gli operatori in ambito sanitario hanno l'obbligo di trasmettere i dati sensibili sulla salute utilizzando sistemi di cifratura ► Cifratura con protocollo SSL.
Sospensione automatica delle sessioni di lavoro.	Il sistema sospende automaticamente la sessione di lavoro in determinate circostanza (tipo dopo un tempo minimo di inattività).
Sospensione manuale delle sessioni di Lavoro.	Sospensione manuale delle sessioni di Lavoro.