Fac simile di testo da inserire nei contratti/convenzioni/lettera d'incarico per la nomina di Responsabile del trattamento dei dati

L'Azienda Provinciale per i Servizi sanitari (APSS) per l'espletamento delle funzioni previste nel presente …….. **(indicare se contratto/convenzione/lettera d'incarico etc.)** si avvale della collaborazione di……**(indicare denominazione del soggetto esterno)** e, a tal fine, trasmette allo/a stesso/a dati personali il cui trattamento sia indispensabile per lo svolgimento di dette funzioni.

……**(indicare denominazione del soggetto esterno)** diviene parte sostanziale dell'APSS, ai fini della privacy, essendo vincolato/a ad utilizzare i dati per le sole finalità perseguite dall'Azienda e secondo le modalità dalla stessa indicate.

L'APSS, in qualità di Titolare del trattamento dei dati personali trasmessi a……**(indicare denominazione del soggetto esterno)**, ai sensi dell'art. 29 del decreto legislativo 196/2003, nomina……**(indicare denominazione del soggetto esterno)** Responsabile del trattamento dei dati personali strettamente inerenti allo svolgimento dell'attività affidata con il presente……**(indicare se contratto/convenzione/lettera d'incarico etc.)**, secondo le definizioni di "trattamento", di "dato personale" e di "dato sensibile" specificate all'art. 4 del citato decreto legislativo 196/2003.

……**(indicare denominazione del soggetto esterno)** con la sottoscrizione del presente ……**(indicare se contratto/convenzione/lettera d'incarico etc.)**, accetta la nomina di Responsabile e si impegna al rispetto delle vigenti disposizioni normative in materia di protezione dei dati personali e degli adempimenti previsti nel Disciplinare per lo scambio informativo tra Azienda Provinciale per i Servizi Sanitari e soggetti "Contitolari" o "Responsabili" di trattamenti di dati personali, di cui si allega copia.

In particolare……**(indicare denominazione del soggetto esterno)** è tenuto a:

- rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza, l'integrità e la completezza dei dati trattati, secondo quanto disposto dal titolo V della parte I "Sicurezza dei dati e dei sistemi" e dal disciplinare tecnico contenuto nell'allegato B) del decreto legislativo 196/2003, allegato alla presente, nonché tutte le altre disposizioni contenute nella normativa e nelle direttive del Garante;
- individuare e dare istruzioni scritte ai propri Incaricati del trattamento, in conformità alla legge; copia di tali istruzioni dovrà essere inviata all'Azienda;
- assicurare che l'eventuale accesso alle banche dati sia consentito solo al personale autorizzato e per ragioni inerenti ai doveri d'ufficio e secondo i principi di pertinenza e non eccedenza;
- sollecitare e verificare il rispetto da parte degli incaricati del trattamento delle misure di sicurezza necessarie per garantire la riservatezza dei dati;
- consentire la comunicazione di dati personali all'esterno unicamente nei casi e con i limiti previsti dagli artt. 18 e 19 del d.lgs. 196/2003, dagli artt. 20 e 22, per quanto riguarda specificatamente i dati sensibili ed in particolare i dati inerenti alla salute, nonché dall'art. 25, in forza del rinvio operato dall'art. 18, comma 5, ed in ogni caso secondo le indicazioni dell'Azienda;
- interagire con il Garante in caso di richieste di informazioni o effettuazione di controlli e accessi da parte dell'Autorità;
- informare prontamente il Titolare di tutte le questioni rilevanti ai fini della legge (ad esempio richieste del Garante, esiti di ispezioni dell'Autorità, richieste degli interessati, etc.);
- rispondere prontamente alle istanze degli interessati, in esecuzione di quanto disposto dall'art. 7 del d.lgs. 196/2003 attenendosi alle istruzioni che verranno impartite dall'Azienda;
- attuare procedure di verifica periodica (almeno annuale) dell'osservanza delle disposizioni del d.lgs. 196/2003; di tali verifiche e delle conseguenti risultanze deve tenere traccia e darne evidenza al titolare su richiesta dello stesso;
- consentire e agevolare le attività di audit svolte dal Titolare o da soggetti terzi da esso incaricati circa il rispetto delle misure minime di sicurezza;
- nel solo caso in cui l'attività contrattualmente prevista corrisponda a quella descritta nel punto 25 dell'allegato B) del decreto legislativo 196/2003 – Disciplinare tecnico in materia di misure minime di sicurezza –

(installazione/aggiornamento misure minime di sicurezza) dovrà essere fornita una descrizione scritta dell'intervanto effettuato che ne attesti la conformità alle disposizioni del medesimo disciplinare tecnico;

- riconsegnare all'Azienda, secondo le indicazioni date dalla stessa in relazione allo specifico trattamento affidato, i dati personali alla cessazione del trattamento degli stessi e conseguentemente distruggere tutte le copie detenute a qualunque titolo (allegato fac simile dichiarazione sostitutiva di atto notorio).

Disciplinare per lo scambio informativo tra Azienda provinciale per i servizi sanitari e soggetti esterni "Contitolari" o Responsabili" di trattamento di dati personali

Versione: 1/2012

Sommario

1. Introduzione

L'Azienda Provinciale per i Servizi Sanitari di Trento (APSS) autorizza l'accesso alla propria rete aziendale ai soggetti (contitolari e responsabili) che a vario titolo concorrono all'erogazione dei servizi sanitari rivolti al cittadino per agevolarne la condivisione di informazioni, dati e servizi.

Sono considerati "contitolari" i Medici di Medicina Generale (MMG), i Pediatri di Libera Scelta (PLS), le strutture accreditate, le Comunità di Valle, il Comune di Trento e il Comune di Rovereto e le farmacie comunali e private.

In particolare, si vuole garantire la messa a disposizione e l'integrazione dei sistemi informativi di APSS con quelli delle strutture pubbliche e private e dei professionisti accreditati del Servizio sanitario provinciale, allo scopo di gestire in rete ed in modo condiviso le informazioni cliniche e sullo stato di salute del paziente durante il suo percorso assistenziale, per assicurare la continuità e la qualità dell'assistenza in qualsiasi struttura coinvolta nel processo (trasferimento da una struttura all'altra o al passaggio in cura dall'una all'altra o comunque l'assunzione in cura presso una struttura del sistema sanitario provinciale per eseguirvi prestazioni diagnostiche che richiedono la valutazione anamnestica).

Le regole contenute nel disciplinare sono estensibili a tutte le altre situazioni diversificate di connessione telematica con soggetti operanti per conto di APSS sulla base di accordi contrattuali e/o convenzionali con il Servizio sanitario provinciale, anche qualora gli stessi fossero designati quali Responsabili (es. partners, fornitori, associazioni di volontariato, cooperative sociali) e quindi tenuti ad osservare, nel trattamento di dati personali, le disposizioni in materia di sicurezza privacy definite da APSS.

Il presente documento riporta le regole da applicare per disciplinare l'uso di risorse aziendali da parte dei soggetti sopra indicati (soggetti esterni) operanti nell'ambito del Servizio sanitario provinciale, a seconda dei casi, in qualità di "Contitolari" o di "Responsabili" del trattamento dei dati personali dei cittadini. Il

rispetto da parte dei soggetti esterni delle regole relative all'uso degli strumenti messi a disposizione da APSS è condizione necessaria per l'accesso ai servizi informatici aziendali e per il loro utilizzo.

Le stesse regole sono da intendersi come base di impegno (reciproco) che i contitolari di trattamento accettano per lo sviluppo delle proprie politiche di adeguamento alla disciplina della protezione dei dati personali.

Il disciplinare rappresenta quindi a sua volta una misura di sicurezza volta a garantire che i trattamenti di dati personali e sensibili condivisi tra APSS e i soggetti esterni si svolgano nel rispetto delle disposizioni di cui al d.lgs. 196/2003 "Codice in materia di protezione dei dati personali" (Codice privacy). Ai sensi dell'art. 4, comma 1, lettera f) del Codice privacy s'intende per "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.

Nell'organizzazione sanitaria della Provincia di Trento, caratterizzata dall'utilizzo di forme diverse di comunicazione bidirezionale tra professionisti sanitari, strutture sanitarie pubbliche e private accreditate, di cui è prevedibile l'evoluzione verso l'attivazione di un sistema informativo integrato, le decisioni in ordine sia alle finalità e modalità del trattamento che agli strumenti utilizzati, ivi compreso il profilo della sicurezza, devono essere prese di comune accordo tra i diversi titolari: quindi si configura una situazione di "contitolarità", tra APSS e gli altri soggetti operanti in ambito sanitario, relativamente ai dati idonei a rivelare lo stato di salute condivisi con la finalità di garantire un livello qualitativamente più elevato di assistenza sanitaria al cittadino.

Ai sensi dell'art. 4, comma 1, lettera g) del Codice privacy s'intende per "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; secondo le indicazioni del Garante può essere designato quale Responsabile sia un soggetto interno che un soggetto esterno all'organizzazione del Titolare: in particolare è necessario procedere alla designazione di un responsabile ogniqualvolta un trattamento di dati sensibili venga effettuato, anche parzialmente, da un soggetto terzo al quale è affidato un servizio in outsourcing.

Le indicazioni riportate nel presente disciplinare valgono come principi di tipo generale e come obiettivo a tendere; la situazione attuale può contemplare un'ampia articolazione di situazioni con specificità connesse a particolari contesti temporanei che verranno progressivamente allineati a quanto di seguito riportato.

I trattamenti di dati personali che attengono allo scambio informativo tra APSS e "Contitolari" o "Responsabili" sopra indicati (soggetti esterni) possono essere prevalentemente ricondotti ai seguenti specifici macrotrattamenti:

- Prescrizione e/o prenotazione di esami diagnostici e visite specialistiche; o Farmaci e presidi terapeutici o protesici;
- Comunicazione elettronica di referti di esami diagnostici e visite specialistiche, estratti cartella clinica, lettere di dimissione, integrazione con i sistemi informativi territoriali e di MMG, telemedicina etc.;
- Informazioni gestionali inerenti gli ospiti in RSA/APSP (scheda UVM, giornate di presenza, piani di trattamento, etc.);
- Dati di attività gestionale (consistenza, presenza e qualifiche del personale, rendicontazione di dati economico finanziari, etc.);
- Gestione dell'informativa e del consenso in materia di sicurezza e privacy, integrazioni delle anagrafiche gestionali;
- Dati correlati a terapie, diagnosi, anamnesi, trattamenti sanitari fisici, farmacologici, ortopedici, chirurgici, ecc.;

- Dati correlati ad attività di manutenzione o di conduzione tecnica di apparati e apparecchiature, di software di base, gestionale o di programmi applicativi;
- Dati correlati alle attività socio sanitarie (accettazione, valutazione, servizi domiciliari, centri diurni etc.)

Al fine di garantire un accesso efficiente, sicuro e affidabile da parte dei soggetti sopra indicati è fondamentale che siano rispettate le seguenti regole tecniche, organizzative, comportamentali e quelle riguardanti i contenuti informativi.

2. Opzioni di servizio disponibili per soggetti esterni Contitolari o Responsabili

APSS propone, in alternativa, tre tipi di servizio che possono essere scelti autonomamente e liberamente dal soggetto esterno in relazione alle sue esigenze o al suo specifico orientamento o al grado di alfabetizzazione informatica, fatta salva la facoltà di APSS di verificare la coerenza e la legittimità dell' opzione:

- servizio di estensione della rete APSS presso il soggetto esterno
- servizio di accesso alla rete ed alle applicazioni APSS senza la fornitura di stazioni di lavoro o servizio di accesso non telematico (fisico) da preferire in caso di operazioni necessariamente realizzabili in loco presso le strutture aziendali

Entrambi i primi due servizi consentono la completa fruizione delle funzionalità di interscambio dei dati fra APSS e soggetto esterno, con prestazioni confrontabili.

I due servizi si differenziano invece sostanzialmente, come ampiamente dettagliato nei successivi paragrafi, in termini di:
- coinvolgimento di APSS in attività tecnologiche;
- autonomia delle scelte in materia di dotazione strumentale (PC) e gestione tecnico operativa; o dotazioni strumentali di supporto alla comunicazione messe a disposizione da APSS

A prescindere dall'opzione scelta dal soggetto esterno, devono in ogni caso essere salvaguardati gli aspetti connessi alla sicurezza del collegamento telematico e all'uso corretto e legittimo dei servizi e degli apparati e dei supporti messi a disposizione da APSS.

3. Servizio di estensione della rete APSS presso il soggetto esterno

Questo servizio è pensato per fornire al soggetto esterno quanto necessario allo scambio informativo senza che l'interlocutore debba preoccuparsi degli aspetti informatici e tecnologici del collegamento telematico.

Pertanto è rivolto a quei soggetti che operano in ambito sanitario, con limitate capacità tecnico informatiche che necessitano di un servizio globale, omnicomprensivo, equivalente a quello fornito alle strutture aziendali.

Il servizio comprende una dotazione strumentale, hardware e software, la fornitura di un collegamento telematico, dei servizi tecnici di supporto e dei servizi di manutenzione.

3.1 Fornitura di dispositivi, apparati e strumentazione

Per promuovere l'interazione con i soggetti esterni, qualora gli stessi non siano fornitori di beni o servizi informatici, APSS mette a disposizione di detti soggetti l'attrezzatura informatica. APSS fornisce ad ogni soggetto esterno, che opti per avere un servizio di estensione della rete APSS presso di sé, la seguente dotazione informatica:

- uno o più Personal Computer con caratteristiche tecniche allineate con quelle dei PC standard in dotazione presso le proprie strutture interne
- una o più stampanti con caratteristiche tecniche allineate a quelle delle stampanti standard aziendali; la stampante sarà assegnata per ogni singola struttura (e non per singolo soggetto) qualora i soggetti operino in rete LAN o siano configurabili in rete LAN.

Il materiale di consumo quale carta, toner, nastri, etichette, ecc. restano a carico del soggetto esterno. Per ragioni di praticità di utilizzo saranno forniti prevalentemente PC in versione DeskTop dotati di schermo a colori secondo le disponibilità dell'azienda, tastiera e mouse. Per i soggetti esterni che per ragioni funzionali ed organizzative necessitassero di più stazioni di lavoro, APSS valuterà l'opportunità di aumentare la dotazione di PC e stampanti. Per la singola struttura in cui opera il soggetto esterno APSS fornirà un collegamento telematico con le seguenti caratteristiche: - collegamento wireless o ADSL o ISDN alla rete aziendale.

La tipologia del collegamento e le caratteristiche di dettaglio saranno individuate da APSS in relazione alla opportunità tecnologica, alle caratteristiche prestazionali e all'onerosità della connessione. Le caratteristiche del collegamento potranno cambiare nel tempo in relazione:

- alla disponibilità sul territorio di particolari tecnologie, o all'evoluzione tecnologica, o alla adeguatezza dei sistemi di comunicazione rispetto ai flussi di dati coinvolti.

Non è prevista la fornitura di accessori delle stazioni di lavoro quali plotter, chiavi USB, stampanti di caratteristiche particolari, modem, penne ottiche, ecc.

Non sono inoltre previsti interventi riguardanti il cablaggio delle sedi operative né collegamenti a LAN preesistenti. Tali problematiche restano di competenza e a carico del soggetto esterno.

APSS si riserva di sostituire o di aggiornare gli apparati messi a disposizione dei soggetti esterni, a propria discrezione valutando caso per caso la relativa obsolescenza tecnologica, con l'obiettivo di mantenere funzionale ed efficiente la connessione telematica.

3.2 Identificazione dei beni forniti da APSS

I beni forniti da APSS saranno identificati da appositi contrassegni o etichette che il soggetto esterno si impegna a non manomettere in alcun modo. In particolare il codice ASP sull'etichetta gialla identifica il posto di lavoro e deve essere utilizzato dal soggetto esterno ogni qualvolta necessiti di interfacciare i servizi di manutenzione, assistenza e supporto di APSS. La presenza del codice qualifica il bene come dotazione strumentale fornita da APSS che può giovarsi dei vari servizi di supporto messi a disposizione.

3.3 Corredo software messo a disposizione da APSS

Sui PC messi a disposizione da APSS saranno installati alcuni software licenziati direttamente da APSS che servono a garantire il buon funzionamento dell'apparato e la sicurezza gestionale del medesimo e della connessione alla rete aziendale. Tale dotazione software potrà mutare nel corso del tempo anche in relazione alle evoluzioni tecnologiche. I software che saranno inizialmente installati sui PC sono:

- il sistema operativo Windows XP Pro o versioni successive individuate da APSS;
- il software antivirus Symantec; o l'agente Tivoli per la teleassistenza;
- qualora necessario l'agente VPN Client per la cifratura dei dati trasmessi;

- il software di office automation per la produttività individuale comprensivo di casella di posta elettronica;
- il software Acrobat Reader per la lettura dei documenti in formato standard pdf; o il software Winzip di compressione file/dati; o il software di connessione alle applicazioni APSS [1]; o il software di connessione ad Internet;
- qualsiasi altro software che APSS riterrà utile per l'uso corretto, sicuro e funzionale della stazione di lavoro.

Il PC sarà configurato in modo tale che non sia possibile la disinstallazione dei software predisposti da APSS e non sia possibile l'installazione di ulteriori software senza specifica autorizzazione.

Qualora la "chiusura" del PC fosse tecnicamente impossibile o inopportuna, o parziale, il soggetto esterno si impegna a garantire il mantenimento della configurazione del bene nello stato consegnato e predisposto da APSS.

Per ragioni connesse alla gestione delle licenze software il soggetto esterno non è autorizzato ad installare sul bene di APSS alcun software nemmeno qualora APSS o il soggetto stesso dispongano di specifica licenza.

L'autorizzazione al caricamento/installazione di software ulteriore sarà data esplicitamente dal Responsabile del Servizio Sistemi Informativi o dai Responsabili di trattamento dei dati presso APSS, previa richiesta specifica che deve essere inoltrata al servizio di Call Center.

3.4 Servizi messi a disposizione da APSS

I servizi messi a disposizione del soggetto esterno sono classificabili in due categorie:

- servizi applicativi funzionali o servizi di supporto alla dotazione strumentale.

I servizi applicativi funzionali comprendono i servizi di scambio di dati fra APSS e soggetto esterno per raggiungere gli obiettivi di efficacia e di efficienza sanitaria previsti per il miglioramento del supporto al cittadino paziente. Rientrano in questa categoria di servizi l'accesso ad applicazioni remote come il SIO, il SIT, Ippocrate, Eusis richieste, Synapse, Atlante o altri applicativi aziendali, l'utilizzo di strumenti di comunicazione come la posta elettronica, Internet, l'accesso alla Intranet aziendale o alla Biblioteca online, la veicolazione di documenti quali i referti, l'elenco degli assistiti, ecc.

Coerentemente con la fornitura degli apparati, l'APSS mette a disposizione dei soggetti esterni i seguenti servizi di supporto alla dotazione strumentale:

- l'installazione degli apparati messi a disposizione da APSS
- la manutenzione degli apparati hardware messi a disposizione da APSS l'assistenza agli utenti limitatamente ai prodotti di APSS cioè gestiti internamente da APSS e/o forniti da APSS a corredo della postazione di lavoro [2] o l'assistenza agli utenti limitatamente ai prodotti di APSS cioè gestiti internamente da APSS e/o forniti da APSS a corredo della postazione di lavoro [2]
- il servizio di Help Desk gestito per APSS da Informatica Trentina (tel. 0461 800150) per:
  la segnalazione di malfunzionamenti la richiesta di informazioni tecniche relative ai prodotti e servizi gestiti da APSS
  la richiesta di ulteriori beni e servizi informatici previsti per i soggetti esterni

[1] Nel caso di MMG e PLS verrà installato sul PC uno dei software di cartella ambulatoriale compresi nel progetto, che dovrà essere attivato dal medico mediante il codice di licenza: si precisa che l'onere della licenza rimane a carico del medico.

[2] E' da precisare che APSS non fornirà supporto e/o manutenzione riguardo i programmi specifici dei medici, quali la cartella ambulatoriale, la gestione dei farmaci, ecc.

- la manutenzione del collegamento telematico e delle sue componenti strutturali ○ l'assistenza tecnica sul collegamento telematico e sul suo funzionamento ○ l'aggiornamento automatico delle impronte virali (antivirus) e del software di sicurezza.

Si ribadisce che i servizi di cui sopra vengono erogati esclusivamente in relazione ai beni strumentali e al software specificatamente messi a disposizione da APSS ed esclude qualsiasi intervento inerente altri strumenti informatici del soggetto esterno e/o altri software non forniti direttamente da APSS.
Non sono previsti altri servizi per i soggetti esterni.
Per usufruire dei servizi, i soggetti esterni dovranno contattare il Call Center di Informatica Trentina al numero 0461 800150, dovranno qualificarsi e dovranno fornire i dati di contesto che saranno richiesti,

In particolare il codice ASP della stazione di lavoro usata dall'utente e per la quale si chiede assistenza. I livelli di servizio previsti per i soggetti esterni sono gli stessi previsti per i soggetti interni ad APSS.

Per l'autorizzazione delle richieste di ulteriori beni e servizi informatici, che verranno gestite tramite la procedura GRU (Gestione Richieste Utente), il soggetto competente è individuato nel Direttore del Servizio Prestazioni e Soggetti Accreditati o nel Direttore del Servizio Amministrazione del Distretto di appartenenza della struttura accreditata .

I servizi di cui al presente paragrafo saranno erogati direttamente da personale APSS o dai suoi fornitori, in particolare Informatica Trentina e Trentino Network, nei giorni feriali e in orario d'ufficio (9:00 – 16:30).

4. Servizio di accesso alla rete ed alle applicazioni APSS senza fornitura di stazioni di Lavoro

Questo servizio è pensato per fornire al soggetto esterno un accesso protetto alla rete aziendale senza nessuna forma di intrusività nel contesto tecnologico dello stesso e garantendo la sua totale autonomia nelle scelte tecnologiche informatiche, nelle relazioni con i suoi partner e fornitori, nella propria dotazione strumentale.

Questa opzione è rivolta a quei soggetti che necessitano di un supporto tecnico limitato da parte di APSS e che non intendono introdurre nei loro asset tecnologici periferiche (PC e stampanti) di APSS per realizzare la connessione telematica con APSS e con le sue applicazioni e pertanto intendono mantenere una sostanziale indipendenza sotto il profilo del corredo hardware e software delle proprie stazioni di lavoro. Ricadono in questa categoria i fornitori di beni e servizi relativi al sistema informativo o informatico aziendale.

Il servizio comprende una dotazione strumentale hardware rivolta alla interconnessione con la rete aziendale, la fornitura di canali di telecomunicazione e servizi tecnici di supporto e di manutenzione analoghi a quelli descritti ai precedenti paragrafi 2.1 e 2.4 associati alle componenti infrastrutturali fornite da APSS (accesso VPN), ma non comprende la fornitura di PC, di stampanti e dei relativi servizi a corredo quali il servizio di call center, la procedura di gestione delle richieste utente (GRU), servizi di consulenza tecnica o di supporto all'installazione o altro.

4.1 Accesso alla rete APSS

Il servizio messo a disposizione da APSS può comprendere in relazione alle varie tipologie di contratto/convenzioni in essere una delle seguenti tipologie alternative di connessione: ○ collegamento ADSL alla rete aziendale ○ collegamento ISDN alla rete aziendale ○ collegamento Wireless alla rete aziendale

- la messa a disposizione di un collegamento ad Internet presso la sede APSS di capacità adeguata ad ospitare i flussi di dati da e verso il soggetto esterno comprendente: la gestione di User Id e Password per l'accesso via VPN alla rete aziendale il software di connessione alla VPN aziendale la documentazione per predisporre l'accesso via VPN

Per essere fruito, il servizio di accesso via VPN necessita che il soggetto disponga di una propria connessione alla rete pubblica (Internet).

Il servizio può mettere inoltre a disposizione, sempre con riferimento alle varie tipologie di contratto/convenzioni in essere:

funzioni di instradamento del traffico (routing) dei flussi di comunicazione funzioni di accesso alla rete ed interfacce fisiche di connessione (switch layer2)
funzioni di sicurezza (firewall) e di traduzione degli indirizzi IP (NAT) ove necessario

La tipologia del collegamento e le caratteristiche di dettaglio saranno individuate da APSS in relazione alla opportunità tecnologica, alle caratteristiche prestazionali e all'onerosità della connessione. Le caratteristiche del collegamento potranno cambiare nel tempo in relazione:

alla disponibilità sul territorio di particolari tecnologie, all'evoluzione tecnologica, all'adeguatezza dei sistemi di comunicazione rispetto ai flussi di dati coinvolti.

4.2 Fornitura di dispositivi, apparati e strumentazione

Il servizio può comprendere, qualora APSS lo ritenga opportuno, la fornitura degli apparati necessari a creare la comunicazione fra i sistemi del soggetto esterno e la rete APSS quali ad esempio:

switch di layer 3° router, bridge di connessione alla rete APSS, eventuali sistemi di antenna radio,
un numero di porte di accesso in tecnologia Ethernet/FastEthernet adeguate alla singola installazione,
firewall di separazione delle reti coinvolte.

Non è prevista la fornitura di alcun dispositivo, apparato o strumentazione per i soggetti esterni che operano come partner o fornitori di beni e servizi informatici.

4.3 Corredo software messo a disposizione da APSS

APSS mette a disposizione del soggetto esterno il software applicativo necessario alla interazione con i server e le basi di dati aziendali. APSS mette a disposizione del soggetto esterno il software già preconfigurato per la realizzazione dell'eventuale VPN.
Il software è liberamente scaricabile dal sito di APSS appositamente predisposto il cui indirizzo sarà comunicato ai soggetti che aderiranno al progetto e opteranno per questa opzione.

4.4 Servizi messi a disposizione da APSS

APSS mette a disposizione i servizi applicativi funzionali.

I servizi applicativi funzionali comprendono i servizi di scambio di dati fra APSS e soggetto esterno per raggiungere gli obiettivi di efficacia e di efficienza sanitaria previsti per il miglioramento del supporto al cittadino paziente. Rientrano in questa categoria di servizi l'accesso ad applicazioni remote come il SIO, il SIT, Synapse, l'utilizzo di strumenti di comunicazione come la posta elettronica, Internet, l'accesso alla Intranet aziendale, la veicolazione di documenti quali i referti, l'elenco degli assistiti, ecc.

In modo complementare mette a disposizione le procedure ed i meccanismi per la segnalazione di guasti e malfunzionamenti degli applicativi, per la richiesta di informazioni sull'uso degli stessi e servizi di formazione ed addestramento.

Non sono previsti servizi di supporto alla dotazione strumentale del soggetto esterno. Non sono previsti servizi di Call Center. Non sono previsti servizi di supporto tecnico/consulenza/assistenza tecnica per le componenti di sistema informativo che esulano dalle componenti fornite da APSS. Non sono previsti servizi di manutenzione sulla rete del soggetto esterno ad esclusione del collegamento fornito da APSS.

Non è prevista la fornitura di alcun servizio funzionale per i soggetti esterni che operano come partner o fornitori di beni e servizi informatici.

5. Obblighi dei soggetti esterni

Il soggetto esterno è tenuto a leggere e seguire scrupolosamente quanto disposto nel presente Disciplinare e si impegna a:

- rispettare e applicare tempestivamente le disposizioni normative sulla sicurezza del trattamento dei dati previste dal Codice della Privacy e le disposizioni emanate dal Garante; le prescrizioni indicate al Titolare devono essere in tal caso recepite senza ulteriore indicazione di APSS dal soggetto terzo nominato Responsabile;
- evitare in qualsiasi caso la diffusione dei dati di cui APSS è Titolare o Contitolare e garantire la comunicazione ai soli soggetti indicati o concordati con APSS. Il soggetto terzo deve garantire di non trasferire ad insaputa di APSS informazioni o dati affidati, verso fornitori, partner o altre destinazioni;
- verificare periodicamente (almeno annualmente) lo stato di consistenza delle misure di sicurezza tecniche, organizzative e procedurali presso la propria organizzazione, la loro efficacia e la loro adeguatezza. Di tali verifiche deve tenere traccia e darne evidenza, su richiesta, ad APSS;
- trattare i beni informatici messi a disposizione da APSS con la massima cura e a non modificarne la configurazione hardware e software, la consistenza, la dotazione sw in alcun modo e per nessun motivo, salvo esplicita autorizzazione scritta di APSS;
- consentire l'accesso ai locali dove sono installate le apparecchiature fornite da APSS da parte dei tecnici di APSS o di quelli che svolgono il servizio di assistenza tecnica per conto di APSS, eventualmente concordando preventivamente l'orario, per ragioni di manutenzione degli apparati e di verifica della connessione telematica;
- garantire ed accettare azioni di controllo e di audit da parte di personale APSS (o di terzi da essa incaricati) al fine di verificare il rispetto delle misure di sicurezza minime ed idonee in accordo con quanto stabilito dalla normativa sulla privacy, nonché il rispetto delle disposizioni contenute nel presente disciplinare;
- informare, formare ed aggiornare costantemente il proprio personale sugli aspetti connessi alla sicurezza del trattamento dei dati.

Il soggetto esterno è direttamente responsabile dei dati in suo possesso e dei trattamenti di cui sono oggetto. E' altresì responsabile dei dati di APSS ad esso affidati per il trattamento di competenza. Il salvataggio periodico dei dati (backup e relativo restore) residenti sulle stazione di lavoro o sui sistemi gestiti (cioè dei quali disponga di accesso a livello di amministratore del sistema) dal soggetto esterno, presso le proprie sedi o presso le sedi di APSS, è di sua competenza ed a suo totale carico.

In caso di guasto delle apparecchiature dovute ad un uso non corretto del bene, ad abuso o a grave incuria, in caso di furto o di perdita, il soggetto esterno risponderà del danno al bene assegnatogli e degli eventuali ulteriori danni arrecati in conseguenza di tale comportamento.

In particolare i soggetti contitolari sono tenuti a gestire l'informativa e la raccolta del consenso previsti dalla Codice della privacy con modalità che siano non solo coerenti con quanto disposto dalla norma ma anche con quelle definite da APSS di concerto con le altre organizzazioni che operano all'interno del servizio sanitario provinciale. In particolare dette modalità devono tener conto delle modalità previste dal progetto TreC (Cartella Clinica del Cittadino) tramite il quale il cittadino può accedere da uno specifico portale, e a seguito di autenticazione forte, ai propri dati riguardanti referti, certificazioni ed altre informazioni sanitarie prodotte dagli operatori che cooperano a tutela della sua salute.

6. Disposizioni tecniche

6.1 Disposizioni tecniche generali

Le stazioni di lavoro del soggetto esterno deputate a collegarsi alla rete aziendale dell'APSS devono essere dotate di un sistema antivirus che deve essere periodicamente aggiornato, con frequenza almeno settimanale. Qualora tali stazioni di lavoro siano connesse ad altre stazioni di lavoro attraverso una rete locale o collegamenti geografici, la stessa disposizione vale anche per tali stazioni di lavoro.

L'APSS è disponibile ad installare (o a far installare) un proprio sistema antivirus sulle stazioni di lavoro interessate al collegamento e a garantirne tecnicamente l'aggiornamento. Tale ipotesi sarà valutata caso per caso sia sotto il profilo tecnico che sotto il profilo economico.

Il soggetto esterno si impegna a non manomettere in alcun modo eventuali componenti software fornite da APSS e le relative configurazioni e ad utilizzarle sistematicamente secondo le indicazioni che verranno fornite dal personale tecnico che provvederà alla predisposizione dell'ambiente tecnologico.

I personal computer usati dal soggetto esterno per accedere alla rete APSS deve montare a bordo il sistema operativo Windows in una delle seguenti versioni: WindowsXP (Standard o Professional), Windows Vista o successivi aggiornamenti come indicato da APSS. L'APSS provvederà ad aggiornare l'indicazione delle tipologie di sistema operativo in relazione all'evoluzione tecnologica. APSS si riserva di accettare l'accesso alla propria rete da parte di stazioni di lavoro con altri Sistemi Operativi. Oltre al sistema operativo sul personal computer dovrà essere disponibile il browser MS Explorer vers.
6.0 o superiore.

Qualora il soggetto debba accedere al sistema di posta elettronica aziendale, il posto di lavoro deve essere dotato di MS Outlook (o Outlook Express).

Il soggetto esterno deve garantire che i personal computer utilizzati per la connessione al sistema informativo di APSS siano mantenuti aggiornati in tutte le componenti del software di sistema ed in particolare il sistema operativo, il software di produttività individuale ed i software di comunicazione, applicando tempestivamente tutte le correzioni al software rilasciate dal fornitore, particolarmente quelle riferite alla sicurezza.

Qualora la stazione di lavoro sia messa a disposizione dal soggetto esterno, il medesimo deve garantire che il personal computer sia dotato degli adeguati tools di comunicazione: scheda di rete, porta USB, porta seriale, funzionanti. Il soggetto esterno deve garantire che i personal computer utilizzati per la connessione al sistema informativo di APSS siano privi di virus o di altri programmi o codici malevoli che possano minacciare la rete di APSS ed i suoi contenuti.

Le stazioni di lavoro del soggetto esterno deputate a collegarsi alla rete aziendale dell'APSS, devono essere dotate di un sistema di screensaver a tutela della riservatezza dei dati in occasione di temporaneo abbandono della stazione di lavoro da parte dell'incaricato. Lo screensaver deve essere configurato per

entrare in azione dopo un tempo di inutilizzo coerente con l'uso della stazione di lavoro e della sua collocazione logistica (in area aperta al pubblico, in area condivisa con colleghi non incaricati, in area riservata, ecc.) con l'operatività dell'incaricato e della finalità della misura di sicurezza.

6.2 Disposizioni tecniche specifiche per i soggetti esterni Responsabili fornitori di beni e servizi informatici

Qualora il soggetto terzo produca software per APSS, lo stesso deve applicare le normative internazionali ed europee relative alla sicurezza. Deve adottare le best practices del settore ed aderire agli standard di qualità quali ISO12207 e ISO/IEC 9126. Deve inoltre garantire l'adesione a quanto stabilito da DigitPA per la "Qualità forniture e servizi ICT".

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, lo stesso deve garantire soluzioni che dispongano di sistemi di autenticazione e di gestione delle credenziali che rispettino l'allegato B del Codice della privacy, preferibilmente integrabile con il sistema LDAP aziendale, con codice utente liberamente scelto da APSS, privo di vincoli in termini di alfabeto usabile e di numero di caratteri, password con requisiti di robustezza configurabili, oscurata durante la digitazione e modificata/modificabile al primo utilizzo. La scadenza delle credenziali deve essere configurabile e forzata. Deve essere disponibile un report degli account con credenziali scadute.

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, lo stesso deve garantire che la soluzione fornita non contenga password d'utente o di amministratore cablate nel codice, che le stesse siano modificabili liberamente in qualsiasi momento da parte di ogni singolo utente, che la creazione di nuovi utenti, l'assegnazione delle credenziali, la loro abilitazione, la modifica e la disabilitazione possa avvenire in maniera autonoma da parte di APSS.

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, lo stesso deve garantire la presenza di meccanismi di profilazione dell'utente, configurabili autonomamente da APSS e la presenza di un sistema di reportistica dei profili e delle abilitazioni / disabilitazioni associate, indicazione delle tipologie di dati gestiti (personali, sensibili, supersensibili, genetici, giuridici, …).

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, lo stesso deve garantire la cifratura dei dati sensibili o la codifica degli stessi secondo quanto disposto dall'Allegato B al Codice della Privacy.

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, lo stesso deve garantire che la soluzione proposta disponga di log applicativo che registri almeno le seguenti informazioni: data e ora di accesso (dell'utente e dell'amministratore), userid, data e ora di utilizzo della funzione / sottofunzione applicativa o amministrativa, data e ora di effettuazione di operazioni particolarmente critiche quali stampe, export di dati, accesso a DB, ecc., creazione e disabilitazione di utenti, abilitazione e disabilitazione di profili, modifica di parametri di configurazione. Il log deve esser leggibile, in formato testo , esportabile e separato da altri log di sistema, configurabile in termini di percorso e verbosità.

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, deve garantire che le funzioni d'utente siano distinte e separate da quelle di amministrazione.

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, lo stesso deve garantire che la soluzione non dispone di backdoors o di meccanismi di accesso occulti (non documentati) nemmeno per manutenzione o

controllo. Gli eventuali supporti consegnati a APSS non devono contenere virus, worms, spyware o altri malware. Deve inoltre garantire che la soluzione non trasferisca ad insaputa di APSS dati o informazioni verso il fornitore/produttore né qualsiasi altra destinazione. Il software fornito non deve obbligare APSS al downgrade delle componenti hardware e/o software presenti in APSS.

Qualora il soggetto fornisca programmi software o componenti di sistemi informativi o esercisca trattamenti utilizzando detti programmi e/o sistemi, lo stesso deve garantire che la soluzione non deve presentare vincoli di utilizzo connessi con dispositivi hardware specifici del fornitore o della soluzione, quali ad es. chiavi hardware da porre su interfacce fisiche di server, di client o su apparati di rete o appliances separate.

Qualora il soggetto fornisca attività di teleassistenza utenti o teleassistenza a prodotti, lo stesso deve adeguarsi ai meccanismi tecnici e ai prodotti indicati da APSS e deve seguire le procedure e le modalità operative indicate da APSS.

Qualora il soggetto esercisca trattamenti utilizzando propri sistemi, lo stesso deve tenere e gestire i log degli accessi degli amministratori di sistema secondo quanto indicato dalla normativa vigente e dal Garante. Tali log dovranno essere resi disponibili su richiesta ad APSS.

Qualora il soggetto esercisca trattamenti utilizzando propri sistemi, lo stesso deve accettare di esser sottoposto a penetration test, anche senza preavviso, da parte di APSS o da terze parti da essa incaricate, fermo restando l'impegno di APSS a non generare disservizi al soggetto terzo.

Qualora il soggetto terzo fornisca prodotti software o sistemi o esercisca trattamenti utilizzando propri sistemi, lo stesso deve garantire lo sviluppo ed il test della soluzione in un ambiente diverso e separato rispetto a quello della produzione e a non utilizzare dati personali e/o sensibili reali o di produzione.

Qualora il soggetto esercisca trattamenti utilizzando propri sistemi, lo stesso deve adottare tutte le misure di sicurezza minime ed idonee, comprese quelle indicate da APSS, atte ad impedire accessi non autorizzati ai server, alle postazioni di lavoro, ai dispositivi di rete attraverso i quali il servizio applicativo viene erogato.

7. Disposizioni organizzative

Il soggetto esterno deve individuare e comunicare ad APSS il nominativo del referente ed i suoi riferimenti di contatto con il quale mantenere la comunicazione per ogni eventualità, anche in caso di emergenza.

Qualora il soggetto fornisca servizi ICT o esercisca trattamenti utilizzando propri sistemi, lo stesso deve predisporre, e rendere accessibili ad APSS, un Piano di continuità operativa ed un Piano di disaster recovery per lo meno per gli elementi di servizio correlati al trattamento.

Il soggetto esterno, all'atto della richiesta di connessione alla rete APSS deve:

- comunicare il numero e la tipologia dei posti di lavoro che saranno utilizzati per collegarsi alla rete aziendale di APSS;
- compilare (far compilare) ed eventualmente sottoscrivere i moduli di richiesta di accesso ai trattamenti secondo le modalità previste e comunicate da APSS;
- comunicare il proprio indirizzo completo ed ogni informazione utile per eventuali attività da svolgere presso la sede del soggetto medesimo, compreso l'indirizzo esatto di eventuali sedi interessate dal collegamento;
- usare la connessione per le sole finalità previste nel contratto / convenzione / accordo di servizio, con le modalità e nei limiti indicati da APSS;

comunicare se il collegamento sarà attestato su un singolo Personal Computer o su una rete interna e, nel secondo caso, se la stessa dispone di collegamenti geografici di qualsiasi natura.

Il soggetto esterno, ad esclusione dei fornitori di beni e servizi informatici, per problemi inerenti il collegamento e/o la dotazione strumentale messi a disposizione da APSS, ovvero per guasti, malfunzionamenti, anomalie di funzionamento, ecc. deve avvalersi del servizio di Customer Service Desk (CSD) di Informatica Trentina contattando il numero telefonico 0461 800150. L'orario di servizio per eventuali chiamate di assistenza va dalle ore 8:00 alle ore 17:00 (sabato e festivi esclusi). L'APSS mette a disposizione del soggetto esterno una struttura tecnica di riferimento per garantire la continuità di servizio, il contatto con l'utenza e per disporre le verifiche sulle eventuali segnalazioni.

Il soggetto terzo fornitore di beni e servizi informatici deve avvalersi per eventuali richieste o segnalazioni, del proprio referente interno alla APSS con la quale ha sottoscritto il contratto di fornitura/servizio.

Il soggetto contitolare si impegna a raccogliere sistematicamente ed a gestire il consenso di contatto espresso dai cittadini utenti e si impegna a trasferire detta informazione concomitantemente con il trasferimento dei dati sanitari ad APSS per quelle necessità connesse alla realizzazione del fascicolo sanitario elettronico ed alla corretta comunicazione disciplinata con altri contitolari.

8. Disposizioni comportamentali

Il soggetto esterno una volta connesso alla rete aziendale deve garantire un uso corretto del collegamento secondo le disposizioni impartite da APSS. In particolare non deve navigare o tentare di navigare all'interno della rete aziendale o su siti o di utilizzare servizi ai quali non è espressamente abilitato.

Il soggetto esterno non deve concedere in uso il collegamento ad altri soggetti (che non siano Incaricati designati dallo stesso) salvo espressa autorizzazione di APSS.

Il soggetto esterno non deve installare e/o utilizzare sulla postazione di lavoro cui è attestato il collegamento, software e/o programmi informatici che operino sul collegamento medesimo o che lo impieghino per scopi eccedenti quelli previsti e concordati con APSS.

Il soggetto esterno deve trattare e utilizzare con cura e diligenza le risorse tecnologiche messe a disposizione da APSS. Il soggetto esterno si impegna a non eseguire il caricamento o lo scarico di file musicali, di video, di software peer-to-peer e di qualsiasi software di cui non possieda licenza utilizzando il collegamento messo a disposizione da APSS e la stazione di lavoro ad esso attestata.

Il soggetto esterno si impegna a non immettere nella rete messaggi di spamming in qualsiasi forma né a fare un uso illegale o illegittimo della posta elettronica. Il soggetto esterno si impegna ad usare il collegamento alla rete di APSS esclusivamente per le applicazioni messe a disposizione dalla stessa e per uso professionale.

Le credenziali di autenticazione, costituite normalmente da codici utente (userid) e parole chiave (password), o strumenti di autenticazione, quali smart card o altri dispositivi elettronici, assegnati al soggetto esterno (Conitolare o Responsabile), sono ad uso esclusivo e riservato e non devono essere comunicati o consegnati in nessun caso a soggetti terzi. In caso di sospetto furto o di perdita di credenziali o strumenti di autenticazione – il codice utente o la parole chiave, la smart card o qualunque altro dispositivo utilizzato per l'autenticazione - assegnati all'utenza, il soggetto esterno si impegna a darne tempestiva comunicazione ad APSS.

Il soggetto esterno si impegna a non comunicare e tanto meno a diffondere informazioni che riguardano la dotazione tecnologica di APSS e/o modalità organizzative e procedurali di cui venisse a conoscenza nei rapporti di cooperazione con l'ente.

Il soggetto esterno si impegna a non alterare in alcun modo la configurazione delle componenti hardware e software messe a disposizione da APSS. Eventuali modifiche o aggiornamenti della configurazione hardware e/o software di componenti proprie del soggetto esterno ed utilizzate per il trattamento in qualsiasi forma o modo, anche indiretto, dovranno essere tempestivamente comunicate ad APSS per le verifiche di compatibilità.

Il soggetto esterno, qualora utilizzi il servizio di posta elettronica di APSS o il collegamento di APSS o il sistema telefonico di APSS è inoltre tenuto all'osservanza delle disposizioni contenute nel vigente disciplinare relativo all'accesso ai servizi Internet, di Posta elettronica e di telefonia, in quanto applicabili, che può essere consultato sul sito di APSS o appositamente richiesto al Servizio Affari Generali di APSS.

Gli incaricati del soggetto terzo, qualora operino all'interno delle sedi e delle strutture di APSS, devono qualificarsi al personale di APSS ed essere riconoscibili attraverso l'esposizione di un cartellino identificatore che riporti in modo evidente l'appartenenza al soggetto terzo. L'accesso ai locali e alle strutture aziendali deve essere condizionato al rispetto delle modalità e delle misure di controllo in essere.

9. Disposizioni riguardanti i contenuti informativi

Tra i principi generali contenuti nel Codice privacy assume particolare rilievo il principio di necessità o meglio della "riduzione al minimo" dell'utilizzazione di dati personali e identificativi da parte dei sistemi informativi e dei programmi informatici, in modo da escludere il trattamento quando le finalità perseguite possono essere realizzate mediante dati anonimi o modalità che consentano di identificare l'interessato solo se necessario.

Per quanto riguarda il trattamento dei dati inerenti la salute il Codice privacy impone il rispetto di alcune regole ed in particolare la necessità di verificare puntualmente l'esattezza, la pertinenza, la completezza dei dati trattati ma nel contempo la non eccedenza degli stessi rispetto alle finalità perseguite nei singoli casi.

Nella comunicazione tra APSS e soggetti esterni vanno applicate le misure previste dal disciplinare tecnico allegato B del Codice privacy, ivi comprese quelle aggiuntive per il trattamento dei dati sensibili, sia che il trattamento avvenga con l'ausilio di strumenti elettronici sia che avvenga con l'ausilio di strumenti diversi ed in particolare:

- Separazione dei dati sensibili da quelli anagrafici trasmessi
- Protezione dei dati su supporto magnetico/ottico
- Trasmissione in busta chiusa/pacchi sigillati dei dati su supporto cartaceo
- Comunicazioni per via elettronica tendenzialmente cifrate salvo eccessiva difficoltà tecnico gestionale o onerosità
- Scambio elettronico utilizzando prevalentemente la rete provinciale
- Utilizzo di vettori affidabili (dipendenti APSS o dei soggetti esterni, delle Poste Spa, ecc.).

Il soggetto terzo deve garantire la riservatezza delle informazioni acquisite nello svolgimento delle proprie attività e dei dati con i quali entra in contatto, anche in modo accidentale o fortuito. Dati personali utilizzati per i trattamenti affidati da APSS a soggetti terzi Responsabili del trattamento devono essere mantenuti per il tempo strettamente necessario alla loro lavorazione secondo quanto predisposto o concordato con APSS. E' fatto divieto al soggetto terzo (e ai suoi incaricati) di farne copie, estrazioni, duplicazioni, anche parziali per ragioni non attinenti al trattamento, fatta salva specifica autorizzazione di APSS.

Il formato dei flussi informativi deve essere aderente alle specifiche concordate con APSS.

10. Gestione dell'informativa/consenso

L'art. 76 del Codice privacy disciplina il trattamento dei dati idonei a rivelare lo stato di salute, specificando che tale trattamento per finalità di tutela della salute dell'interessato, di terzi o della collettività da parte di esercenti professioni sanitarie e organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'art. 85 (Compiti del Servizio sanitario nazionale), può avvenire:

a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante se il trattamento riguarda dati e operazioni indispensabili per perseguire finalità di tutela della salute o dell'incolumità fisica dell'interessato;
b) anche senza il consenso dell'interessato e previa autorizzazione del Garante se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

Ai sensi del successivo art. 77 gli organismi sanitari pubblici e privati, gli esercenti le professioni sanitarie e i competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro possono applicare modalità semplificate per informare l'interessato relativamente ai dati raccolti presso il medesimo o presso terzi, per acquisire il consenso al trattamento nei casi in cui ciò è richiesto e per il trattamento dei dati personali; dette modalità semplificate sono individuate negli articoli successivi.

In applicazione delle sopraccitate disposizioni con deliberazione del Direttore Generale n. 1354/2007 di data 21 novembre 2007 venne approvata una procedura per la gestione integrata dell'informativa e del consenso al trattamento dei dati personali per finalità di tutela della salute dell'interessato, con modalità semplificate ai sensi degli artt. 77 e seguenti Codice privacy, basato sulla collaborazione tra APSS, Medici di Medicina generale (MMG) e Pediatri di libera scelta (PLS) per l'acquisizione *una tantum* di un consenso di tipo generale.

Con successiva delibera del Direttore Generale n. 167/2010 del 19 marzo 2010, avente per oggetto le regole per l'accesso ai dati e ai documenti contenuti nel fascicolo sanitario elettronico e la disciplina dell'attività di vigilanza e prevenzione, è stata aggiornata ed integrata la procedura di gestione dell'informativa/consenso con modalità semplificata.

Manifestando il consenso di tipo generale il cittadino può autorizzare il trattamento dei dati inerenti la sua salute sia da parte del proprio medico di fiducia, sia da parte delle strutture dell'APSS, con o senza autorizzazione allo scambio reciproco di informazioni, in particolare prescrizioni e referti, tramite la rete informatica aziendale.

L'"interconnessione" per finalità di cura e di assistenza sanitaria, alla luce del Codice privacy, costituisce un'operazione di "comunicazione" di dati sanitari e richiede il consenso dell'interessato. Tale consenso può intendersi validamente prestato solo se espresso liberamente, in forma specifica e annotato ai sensi dell'art. 81, comma 1 del Codice privacy, oltre che preceduto da idonea informativa. Tale modalità di acquisizione del consenso trova applicazione anche nel caso di pazienti ospiti di RSA/APSP.

I valori che l'interessato può scegliere per esprimere il consenso generale sono i seguenti:

Tabella relativa al CONSENSO PRIVACY GENERALE		
TIPO CONSENSO	SIGNIFICATO	NOTE

0	Negazione totale del consenso	l'eventuale rifiuto a dare il consenso comporta l'impossibilità di ricevere le prestazioni sanitarie (con l'eccezione dei trattamenti urgenti)
3	Consenso rilasciato al MMG/PLS, ai suoi sostituti e associati, all' APSS ed ai soggetti accreditati del SSP. Consente il trattamento dei dati da parte dei singoli attori e il trasferimento dei dati in formato elettronico tra gli stessi (consenso salute)	lo raccoglie sia il MMG/PLS che APSS
5	Consenso rilasciato al MMG/PLS, ai suoi sostituti e associati, all'APSS ed ai soggetti accreditati del SSP. Consente il trattamento dei dati da parte dei singoli attori ma non il trasferimento dei dati in formato elettronico tra APSS, strutture convenzionate e MMG/PLS	lo raccoglie sia il MMG/PLS che APSS

A decorrere dall'1 ottobre 2009 sono state attivate nuove modalità informatiche di acquisizione del consenso in occasione dei singoli contatti del cittadino con le strutture aziendali.

I valori che l'interessato può scegliere per esprimere il consenso per contatto di ricovero, di accesso al Pronto soccorso ed ambulatoriale sono i seguenti:

Tabella relativa al CONSENSO PRIVACY DI CONTATTO		
TIPO CONSENSO	SIGNIFICATO	NOTE
3	Consenso salute, consenso al trattamento dei propri dati sanitari rilasciato all'Azienda Provinciale per i Servizi Sanitari, alle Strutture Sanitarie Convenzionate, al Medico di medicina generale/Pediatra di libera scelta dell'assistito. Tale tipo di consenso consente il trattamento dei dati da parte dei singoli attori ed il trasferimento dei dati in formato elettronico tra gli stessi	
5	Consenso ad APSS e Strutture Convenzionate, consenso al trattamento dei propri dati sanitari rilasciato all'Azienda Provinciale per i Servizi Sanitari, alle Strutture Sanitarie Convenzionate, autorizza l'accesso ai dati sanitari in formato elettronico ai soggetti sopra indicati	Rispetto al consenso di valore 3 esclude la comunicazione al proprio medico di medicina generale/pediatra di libera scelta
6	Consenso alla Struttura Erogante, consenso al trattamento dei propri dati sanitari alla sola Struttura Erogante (APSS o Struttura convenzionata) che interviene nel percorso assistenziale; NON autorizza l'accesso ai dati sanitari in formato elettronico ad altre strutture sanitarie ed ai medici di medicina generale/pediatri di libera scelta	E' il valore di consenso più restrittivo

7	Consenso a Strutture Eroganti e MMG/PLS, consenso al trattamento dei propri dati sanitari alla Struttura Erogante (APSS o Struttura convenzionata) e al medico di medicina generale/pediatra di libera scelta dell'assistito, autorizza l'accesso ai dati sanitari in formato elettronico ai soggetti sopra indicati	

Per le strutture accreditate, fermo restando l'obbligo di fornire al paziente idonea informativa e raccogliere il consenso specifico al trattamento dei dati personali, nel caso il cittadino abbia già dato il "consenso generale" quest'ultimo può essere acquisito come consenso di contatto anche se può essere modificato a discrezione del paziente.
In assenza di "consenso generale", viene richiesto obbligatoriamente un consenso per ogni contatto di ricovero e ambulatoriale con la struttura accreditata.
Per le modalità di oscuramento dei dati e le altre modalità di gestione dei dati inerenti la salute del cittadino valgono le regole vigenti presso APSS per il trattamento SIO Sistema Informativo Ospedaliero contenute nel documento allegato alla deliberazione del Direttore Generale n. 297/2009 di data 4 marzo 2009, aggiornato con deliberazione n. 167/2010 di data 19 marzo 2010 e successive modifiche e integrazioni.

Codice in materia di protezione dei dati personali
B. Disciplinare tecnico in materia di misure minime di sicurezza
(Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell´incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l´identificazione dell´incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell´incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell´incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l´autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell´incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all´incaricato ed è modificata da quest´ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l´identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all´incaricato l´accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l´accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l´autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell´incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l´incaricato dell´intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all´inizio del trattamento, in modo da limitare l´accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza
15. Nell´ambito dell´aggiornamento periodico con cadenza almeno annuale dell´individuazione dell´ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di

incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell´azione di programmi di cui all´art. 615-*quinquies* del codice penale, mediante l´attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l´aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. [soppresso] (1)

19.1. [soppresso](1)
19.2. [soppresso](1)
19.3. [soppresso](1)
19.4. [soppresso](1)
19.5. [soppresso](1)
19.6. [soppresso](1)
19.7. [soppresso](1)
19.8. [soppresso](1)

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l´accesso abusivo, di cui all´art. 615-*ter* del codice penale, mediante l´utilizzo di idonei strumenti elettronici.
21. 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.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono 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 a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all´articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all´identità genetica sono trattati esclusivamente all´interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all´esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall´installatore una descrizione scritta dell´intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. [soppresso] (1)

Trattamenti senza l´ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell´incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l´intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell´ambito dell´aggiornamento periodico con cadenza almeno annuale dell´individuazione dell´ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono

controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L´accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l´orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

(1) Paragrafi soppressi dall´art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

Per completezza, si riporta di seguito il testo dei paragrafi soppressi.

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l´elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell´ambito delle strutture preposte al trattamento dei dati;
19.3. l´analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l´integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire 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 minime adottate dal titolare. La formazione è programmata già al momento dell´ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l´adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all´esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l´individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell´interessato.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d´esercizio, se dovuta, dell´avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.