Antonio Cardarelli
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA DEI DATI

Il presente DPS è stato redatto ai sensi del D.Lgs. 196/2003

Ultimo aggiornamento notificato in data 18-04-2013

Titolare del Trattamento dei Dati
Il Direttore Generale

Indice

Premessa

1.1. Quadro normativo di riferimento, da pag. 4 a pag. 7

1.2 Ambito di applicazione , da pag. 7 a pag. 9

1.3 Soggetti che effettuano il trattamento, da pag. 9 a pag. 11

1.4 Misure logiche ed organizzative, da pag. 11 a pag. 13

1.5 Elencazione delle azioni e procedure privacy attivate, da pag. 13 a pag. 16

1.6 Modello di gestione dei trattamenti dei dati, da pag. 17 a pag. 22

1.7 Metodologia di rilevazione del patrimonio informativo, da pag. 22 a pag. 24

1.8 La classificazione dei trattamenti dei dati, da pag. 24 a pag. 29

1.9 Accesso ai data base della rete aziendale per fini istituzionali da pag. 29 a pag 34

"Regolamento per una corretta gestione degli archivi informatici e delle apparecchiature informatiche" redatto ed aggiornato a cura del Servizio Informatico aziendale.

Fonte normativa : D.Lgs 196/2003 (Codice in materia di protezione dei dati personali)

Allegati

- Modelli recanti gli Atti di nomina: del Sostituto del Responsabile del trattamento; degli Incaricati
- Scheda n° 17 recante la denominazione del trattamento: "Attività amministrativa, programmatoria, gestionale, relativa all'assistenza in regime di ricovero ospedaliero"
- Scheda n° 20 recante la denominazione del trattamento: "Soccorso sanitario di emergenza. Sistema 118. Assistenza sanitaria di emergenza"
- Scheda n° 22 recante la denominazione del trattamento: "Trapianti"
- Scheda n° 41 recante la denominazione del trattamento: "Videosorveglianza con finalità di sicurezza e protezione dei beni e delle persone"
- Scheda 54 recante la denominazione del trattamento: "Gestione delle Risorse Umane"
- Scheda n° 50 recante la denominazione del trattamento: "Gestione del Fondo economale. Acquisizione di Beni e Servizi"
- Scheda B per la ricognizione delle Banche dati standardizzata
- Scheda C per la rilevazione delle misure di sicurezza adottate per la protezione delle banche dati standardizzata
- Informativa all'Assistito in materia di protezione dei dati personali
- Modello per acquisire il consenso al trattamento dei dati da parte dell'interessato
- Informativa al Personale dipendente in materia di protezione dei dati personali

Premessa

La privacy regola l'osservanza del principio di riservatezza che è un diritto inviolabile dell'individuo ed un valore civile a tutela della collettività.

La tutela della privacy, che è finalizzata alla protezione dei dati personali, è normata dal D.lgs 196 del 2003. Il legislatore, al fine di favorire un corretto trattamento dei dati personali e di assicurare l'osservanza delle misure che attuano il dettato normativo, ha fornito esplicite indicazioni in materia di protezione dei dati personali ed ha prescritto l'individuazione di profili con funzioni organizzative ed operative degli interventi finalizzati a garantire un corretto trattamento dei dati personali, prestando particolare attenzione alle strutture sanitarie pubbliche o private. I soggetti che rivestono tali profili sono rispettivamente: il Titolare del trattamento, il Responsabile del trattamento, l'Incaricato del trattamento.

La responsabilità giuridica rivestita dal Titolare del trattamento e gli oneri organizzativi derivanti dall'ottemperanza della normativa, hanno comportato lo sviluppo di un settore di attività incaricato di curare le procedure aziendali in materia di protezione dei dati personali. A tal fine, è operante, nell'ambito della UOSD Ufficio Relazioni col Pubblico e Marketing sanitario, il settore privacy aziendale che assolve il compito di monitorare l'osservanza della privacy aziendale attraverso la promozione costante di una policy sulla sicurezza dei dati, condivisa e diffusa.

1.1 Quadro normativo di riferimento

Il vigente Codice sulla protezione dei dati personali ha perfezionato la disciplina in materia di sicurezza nel trattamento dei dati, rispetto alla precedente Legge 675/96. Infatti, esso attribuisce maggiore rilevanza giuridica al dettato concernente l'osservanza delle "misure minime" di sicurezza. E' uopo, precisare che la non osservanza delle misure minime di sicurezza finalizzate alla tutela dei dati sensibili rende il trattamento illecito, pur non cagionando un danno diretto agli interessati, in quanto espone il

Titolare del trattamento alla violazione delle indicazioni normative che garantiscono la protezione dei dati personali.

In tal senso, il Dlgs 196/03 afferma il principio secondo cui l'omessa adozione delle misure indispensabili o "minime", le cui modalità sono dettate dagli artt. 31, 33, 34 e 35 del suddetto Codice, "*costituisce anche reato"* ai sensi dell'art. 169 del Codice. Il reato di omissione prevede, generalmente, un'ammenda da 10 mila euro a 50 mila euro, nonchè il ravvedimento operoso per chi adempie alle prescrizioni impartite dal Garante, una volta accertato il reato ed effettuato un pagamento in sede amministrativa per ottenere l'estinzione del reato.

Il decreto legge n. 5 del 9 febbraio 2012, convertito in legge il 4 aprile 2012, che reca *"Disposizioni urgenti in materia di semplificazione e di sviluppo*", con l'art. 45 recante *"Semplificazioni in materia di dati personali"* abroga nel Disciplinare tecnico del D.lgs 196/03 i paragrafi da 19 a 19.8 e 26 i quali dettano l'obbligo di redigere il Documento programmatico della sicurezza dei dati.

Tuttavia, alla luce dell'incremento delle attività di gestione delle informazioni istituzionali eseguite utilizzando la rete e, quindi, considerata la potenziale esposizione ai rischi derivanti da eventuali inadempienze dell'osservanza delle misure di sicurezza in materia privacy, il proponente del presente rapporto, su indicazione del Titolare del trattamento, redige il documento in epigrafe con l'intento di definire le procedure atte all'ottemperanza delle indicazioni normative dettate dagli artt. 31, 33, 34 e 35 del D.lgs 196/03 e specificate nel Disciplinare tecnico del predetto Codice.

Il dettato normativo che richiede l'obbligo da parte del Titolare di verificare l'osservanza degli adempimenti che attengono alle misure di sicurezza nel trattamento dei dati è il seguente:

1. L'art. 31 del D.lgs. n. 196/2003 stabilisce che i dati personali oggetto di trattamento devono essere custoditi e protetti, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

2. L'art. 33 del D.lgs. n. 196/2003 stabilisce che, i Titolari del trattamento sono comunque tenuti ad adottare le "misure minime" individuate nel capo II o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

3. L'art. 34 del D.lgs. n. 196/2003 stabilisce che, qualora il trattamento di dati sensibili sia realizzato mediante strumenti elettronici, devono essere rispettate le misure minime previste dal disciplinare tecnico contenuto nell'allegato B della predetta norma. In epoca antecedente alla emanazione della legge n. 35 del 4 aprile 2012 esisteva anche l'obbligo di aggiornare con cadenza annuale il documento programmatico sulla sicurezza dei dati. Tuttavia, alla luce del recente incremento delle attività organizzative ed assistenziali che si esplicano utilizzando la rete aziendale, si impone l'esigenza di vigilare sui criteri di sicurezza che consentono l'analisi dei rischi ed individuano le varie responsabilità nell'ambito delle strutture operative deputate al trattamento dei dati stessi. L'ottemperanza dell'art. 34 prevede l'adozione delle seguenti misure:

a) i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
b) i criteri e le procedure per assicurare l'integrità dei dati;
c) i criteri e le procedure per la sicurezza delle trasmissione dei dati, ivi compreso quelli per le restrizioni d'accesso per via telematica;
d) protezione degli strumenti elettronici dall'aggressione di agenti che possono danneggiare le banche dati

4. L'art. 35 del D.lgs. n. 196/2003 regola i "trattamenti senza l'ausilio di strumenti elettronici" e stabilisce che il trattamento dei dati personali effettuato senza l'ausilio di strumenti elettronici è consentito se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B, le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati nell'ambito delle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti e disciplina delle modalità di accesso degli incaricati.

5. Il Disciplinare tecnico o Allegato B del D.lgs. n. 196/2003, che indica le varie misure di sicurezza da ottemperare per effettuare, senza incorrere in violazioni, il trattamento dei dati automatizzati. Esso racchiude una serie di indicazioni o di regole finalizzate alla liceizzazione dei trattamenti effettuati mediante strumenti elettronici.

1.2 Ambito di applicazione

Nel presente documento sono definite le modalità di trattamento dei dati e le misure di sicurezza adottate dall'Azienda ospedaliera "A.Cardarelli" di Napoli, in ottemperanza a quanto disposto dagli artt. 31, 33, 34, 35 del Dlgs 196/03 e dal Disciplinare tecnico dello stesso Codice. Le misure di sicurezza dei dati prese in esame potranno essere oggetto di monitoraggio periodico e gli obiettivi di miglioramento connessi al trattamento dei dati dovranno ridurre al minimo:

- l'inadempienza degli obblighi di protezione dei dati personali,
- i rischi di distruzione e perdita dei dati,
- l'accesso non autorizzato ai medesimi,
- il trattamento non consentito e non conforme alla norma,
- il trattamento non pertinente ed eccedente alle finalità d'istituto.

Gli interventi organizzativi e tecnico-strumentali in materia di protezione dei dati personali atti a prevenire, contrastare e/o ridurre i rischi, che possono cagionare

eventuali violazioni, saranno soggetti ad una costante rimodulazione dettata dalle esigenze e dai cambiamenti del contesto strutturale ed organizzativo.

L'analisi del livello di conformità alla norma prende in esame tutte le tipologie di trattamento dei dati che l'Azienda "Cardarelli" rileva nell'esercizio delle sue funzioni istituzionali. I dati personali trattati in ambito sanitario sono, in massima parte, idonei a rivelare lo stato di salute degli utenti che fruiscono di prestazioni sanitarie e, per questa connotazione, assumono il carattere di dati sensibili ai sensi dell'art. 26 del Dlgs 196/03. Tuttavia, le aziende sanitarie trattano i dati personali e sensibili anche di categorie di interessati che non sono pazienti ed assistiti.

Infatti, le finalità del trattamento dei dati in ambito sanitario derivano anche da compiti istituzionali correlati allo svolgimento di funzioni di gestione della struttura nel suo complesso, quali il rapporto con altri enti, con i fornitori e, soprattutto, con il personale dipendente.

Le tipologie dei dati trattati secondo le finalità concernenti la gestione delle risorse strutturali ed umane dell'azienda, generalmente, riguardano:

- i dati inerenti al trattamento economico, giuridico e previdenziale delle risorse umane,
- i dati che regolano l'acquisizione di beni e servizi, nonchè la gestione economica finanziaria delle risorse,
- i dati che rilevano le risorse patrimoniali dell'azienda e gli interventi manutentivi,
- i dati inerenti all'accesso degli atti amministrativi e dei protocolli in entrata, dati che regolano i rapporti con enti terzi,
- i dati che regolano l'accesso alle prestazioni concernenti gli atti ed i referti clinici, le schede di dimissione ospedaliera, i dati che attengono alla gestione delle cartelle cliniche,
- i dati che verificano l'appropriatezza degli interventi organizzativi attraverso il controllo di gestione delle risorse, i dati che indicano il rispetto degli standard dei servizi nell'ambito delle strutture sanitarie ed i dati connessi alle attività di informazione e comunicazione istituzionale nel rapporto col pubblico.

Il trattamento dei dati può essere esplicato in forma automatizzata ed in forma non automatizzata la diversa tipologia di trattamento è contemplata rispettivamente dagli artt. 34 e 35 del Dlgs 196/03.

Il trattamento non automatizzato si riferisce alla raccolta, registrazione, archiviazione, dei dati con metodi che utilizzano supporti e strumenti cartacei. In tal caso, la puntuale custodia e la corretta archiviazione degli atti contenenti i dati deve rispecchiare le indicazione contenute nell'art. 11 del D.lgs 196/03

Il trattamento automatizzato dei dati, invece, si effettua con strumenti elettronici ed impone la protezione delle informazioni raccolte e delle banche dati. Comporta, pertanto, l'applicazione di dispositivi atti a contrastare l'intrusione di agenti presenti nella rete che potrebbero danneggiare i dati, compromettendo le procedure di trattamento degli stessi nonché la corretta conservazione delle informazioni raccolte nei "data base".

Entrambe le suindicate tipologie di trattamento dei dati devono rispettare le indicazioni normative dettate dagli artt. 31, 33, 34 e 35 del Codice in materia di protezione dei dati personali, nonchè le regole contemplate dal Disciplinare tecnico per quanto riguarda il trattamento dei dati effettuato con strumenti elettronici.

Le indicazioni contenute nel presente documento sono state aggiornate con cadenza annuale, in esito alla verifica delle misure di sicurezza in esso determinate ed in relazione al dettato contenuto nel disciplinare tecnico del D.lgs 196/03.

1.3 Soggetti che effettuano il trattamento

Il Codice in materia di tutela della privacy, al fine di favorire una gestione dei dati personali il più possibile pertinente e funzionale, individua i soggetti che effettuano il trattamento attribuendovi un profilo funzionale a cui corrisponde una differente responsabilità organizzativa ed esecutiva nell'esercizio del trattamento dei dati.

I soggetti che effettuano il trattamento sono :

- il Titolare del trattamento,
- il Responsabile del trattamento,
- l'Incaricato del trattamento.

Il Titolare del trattamento dei dati, ai sensi dell'art. 28 del Dlgs 196/03, è la persona fisica dotata di personalità giuridica che esercita il potere decisionale sulle finalità e le modalità del trattamento dei dati nel rispetto della norma vigente. Il Titolare del trattamento dell'Azienda Cardarelli è il Direttore Generale. Egli risponde, anche in sede penale, di eventuali illeciti e/o violazioni amministrative che la norma cita al titolo III del Codice facendo un'elencazione di tutte le possibili violazioni amministrative e delle rispettive sanzioni pecuniarie che sono cagionate da trattamenti illeciti o da omissioni delle prescrizioni indicate nel Dlgs 196/03.

Il Responsabile del trattamento, ai sensi dell'art. 29 del Codice, è la figura designata dal Titolare del trattamento, dotata di responsabilità organizzativa ed individuata tra soggetti che, per esperienza capacità ed affidabilità, forniscano idonea garanzia di rispetto della normativa in materia di privacy, ivi compreso il profilo della sicurezza.

Nell'Azienda Cardarelli i Responsabili del trattamento dei dati sono i Coordinatori – referenti di dipartimento per l'area sanitaria ed i Direttori di Struttura operativa complessa ovvero di Direzione funzionale amministrativa per l'area amministrativa. La designazione del profilo di Responsabile del trattamento ai professionisti rispettivamente dell'area sanitaria ed amministrativa è stata acclarata dal Titolare del trattamento, in primis, con la delibera n. 42 del 24 gennaio 2011 recante il Documento Programmatico della Sicurezza dei Dati

I precedenti D.P.S. hanno declinato le misure organizzative in materia di privacy sulla base dell'organizzazione dipartimentale in attuazione al decreto commissariale della Regione Campania n. 49 del 27-09-2010. L'attribuzione del ruolo di Coordinatore-referente di Dipartimento prevede, su esplicita indicazione del Titolare del trattamento, il riconoscimento della funzione di Responsabile del trattamento. Pertanto, si indica nel presente documento lo schema organizzativo illustrato nel "Report dei processi e dei profili organizzativi" che contempla l'elencazione dei Dipartimenti sanitari e dei

rispettivi Coordinatori nonchè delle Direzioni funzionali amministrative a struttura complessa e dei rispettivi Dirigenti di II livello, i quali assolvono specificatamente la funzione di Responsabili del trattamento.

Il Responsabile del trattamento pone in essere le misure organizzative in materia di sicurezza dei dati e può nominare, nell'area sanitaria, uno o più Sostituti del Responsabile al fine di ottimizzare la gestione degli interventi in materia di privacy ed allo scopo di segmentare le responsabilità, tenuto conto delle articolazioni complesse e multidisciplinari dei dipartimenti.

L'Incaricato del trattamento, ai sensi dell'art. 30 del Dlgs 196/03, è la persona che assolve gli adempimenti inerenti al trattamento dei dati nell'osservanza della normativa e delle indicazioni impartite dal Titolare e/o dal Responsabile del Trattamento.

L'Incaricato è designato per iscritto dal Responsabile del trattamento ed è tenuto a rispettare la riservatezza e ad osservare le procedure che assicurano il profilo della sicurezza dei dati che vengono trattati con gli strumenti elettronici .

1.4 Misure logiche ed organizzative

Gli adempimenti amministrativi ed organizzativi che regolano, in ambito sanitario, la gestione delle procedure e degli atti in materia di privacy risultano essere onerosi e complessi, soprattutto, se l'azienda sanitaria è di vaste proporzioni.

L'Azienda Cardarelli ha intrapreso, a partire dall'anno 2001, le prime azioni finalizzate alla tutela della privacy in osservanza alla legge 675/96. Le procedure attivate, in epoca antecedente e successiva all'emanazione del Dlgs 196/03, sono tutte menzionate nel paragrafo che segue. E', tuttavia, importante sottolineare che buona parte degli interventi posti in essere dal settore operativo che gestisce la privacy aziendale costituiscono, in ottemperanza della normativa, le misure logiche ed organizzative che sono basilari per l'adozione delle misure di sicurezza contemplate dagli artt. 31 e 33 del Codice sulla protezione dei dati personali.

Gli interventi e le procedure che attengono alle misure logiche ed organizzative sono le seguenti::

- Designazione dei Responsabili del trattamento: art. 29 del Dlgs 196/03.
- Designazione degli Incaricati del trattamento: art. 30 del medesimo decreto.
- Informativa agli utenti sulle finalità e le modalità di trattamento dei dati, ai sensi dell'art. 13 del Dlgs 196/03, che può essere fornita come parte integrante della cartella clinica e/o essere somministrata anche in formato pubblicitario ovvero affissa nei luoghi di maggiore afflusso dell'utenza. L'omissione dell'Informativa agli interessati costituisce, ai sensi dell'art. 161 del Codice, una violazione punibile con una sanzione amministrativa che comporta il pagamento di una somma che varia da tremila a diciottomila euro.
- Espressione del consenso dell'interessato al trattamento dei dati che lo riguardano, ai sensi dell'art. 23 del Dlgs 196/03. I dati sensibili richiedono l'acquisizione del consenso per iscritto da parte dell'interessato. Tuttavia, in ambito sanitario, l'acquisizione del consenso dell'interessato al trattamento dei dati può essere facoltativa, in quanto "*per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato"* (art. 18 comma 4). Ciononostante, per motivi di carattere cautelativo il modello di acquisizione del consenso al trattamento dei dati è parte integrante della cartella clinica.
- Notificazione al Garante (artt. 37-38 del Dlgs 196/03) che consiste in una comunicazione ufficiale che il Titolare del trattamento inoltra al Garante per la protezione dei dati personali. Essa indica la ragione sociale dell'ente, la tipologia dei dati trattati, le finalità e le modalità di trattamento dei dati che costituiscono il patrimonio informativo dell'Azienda. L'omissione dell'atto di notificazione al Garante, ai sensi dell'art. 163 del Codice, può comportare una sanzione amministrativa che cagiona il pagamento di sessantamila euro. La notificazione è obbligatoria e può essere effettuata "una tantum".
- Formazione del personale rivolta sia ai Responsabili del trattamento che agli Incaricati. La formazione del personale, che è prescritta dal Disciplinare tecnico nel

paragrafo dedicato al Documento programmatico della sicurezza, nell'azienda Cardarelli è stata effettuata a partire dall'anno 2004 fino all'anno 2009

- I Regolamenti e le informative aziendali che indirizzano i comportamenti dei Responsabili e degli Incaricati dei trattamenti, in materia di protezione dei dati personali.
- Il "Regolamento per una corretta gestione degli archivi informatici, delle apparecchiature informatiche e degli archivi cartacei" che è stato redatto a cura del Servizio Informatico aziendale in data 31.03.2007 e, successivamente, soggetto ad un aggiornamento periodico
- Il Documento programmatico della sicurezza dei dati che è stato redatto ed approvato in data 24-01-2011 con delibera n. 42 e, successivamente, aggiornato ed approvato con delibera n. 297 del 20 aprile 2012.

A seguito della emanazione del decreto legge n. 5 del 9 febbraio 2012 convertito in legge il 4 aprile 2012 e recante "Disposizioni urgenti in materia di semplificazione di sviluppo", il documento programmatico della sicurezza dei dati è stato abrogato.

1.5 Elencazione delle azioni e procedure attivate in materia di privacy

Nell'ottica di documentare la realizzazione delle suddette procedure, si elencano, di seguito, le azioni e gli interventi esplicati in materia di protezione dei dati personali dal settore che coordina la privacy aziendale, nell'esercizio delle funzioni istituzionali esplicate dall'U.R.P.:

1) Individuazione dei Responsabili del trattamento dei dati ed approvazione del primo regolamento aziendale ai sensi della Legge 675/96

2) Prima notificazione del trattamento dei dati inoltrata al Garante, elaborata ai sensi della Legge 675 /96

3) Adozione del Manuale in applicazione del regolamento aziendale sulla tutela della privacy, redatto ai sensi della Legge 675/96. Nomina del Referente Privacy aziendale e riconferma dei Responsabili del trattamento

4) Adozione standardizzata del modello di informativa all'utente sulle finalità e le modalità di trattamento dei dati e del modello di acquisizione del consenso al trattamento dei dati personali, entrambi resi parte integrante della cartella clinica (ai sensi della L. 675/96).

5) Atto di nomina degli Incaricati da parte dei Responsabili del trattamento. Notifica e rilevazione dei suddetti atti di nomina (ai sensi della L. 675/96)

6) Informativa formulata il personale dell'Azienda con l'indicazione delle procedure e dei comportamenti da adoperare per tutelare la privacy dei pazienti e proteggere i dati personali

7) Revisione della preesistente modulistica, adottata ai sensi della L. 675/96, ai fini della modifica apportata in osservanza al Dlgs 196/03.

8) Attivazione sul portale aziendale della web page: *Ufficio Privacy aziendale*, consultabile al link *"Privacy"*. E' possibile prendere visione, consultando la web page "Privacy", delle procedure e delle misure adottate dall'Azienda a tutela dei dati personali.

9) Accreditamento in ECM e realizzazione del primo progetto formativo aziendale sulla tutela della privacy nelle Aziende sanitarie per Responsabili del trattamento dei dati (anno 2004).

10) Redazione del primo Documento Programmatico della Sicurezza dei dati, approvato con atto deliberativo nel luglio 2005

11) Seconda notificazione al Garante per la protezione dei dati, redatta ai sensi del Dlgs 196/03 (luglio 2005)

12) Approvazione e divulgazione del Regolamento aziendale attuativo sulla tutela della privacy, adottato ai sensi del Dlgs 196/03, deliberato nell'anno 2006.

13) Formazione in ECM sulla tutela della privacy per il personale dell'area sanitaria e tecnico-amministrativa che riveste le funzioni di incaricato del trattamento: n° 5 edizioni nell'anno 2005

14) Prosieguo dei corsi di formazione in ECM sulla tutela della privacy per il personale dell'area sanitaria e tecnico-amministrativa che riveste le funzioni di incaricato del trattamento: n° 11 edizioni nell'anno 2006 e 2 edizioni nell'anno 2007

15) Affiancamento progettuale nella redazione del "Regolamento per una corretta gestione degli archivi informatici, delle apparecchiature informatiche e degli archivi cartacei", redatto dal Dirigente del Servizio Informatico aziendale in data 31.03.2007.

16) Redazione di un opuscolo contenente una dettagliata informativa sulle modalità di tutela della privacy aziendale, realizzata a cura dell'Ufficio Relazioni col Pubblico ed adottata come strumento di formazione sulla normativa in materia di privacy sanitaria.

17) Formazione in ECM sulla tutela della privacy per il personale dell'area sanitaria e tecnico-amministrativa che riveste le funzioni di incaricato del trattamento: 16 edizioni nel 2008

18) Formazione in ECM sulla tutela della privacy per il personale dell'area sanitaria e tecnico-amministrativa che riveste le funzioni di incaricato del trattamento: 12 edizioni nel 2009.

19) Rilevazione degli atti di nomina degli Incaricati del trattamento designati dai Responsabili del trattamento, sia dell'area sanitaria che amministrativa (anno 2010)

20) Rimodulazione dei modelli di Informativa e di acquisizione del consenso da parte dell'interessato, che sono parte integrante della cartella clinica (anno 2010)

21) Produzione, in formato manifesto, di una Informativa all'assistito sulle finalità e le modalità di trattamento dei dati da affiggere nei luoghi di maggior accesso degli utenti.

22) Redazione del Documento Programmatico della Sicurezza dei Dati approvato con delibera n. 42 del 24-01-2011

23) Pubblicazione del Documento Programmatico della Sicurezza dei Dati sul portale dell'Azienda Cardarelli consultabile alla web page "Privacy"

24) Aggiornamento del Documento Programmatico della Sicurezza dei Dati approvato con delibera n. 297 del 20 aprile 2012

25) Rilevazione delle procedure che consentono la interconnessione delle banche dati mediante il sistema di accesso "order entry"

Gli atti, che attengono agli interventi suelencati, sono reperibili presso l'Ufficio Relazioni col Pubblico, nel cui ambito opera il settore di attività dedicato alla tutela della privacy aziendale.

La pianificazione delle attività finalizzate alla protezione dei dati personali si sviluppa monitorando le azioni ed il loro grado di efficacia perseguendo i seguenti obiettivi:

- vigilando sull'ottemperanza delle indicazioni normative e delle direttive aziendali dirette alla protezione dei dati personali,
- rilevando le modalità di osservanza delle misure fisiche, logiche ed organizzative che garantiscono la tutela della privacy in ambito sanitario,
- formando periodicamente il personale dell'Azienda sulle responsabilità connesse alle relative funzioni in materia di privacy,
- effettuando un monitoraggio periodico delle misure minime di sicurezza.

In epoca antecedente al decreto legge n. 5 del 09-02-2012 recante "Disposizioni urgenti in materia di semplificazione e di sviluppo" esisteva l'obbligo di redazione del Documento programmatico della sicurezza dei dati entro e non oltre il 31 marzo di ogni anno.

1.6 Modello di gestione dei trattamenti dei dati

La metodologia adottata per la valutazione dei rischi inerenti alla sicurezza dei dati prevede innanzitutto l'adozione di un modello che rispecchi l'assetto organizzativo e funzionale dell'Azienda, con l'indicazione di "Chi fa cosa", sia in termini di responsabilità che di operatività nel trattamento dei dati.

In questo documento programmatico, che descrive le modalità di trattamento dei dati, sono state rilevate le informazioni più rilevanti e rappresentative della realtà aziendale a cui vanno ascritte le misure di sicurezza senza, peraltro, pretendere l'esaustività nella rilevazione delle variabili, considerata la complessità e le grandi dimensioni della struttura ospedaliera "A. Cardarelli"

Il Documento programmatico della sicurezza dei dati, si sviluppa confrontando lo stato di conformità delle procedure connesse al trattamento dei dati personali alla norma, che impone regole tecniche e comportamentali a tutti coloro che gestiscono i dati ed il patrimonio informativo di un ente.

Esso è ispirato a tre principali direttive finalizzate all'analisi conoscitiva:

- la rilevazione dell'organizzazione e degli elementi che caratterizzano il patrimonio informativo aziendale;
- il riscontro delle disposizioni di legge sulla base dell'analisi dello stato di conformità;
- l'identificazione delle aree di intervento e delle principali azioni conseguenti.

Il report dei processi e dei profili organizzativi, qui di seguito indicato, rappresenta, in maniera schematica, l'assetto funzionale ed organizzativo dell'Azienda in ottemperanza alle direttive interne in materia di privacy, con riferimento alle risorse umane che esplicano la funzione di Responsabili e di Incaricati del trattamento dei dati.

Per Referente organizzativo di un struttura operativa si intende il Responsabile del trattamento dei dati. Egli stabilisce le modalità operative dei trattamenti dei dati nell'ambito della struttura o dell'area funzionale che coordina, in base alla normativa vigente ed alle direttive aziendali. Sono, pertanto, indicati i nominativi dei Dirigenti

delle Strutture complesse amministrative e dei Coordinatori-referenti dell'area sanitaria nominati con delibera n. 761 del 29-11-2010 i quali, in epoca antecedente al presente documento, già assolvevano la funzione di Responsabili del trattamento limitatamente alla struttura complessa che dirigevano e che dirigono tuttora.

Per Organizzazioni operative si intendono le risorse strutturali ed organizzative coinvolte nel trattamento dei dati in termini di operatività ovvero, nella fattispecie, le risorse umane preposte ai trattamenti dei dati che assolvono la funzione di Incaricati del trattamento.

Report dei processi e dei profili organizzativi

Processo	Sottoprocessi	Trattamenti	Referente Organizzativo	Organizzazioni Operative
Gestione dell'Area delle Direzioni Amministrative e di staff alla D.G.	Attività afferenti all'area funzionale amministrativa e di staff alla D.G.	Trattamento di dati concernenti la gestione dei piani di utilizzo delle risorse umane, strutturali ed economiche aziendali	Direttore Generale: Avv. Rocco Granata Titolare del trattamento	Ufficio di Direzione Generale Personale Incaricato
		Trattamento di dati concernenti le attività del Collegio Sindacale e del Collegio di Direzione, interpellanze di Organi istituzionali esterni	Dirigente della UOSC Segretaria Generale, Capo Gabinetto e Coordinatrice degli Uffici in staff Dott.ssa Anna Iervolino Responsabile del trattamento	Segreteria Generale Personale Incaricato
		Trattamento dei dati che attengono alle attività di informazione e comunicazione istituzionale. Applicazione del Regolamento di pubblica tutela, rapporti con Associazioni di volontariato. Gestione del Settore Privacy aziendale	Dirigente (FF) della UOSD Ufficio Relazioni col Pubblico e Marketing sanitario, in qualità di Coordinatrice degli Uffici in staff Dott.ssa Anna Iervolino Responsabile dei procedimenti a tutela della privacy aziendale nell'ambito della Direzione strategica ed amministrativa, in qualità di Referente Privacy aziendale: Dott.ssa Maria Perillo	Ufficio Relazioni col Pubblico e Marketing sanitario Personale Incaricato

Processo	Sottoprocessi	Trattamenti	Referente Organizzativo	Organizzazioni Operative
		Messa in sicurezza della rete LAN aziendale Super visor dei sistemi operativi di gestione che vengono impiegati utilizzando la rete aziendale Elaborazione ed archiviazione dei cedolini di pagamento del personale	Dirigente del Servizio Informatico aziendale: Dott. Pasquale Indizio Responsabile del trattamento	Servizio Informatico aziendale Personale Incaricato
		Trattamento di dati concernenti le attività in materia di prevenzione e della sicurezza sul lavoro delle risorse umane dell'Azienda	Dirigente del Servizio di Prevenzione e protezione: Dott. Rosario Di Mizio Responsabile del trattamento	Servizio di Prevenzione e Protezione aziendale. Personale Incaricato
		Trattamento dei dati concernenti la gestione degli affari generali, i rapporti con le Assicurazioni, con enti terzi, gestione del Protocollo generale	Dirigente UOSC Affari Generali: Dott.ssa Anna Iervolino Responsabile del trattamento	Ufficio Affari Generali Personale Incaricato
		Trattamento dei dati concernenti il controllo di gestione: schede di valutazione dei dirigenti, del personale del comparto, controllo di gestione delle risorse e delle attività erogate	Dirigente UOSC Controllo di Gestione Dirigente: Dott.ssa Vera Giuliano Responsabile del trattamento	Ufficio Controllo di Gestione. Personale Incaricato
		Trattamento dei dati inerenti alla gestione di contenziosi in materia legale, istanze di ricorso, cause di risarcimento, patrocini legali	Dirigente UOSC Affari Legali, Dirigente: Dott.ssa Vera Giuliano Responsabile del trattamento	Ufficio Affari Legali Personale Incaricato

Processo	Sottoprocessi	Trattamenti	Referente Organizzativo	Organizzazioni Operative
		Trattamento di dati concernenti l'acquisizione di beni e servizi, dati concernenti l'esecuzione dei bandi di gara per gli acquisti	Dirigente UOSC Acquisizione di Beni e Servizi: Dott. Ciro Verdoliva Responsabile del trattamento	Ufficio Acquisizione di Beni e Servizi Personale Incaricato
		Trattamento dati per la gestione economico finanziaria delle risorse finanziarie e creditizie. Gestione bollettario pagamenti ALPI Gestione crediti e pagamenti	Dirigente UOSC Gestione delle risorse economico-finanziarie e della contabilità Dott. Felice Capece (f.f.) Responsabile del trattamento	Ufficio per la Gestione delle risorse economiche e finanziarie e della contabilità. Personale Incaricato
		Trattamento di dati relativi ai rapporti con società ed enti terzi per la manutenzione, trattamento di dati concernenti il patrimonio strutturale aziendale	Dirigente UOSC Attività Tecniche e della Manutenzione Ing. Ciro Verdoliva Responsabile del trattamento	Ufficio per le Attività Tecniche e della Manutenzione Personale Incaricato
		Trattamento di dati per la gestione giuridica e previdenziale delle risorse umane, trattamento di dati concernenti le procedure di selezione del personale, le immissioni in servizio e gestione di dati per il trattamento economico di base ed accessorio del personale.	Dirigente della UOSC Gestione delle Risorse Umane: Dott.ssa Maria Maiorano Responsabile del trattamento	Ufficio per la Gestione delle Risorse Umane. Personale Incaricato
Area Sanitaria e Medica di Presidio		Direzione Sanitaria	Direttore Sanitario Dott.ssa Patrizia Caputo	Ufficio Direzione Sanitaria Personale incaricato

Processo	Sottoprocessi	Trattamenti	Referente Organizzativo	Organizzazioni Operative
	Dipartimenti	Direzione Medica di Presidio Trattamento dei dati concernenti la gestione delle funzioni di coordinamento della Direzione Medica di Presidio.	Direttore Medico di Presidio Dott. Franco Paradiso Responsabile del trattamento della Direzione Medica di Presidio Coordinatore dell'Area Generale delle Attività Sanitarie	Ufficio della Direzione Medica di Presidio e struttura di coordinamento della dell'Area Generale delle Attività Sanitarie Personale Incaricato
		Trattamenti di dati sensibili: Accettazione di P.S. Gestione delle cartelle cliniche di P.S. e del ricovero ordinario, referti clinici di pazienti	Responsabile del trattamento del Dipartimento di Emergenza Coordinatore -referente Dott. Ciro Mauro	UOSC afferenti al Dipartimento di Emergenza Accettazione Personale Incaricato
		Trattamenti di dati sensibili: gestione cartelle cliniche, referti clinici di pazienti	Responsabile del trattamento del Dipartimento Medico Polispecialistico: Coord. Dott. Piergiorgio Rabitti	UOSC afferenti al Dipartimento di Medicina Polispecialistica Personale Incaricato
		Trattamenti di dati sensibili: gestione cartelle cliniche, referti clinici di pazienti	Responsabile del trattamento del Dipartimento Chirurgico Polispecialistico: Coord. Dott. Maurizio De Palma	UOSC afferenti al Dipartimento di Chirurgia Polispecialistica Personale Incaricato
		Trattamenti di dati sensibili: gestione dei dati concernenti i trapianti, cartelle cliniche, referti clinici di pazienti	Responsabile del trattamento del Dipartimento Trapianti: Coord. Dott. Oreste Cuomo	UOSC afferenti al Dipartimento dei Trapianti Personale Incaricato
		Trattamenti di dati sensibili: gestione cartelle cliniche, referti clinici di pazienti	Responsabile del trattamento del Dipartimento di Onco-pneumo-ematologia: Coord. Dott. Felicetto Ferrara	UOSC afferenti al Dipartimento di Onco-pneumo-ematologia Personale Incaricato
		Trattamenti di dati sensibili: gestione delle immagini di radiologia, gestione cartelle cliniche, referti clinici dei pazienti	Responsabile del trattamento del Dipartimento delle Tecnologie Avanzate Diagnostico -terapeutiche: Coord. Dott. Franco Maglione	UOSC afferenti al Dipartimento delle Tecnologie Avanzate Diagnostiche: Personale Incaricato

Processo	Sottoprocessi	Trattamenti	Referente Organizzativo	Organizzazioni Operative
		Trattamenti di dati sensibili: gestione dei referti diagnostici di laboratorio ed isto - citopatologici dei pazienti	Responsabile del trattamento del Dipartimento dei Servizi: Coord. Dott. Oscar Nappi	UOSC afferenti al Dipartimento dei Servizi Personale Incaricato
		Trattamenti di dati sensibili: gestione cartelle cliniche, referti clinici di pazienti	Responsabile trattamento del Dipartimento di Anestesia e Rianimazione: Coord. Dott. Carlo Di Iorio	UOSC afferenti al Dipartimento di Anestesia e Rianimazione Personale Incaricato

Alla luce delle recenti direttive emanate dalla Presidenza del Consiglio, che impongono alle pubbliche amministrazioni l'assunzione di direttive e metodologie finalizzate alla digitalizzazione degli atti amministrativi, la corretta gestione degli adempimenti finalizzati alla protezione dei dati personali rappresenta una premessa fondamentale e costituisce un punto di forza per l'innovazione di tutto il management aziendale.

1.7 Metodologia di rilevazione del patrimonio informativo in materia di privacy

La metodologia adottata per effettuare la ricognizione del patrimonio informativo e tecnico-strumentale in materia di sicurezza dei dati si avvale dell'impiego di tre tipologie di schede distinte, strutturate per tre differenti campi dell'indagine conoscitiva e finalizzate all'analisi complessiva delle misure di sicurezza oggetto dell'elaborato. La procedura d'indagine deve essere configurata partendo dalla definizione delle risorse aziendali che esplicano la funzione di Responsabili e di Incaricati del trattamento. In merito a tali funzioni e alla graduazione delle responsabilità in materia di privacy sono stati elaborati due modelli recanti: l'atto di nomina dei Sostituti del Responsabile del trattamento e l'atto di nomina degli Incaricati. Entrambi i modelli individuano i soggetti che effettuano i trattamenti dei dati, rispettivamente nelle strutture sanitarie che

afferiscono ai Dipartimenti diretti dai Coordinatori dipartimentali e nelle UOSC dell'area funzionale amministrativa e/o in staff alla Direzione Generale.

Sono, inoltre, impiegate tre differenti schede ai fini della rilevazione e della catalogazione delle informazioni ritenute indispensabili ai fini della redazione del DPS

La prima delle tre schede utilizzate è indicata come scheda A ed è finalizzata alla catalogazione dei dati trattati in relazione alle caratteristiche del servizio o della prestazione erogata. L'esigenza di adoperare questo tipo di scheda è connessa all'indicazione metodologica, dettata dal Garante, di configurare in base alla tipologia i dati personali trattati nelle aziende sanitarie. A tal fine, è stato preso in esame il "Regolamento per il trattamento dei dati personali sensibili e giudiziari" redatto per le Aziende sanitarie e recepito dalla Regione Campania, il quale reca una molteplicità di schede "schema tipo di regolamento" che sono raccolte in un "Elenco dei trattamenti di competenza delle Aziende sanitarie operanti nel SSN" approvato con deliberazione n. 625 del 12 maggio 2006 dalla Regione Campania.

Sono state prese a campione dal suddetto elenco ed opportunamente rimodulate per implementare il presente rapporto sei schede "schema tipo di regolamento per le Aziende sanitarie" che sono rappresentate in allegato ed accluse in appendice. Esse recano le seguenti indicazioni:

a) denominazione del trattamento,
b) fonti normative e legislative a cui si riferiscono le prestazioni che caratterizzano il tipo di informazioni trattate,
c) altre fonti,
d) finalità del trattamento,
e) tipologia dei dati trattati,
f) modalità di trattamento dei dati,
g) tipologia delle operazioni eseguite (relative alle forme di trattamento dei dati),
h) descrizione del tipo di trattamento e del flusso informativo correlato ad esso.

Per poter realizzare un'analisi complessiva delle misure di sicurezza dei dati trattati con gli strumenti elettronici è necessario ricorrere all'impiego di altre due schede, di seguito indicate:

- la scheda B, necessaria per la rilevazione e localizzazione delle banche dati che raccolgono il patrimonio informativo e le forme di trattamento eseguite dalle Direzioni dell'area amministrativa e dalle Strutture dipartimentali sanitarie;
- la scheda C, indispensabile per la rilevazione, presso tutte le UOSC aziendali, delle misure minime di sicurezza adottate per la protezione delle banche dati e degli strumenti elettronici che consentono il trattamento informatizzato dei flussi informativi e dei dati personali.

La metodologia d'indagine posta in essere mediante l'impiego delle tre schede di rilevazione suindicate e l'elenco degli Incaricati e dei Sostituti del Responsabile del trattamento, individuati in relazione alla struttura amministrativa o dipartimentale sanitaria, è finalizzata a formulare un rapporto informativo che associa gli esiti di risultato forniti dalle schede B e C alla sintesi descrittiva dei trattamenti fornita dalle schede A, le quali recano la tipologia dei trattamenti in relazione alle diverse caratteristiche di prestazioni erogate. La suindicata metodologia di rilevazione e di analisi consente di realizzare una ricognizione analitica dei vari elementi che compongono l'indagine conoscitiva finalizzata al rapporto programmatico sulla sicurezza dei dati.

1.8 La classificazione dei trattamenti dei dati

La procedura di catalogazione delle informazioni rinvenute mediante l'utilizzo delle suindicate schede di rilevazione, adottate ai fini dell'indagine conoscitiva, può essere sinteticamente rappresentata nel seguente prospetto:

identificativo del	**UOSC Amministrativa Area dipartimentale**	**1) Scheda A**	**2) Scheda B**	**3) Scheda C**

trattamento	sanitaria			
Numero identificativo del trattamento individuato nella scheda A riportato nelle schede B e C	Denominazione del Responsabile del Trattamento della Struttura Amministrativa o del Dipartimento Sanitario, Nomina dei Sostituti del Responsabile e degli Incaricati del trattamento	Denominazione del tipo di trattamento dei dati recante la tipologia dei dati, delle modalità di trattamento sulla base delle prestazioni e dei servizi erogati	Rilevazione e localizzazione delle banche dati, dei programmi e dei software applicativi, dei sistemi di backup adottati nelle UOSC amministrative oppure nei Dipartimenti dell'area sanitaria	Rilevazione delle misure di sicurezza adottate per la protezione delle banche dati, delle credenziali di accesso richieste per la sicurezza degli strumenti elettronici: PC

La denominazione della Unità operativa complessa amministrativa o del Dipartimento di Area sanitaria e, pertanto, dei rispettivi Responsabili del trattamento, la ricognizione degli Incaricati e dei Sostituti del Responsabile, individuati mediante atto formale sottoscritto dai Responsabili del trattamento che esplicano tale funzione nell'area amministrativa o sanitaria, costituiscono gli elementi di base per poter articolare l'indagine attraverso cui si snoda il presente rapporto. Gli atti di nomina degli Incaricati e dei Sostituti dei Responsabili del trattamento sono reperibili presso l'Ufficio Relazioni col Pubblico, dove sono custoditi tutti gli atti che documentano gli interventi attivati in materia di privacy.

1) La scheda A recante lo "schema tipo di regolamento per le aziende sanitarie" assolve una funzione di carattere connotativo nell'indicazione dei trattamenti dei dati.

Infatti, nella denominazione e descrizione dei trattamenti, la scheda A rileva la tipologia e le modalità di trattamento dei dati in relazione alle caratteristiche delle prestazioni erogate, prescindendo dalla individuazione strutturale ed organizzativa dei singoli Dipartimenti o Strutture amministrative che esplicano il trattamento.

La logica perseguita dal proponente del presente rapporto, ai fini della selezione delle schede A, di seguito elencate, è subordinata alla catalogazione delle categorie degli interessati in base alle quali sono desumibili le finalità dei trattamenti dei dati.

Le categorie degli interessati, a cui si riferiscono i dati trattati nell'Azienda Cardarelli, sono essenzialmente quattro: i pazienti, gli assistiti, i dipendenti ed i fornitori. Pertanto, le schede recanti lo "schema tipo di regolamento per le aziende sanitarie" individuate per l'elaborazione del presente documento sono:

- la scheda n. 17 recante la denominazione del trattamento: "Attività amministrativa, programmatoria e gestionale, relativa all'assistenza in regime di ricovero";
- la scheda n. 20 recante la denominazione del trattamento: "Soccorso sanitario di emergenza. Sistema 118. Assistenza sanitaria di emergenza";
- la scheda n. 54 recante la denominazione del trattamento: "Gestione delle Risorse Umane";
- la scheda n. 50 recante la denominazione del trattamento: "Gestione del fondo economale. Acquisizione di Beni e Servizi"

Alle quali si aggiungono, al fine di conferire liceità ad ulteriori tipologie di trattamenti, le seguenti schede:

- la scheda n. 41 recante la denominazione del trattamento: "Videosorveglianza con finalità di sicurezza e protezione di beni e persone"
- la scheda n. 22 recante la denominazione del trattamento: "Trapianti"

Tutte le schede sopra menzionate sono allegate in appendice al presente documento.

E' doveroso precisare, che l'Azienda ospedaliera "A. Cardarelli" si afferma nello scenario sanitario regionale, sia per le prestazioni erogate in emergenza che per le discipline mediche e chirurgiche generali e specialistiche, le quali possono erogare assistenza anche in day hospital e in day surgery nonché, su richiesta degli utenti, in attività libero-professionale intramuraria. Pertanto, le schede "schema tipo di regolamento per le aziende sanitarie" recanti la tipologia dei trattamenti in osservanza alle finalità istituzionali consentite, sono essenzialmente due: la scheda 17 e la scheda 20 le quali definiscono, in maniera concisa, la tipologia e le modalità di trattamento che sono peculiari per l'operatività delle Azienda sanitarie.

Le schede B e C rispecchiano, invece, le misure di sicurezza tecnico-strumentali .

Le schede B e C richiedono la rilevazione delle informazioni, di seguito descritte, delle strutture con funzione dipartimentale o amministrativa a cui sono preposti i Responsabili del trattamento. Tali schede vengono correlate mediante un numero identificativo del trattamento alla corrispondente scheda A recante lo "schema tipo di regolamento", allo scopo di qualificare le informazioni rilevate nell'ambito della struttura rapportandole al tipo di trattamento.

2) La scheda B, utilizzata per la rilevazione e localizzazione delle banche dati contenenti il patrimonio informativo digitale dell'entità strutturale ed organizzativa presa in esame, indica, oltre alla denominazione della struttura di riferimento, le quattro categorie degli interessati a cui si riferiscono i dati trattati, che sono:

- i pazienti ricoverati,
- gli assistiti,
- i dipendenti,
- i fornitori.

La stessa scheda, inoltre, rileva i programmi e gli strumenti software utilizzati per l'impiego degli strumenti elettronici, che nell'Azienda Cardarelli possono essere applicabili utilizzando le risorse disponibili nella rete. Infatti, all'indicatore della scheda B che rileva programmi e strumenti software, è stata data la denominazione standardizzata di "web application".

L'ulteriore categoria di indicatori contenuti nella scheda B serve a configurare i dispositivi di protezione e di sicurezza delle banche dati ovvero il "sistema di back up" e le protezioni fisiche delle banche dati.

Il "sistema di back up" è impiegato per il salvataggio delle informazioni contenute nelle banche dati che sono gestite dalle strutture operative aziendali. Tale metodo di salvaguardia delle informazioni viene assicurato, in modo standardizzato, grazie ad un sistema di archiviazione robotizzato e centralizzato che raccoglie tutti i dati trattati nell'Azienda Cardarelli e li custodisce presso il "Centro Stella", ubicato al piano terra del padiglione N (padiglione monumentale).

La frequenza della procedura di salvataggio delle informazioni operata dal "Centro Stella" avviene ciclicamente ogni ventiquattro ore. E', oltretutto, attuabile il piano di ripristino mediante la disponibilità di dispositivi e procedure che assicurano il "disaster recovery". Inoltre, è adottato il sistema di protezione per assicurare la continuità dell'erogazione elettrica (UPS), impiegato per proteggere gli strumenti e gli impianti elettronici da improvvise interruzioni dell'erogazione elettrica che potrebbero causare la perdita di dati.

3) La scheda C che è stata utilizzata per la ricognizione, presso tutte le unità operative complesse dell'azienda sia dell'area sanitaria che amministrativa, delle misure minime di sicurezza adottate per la protezione delle banche dati e degli strumenti elettronici è caratterizzata dai seguenti indicatori:

- tipologia e numero di personal computer in dotazione delle varie strutture,
- controllo elettronico per l'accesso alla banca dati,
- dispositivi di protezione dagli attacchi alla banca dati (antivirus),
- modalità di accesso del sistema di elaborazione e caratteristica dei server.

Le misure logiche e fisiche che proteggono la rete aziendale hanno consentito di standardizzare la rilevazione indicata nello schema della scheda C.

I dispositivi utilizzati comunemente per prevenire gli attacchi causati da agenti che possono danneggiare gli strumenti e le banche dati sono i seguenti:

- Firewall perimetrale "Fortinet",
- Sophos antivirus,
- Web filtering.

Inoltre, in adempimento all'indicazione di definire il numero e la tipologia dei PC in dotazione delle UOSC dell'ospedale, il settore privacy aziendale, incaricato della rilevazione, ha utilizzato l'elenco inventariale aggiornato che reca il numero dei PC in dotazione dell'Azienda, catalogato per unità operativa complessa, elaborato su committenza della Direzione funzionale complessa Acquisizione Beni e Servizi anche

nell'ottica di documentare la licenza all'utilizzo delle apparecchiature e degli strumenti elettronici acquistati dall'Azienda.

L'accesso ai data base dell'Azienda è protetto da dispositivi per la sicurezza dei dati che profilano l'utenza abilitata all'accesso, in maniera standardizzata. Le UOSC di Immunoematologia Trasfusionale, del Laboratorio di Analisi e dell'Anatomia Patologica utilizzano, per fini istituzionali, anche l'accesso remoto mediante il canale VPN (virtual private network) che è un canale di comunicazione protetto che consente l'interoperabilità in rete con piattaforme esterne.

Le caratteristiche dei server sono conformi alle indicazioni in materia di sicurezza previste dalla normativa in materia di protezione dei dati personali. Non a caso, le informazioni che circolano nella rete aziendale e raccolte nei vari server vengono centralizzate nel "Centro Stella", ubicato al piano terra del padiglione amministrativo. Il "centro stella" rappresenta il punto di confluenza della rete informatica di tutta la struttura ospedaliera. Il cablaggio della rete LAN è in fibra ottica e decorre dal "Centro Stella" ai padiglioni e dai padiglioni alle varie strutture operative dell'ospedale.

Le schede recanti lo "schema tipo di regolamento delle Aziende sanitarie" ed elaborate per indicare le tipologie di trattamento, le schede di rilevazione B e C, compilate in maniera standardizzata per le finalità dell'indagine, i modelli recanti gli atti di nomina dei sostituti del Responsabile del trattamento e degli Incaricati, i format per le informative agli interessati e per l'acquisizione del consenso al trattamento dei dati personali, le rappresentazioni standardizzate dei dati riferibili alle schede B e C, sono consultabili nell'appendice che reca gli allegati e che è acclusa al presente rapporto.

1.9 Accesso ai data base della rete aziendale per fini istituzionali.

L'Azienda "A. Cardarelli" esplica la protezione dei dati raccolti nei data base proteggendo la rete LAN con il dispositivo "single sign on" (SSO), il quale mette in sicurezza le informazioni mediante meccanismi standard di protezione dei dati. Il mantenimento di tali standard si concretizza nell'accesso alla rete mediante

l'autenticazione dell'utente. Infatti, il sistema di protezione "single sign on" consente all'incaricato del trattamento di autenticarsi una sola volta per accedere alle risorse informatiche alle quali è abilitato. Tale sistema finalizzato alla sicurezza dei dati semplifica la gestione degli accessi ai vari servizi grazie ad una profilazione unica dell'utente abilitato.

L'ospedale "A. Cardarelli" per adeguarsi alle esigenze di servizio ed alle direttive emanate col Codice dell'Amministrazione digitale (D.Lgs n. 82 /2005), che regola la funzione e l'organizzazione delle procedure informatiche nelle P.A., ha avviato un piano di razionalizzazione dei sistemi informativi e delle risorse informatiche disponibili nella rete aziendale, al fine di rendere più funzionale la gestione delle informazioni che assolvono una funzione di servizio in Azienda.

Il sistema informativo che gestisce l'anagrafica generale dei dati personali degli utenti che vengono trattati ai fini della *accettazione, dimissione e trasferimento,* in adempimento all'esercizio dei ricoveri e delle altre funzioni d'istituto, si chiama con un acronimo "ADT". Tale sistema informativo funziona utilizzando l'infrastruttura di trasporto presente nella rete LAN dell'Azienda

L'impiego del sistema informativo ADT apporta un vantaggio concreto all'organizzazione, sia in termini di semplificazione delle procedure che di economicità nell'impiego delle risorse. Esso rispetta il dettato normativo contemplato dagli artt. 31, 33, 34 e dal Disciplinare tecnico del Codice in materia di protezione dei dati personali. Ottempera, inoltre, alle direttive contenute nei seguenti articoli del D.Lgs 82/2002 *(Codice dell'Amministrazione digitale) :*

art. 2 (*Finalità ed ambito di applicazione),* comma 5;

art. 3 (*Diritto all'uso delle tecnologie*), comma 1;

art. 51 *(Sicurezza dei dati, dei sistemi e delle infrastrutture informatiche),*comma 1 e 2;

art. 73 *(Sistema Pubblico di Connettività),* comma 1 e 2;

art. 76 (*Scambio di documenti informatici nell'ambito del Sistema Pubblico di Connettività)*

Il sistema di software ADT consente agli incaricati del trattamento di accedere alle banche dati raccolte nella rete aziendale e di esplicare le funzioni che attengono all'inoltro ed alla ricezione delle informazioni riconducibili all'anagrafica generale degli utenti, come gli esami di laboratorio, i referti diagnostici, i referti e le immagini della diagnostica per immagini, le prenotazioni di prestazioni, i ricoveri di pronto soccorso, i ricoveri programmati, i ricoveri in day hospital .

L'accesso ai data base che recano le informazioni raccolte nella rete aziendale può essere effettuato dagli incaricati soltanto se si attua la procedura di autenticazione che consente, mediante la digitazione delle credenziali di accesso al sistema, l'identificazione dell'utente abilitato ad entrare nella rete.

La corretta applicazione delle procedure di autenticazione, che consentono agli incaricati di trattare i dati sensibili degli utenti per l'esercizio esclusivo delle attività istituzionali, deve essere oggetto di vigilanza costante da parte dei Responsabili del trattamento e da parte delle risorse incaricate dal Titolare del trattamento di esercitare la tutela della privacy aziendale.

Le finalità che l'Azienda "Cardarelli" tende a perseguire per lo sviluppo tecnologico ed organizzativo della rete aziendale riflette le indicazioni enunciate dagli artt. 73 e 76 del *Codice dell'Amministrazione Digitale* . La gestione delle informazioni mediante l'impiego del protocollo standard per medicali HL7, progettato per la comunicazione e la cooperazione automatica dei sistemi informativi di rete, costituisce il presupposto per una comunicazione istituzionale che si concretizza nell'*interoperabilità* delle funzioni esplicate dai soggetti erogatori di servizi e prestazioni.

Tuttavia, considerata la delicatezza dei tipi di trattamento che riguardano quasi esclusivamente dati sensibili, diventa più cogente l'adempimento delle procedure che assicurano l'osservanza delle norme vigenti in materia di privacy.

Per le finalità perseguite dal presente rapporto, si formula l'elenco delle Unità Operative Complesse che hanno accesso alle informazioni che attengono alla diagnostica di laboratorio e che sono gestite col sistema informativo "open LIS" (laboratory information system) :

1) Broncologia endosc.
2) Cardiologia con UTIC
3) Cardiologia Riabilitativa
4) CEB Trapianto di Fegato
5) Centro Antiveleni
6) Centro Ustioni e Ch. Plastica
7) Chirurgia 1
8) Chirurgia 2
9) Chirurgia 3
10) Chirurgia D'Urgenza
11) Chirurgia Maxillo-facciale
12) Chirurgia Toracica
13) Chirurgia Vascolare
14) CLSE Trapianto di Fegato
15) Detenuti
16) Ematologia con Trap. di Midollo
17) Fisiokinesiterapia
18) Gastroenterologia
19) Medicina 1
20) Medicina 3
21) Medicina 4
22) Medicina 5
23) Medicina D'Urgenza
24) Nefrologia e Dialisi
25) Neurochirurgia
26) Neurologia
27) Oculistica
28) Odontoiatria
29) Oncologia
30) Ortopedia 1
31) Ortopedia 2
32) Ostetricia e Ginecologia
33) Otorinolaringoiatria
34) Pneumologia 1
35) Pneumologia 2
36) Rianimazione DEA
37) T.I.N.
38) T.I.P.O.
39) Terapia del Dolore
40) TERE Ematologia
41) U.T.I.F.
42) Urologia

L'ottemperanza degli standard di sicurezza attuati col sistema di protezione "SSO" e la revisione costante dell'infrastruttura di trasporto che assicura la circolazione dei flussi informativi nella rete aziendale, ha consentito l'impiego di un sistema informativo per l'accesso ai data base dedicato alla raccolta e comunicazione dei dati che attengono alle attività di refertazione e di custodia delle immagini in materia di diagnostica per immagini. Il sistema informativo che consente il trattamento della tipologia dei dati sopra descritti è definito PACS. L'acronimo sta ad indicare "Picture Archiving and

Communications System" che significa: archiviazione delle immagini e sistema di comunicazione delle stesse.

Elenco delle strutture operative che hanno accesso al PACS aziendale:

1) Chirurgia D'Urgenza
2) Neurologia
3) Neurochirurgia
4) Chirurgia Toracica
5) UTIF
6) TIN
7) CEB
8) Chirurgia 1
9) Chirurgia 2
10) Endocrinologia
11) Chirurgia Vascolare
12) Ortopedia 1
13) Ortopedia 2
14) Maxillo Facciale
15) Medicina 1
16) Cardiologia Riabilitativa
17) Oncologia
18) Pneumologia
19) Broncologia Endoscopica

I sistemi operativi che consentono l'accesso ed il trattamento dei dati inerenti alla diagnostica di laboratorio (LIS) ed alla diagnostica per immagini (PACS) utilizzano come supporto, per la ricerca anagrafica degli utenti, il sistema informativo ADT.

Al fine di informatizzare le procedure che attengono all'inoltro ed alla ricezione degli ordini oppure degli esami diagnostici e/o di laboratorio, è stato applicato al sistema software un programma che assolve la funzione di "broker di messaggio" che prende la denominazione di "order entry".

Il programma operativo “order entry” consente di effettuare ordini di prodotti farmaceutici o di armamentario; di inoltrare le richieste di esami diagnostici e/o di laboratorio; di richiedere referti diagnostici e di laboratorio; di inoltrare le richieste di esami radiologici e di acquisirne i referti ai fini della diagnostica radiologica per immagini.

Le unità operative che possono utilizzare il programma “order entry” e che, quindi, hanno la facoltà di collegarsi alla Farmacia, al Laboratorio di Analisi, alle strutture di Radiologia, per esplicare i compiti e le funzioni d’istituto, sono già state menzionate in elenco nel presente paragrafo.

Nell’ottica di ampliare e mettere in sicurezza l’infrastruttura di trasporto che consente la comunicazione dei dati nella rete LAN aziendale, è in programmazione una nuova “server farm” la quale dovrà assolvere la funzione di “business continuity” ovvero dovrà essere in grado di assicurare la continuità operativa dei servizi ICT, anche nel caso in cui l’infrastruttura preesistente non sia più funzionante per motivi contingenti.

L’Azienda “A. Cardarelli” ha realizzato nell’anno 2007 un primo piano di cablaggio della rete LAN che consente, a tutt’oggi, la centralizzazione di tutti i flussi informativi e dei data base che contengono i dati trattati dalle varie unità operative dell’ospedale. Tale piano che ha consentito la realizzazione di un punto di confluenza unificato della rete LAN aziendale, identificabile con la struttura definita “Centro Stella”, è ancora *in progress* per consentire l’adeguamento della rete alle crescenti esigenze organizzative dei servizi e delle strutture sanitarie che erogano assistenza.

ALLEGATI

Informativa all'assistito in materia di protezione dei dati personali

Gentile Utente,
ai sensi dell'art. ***13*** *del* ***D.lgs n. 196/2003*** *(Codice in materia di protezione dei dati personali), recante la normativa in materia di tutela della privacy, La informiamo che il trattamento delle informazioni che La riguardano, sarà improntato ai principi di correttezza e liceità a tutela della Sua riservatezza e dei Suoi diritti in materia di privacy.*
I dati sensibili, idonei a rivelare il Suo stato di salute e/o la vita sessuale, possono essere oggetto di trattamento secondo le indicazioni dettate dall'art. ***26 del d. lgs n. 196/2003****.*

Ai sensi dell'articolo **13 del d.lgs n. 196/2003**, Le forniamo le seguenti informazioni:

1. I dati personali da Lei forniti saranno trattati nel rispetto degli obblighi di riservatezza e della normativa vigente in materia di privacy. I Suoi dati saranno raccolti per le finalità previste dal trattamento e consentite dalla legge.
2. Il conferimento dei Suoi dati è obbligatorio per le finalità ed i compiti d'istituto che ottemperano alla tutela della salute pubblica e l'eventuale rifiuto a fornire i dati personali non comporta alcuna conseguenza.
3. I Suoi dati non saranno comunicati a terzi se non per i motivi consentiti dalla legge e per le finalità d'istituto. In ogni caso, non saranno oggetto di diffusione. I dati potranno essere/saranno comunicati esclusivamente per i motivi connessi ai compiti istituzionali e per le finalità previste dal dettato del **d. lgs n. 196/2003**.
4. La presente informativa ed il consenso da Lei prestato si riferiscono alla pluralità delle prestazioni erogate, anche in tempi diversi, dalle Unità operative complesse che Le forniscono assistenza in ospedale durante e dopo la degenza.
5. Il Titolare del trattamento è il Direttore Generale dell'Azienda Ospedaliera di Rilievo Nazionale "A. Cardarelli"
6. I Responsabili del trattamento dei dati, individuati dal Titolare del trattamento con atto formale, sono i Coordinatori dei Dipartimenti sanitari e/o i Direttori delle Unità Operative Complesse dell'Area amministrativa
7. L'Azienda "A. Cardarelli" ha individuato, per consentire l'esercizio dei diritti degli interessati a tutela della propria privacy, il Settore Privacy aziendale che coordina le attività finalizzate alla protezione dei dati personali nell'ambito delle funzioni istituzionali esplicate dall'Ufficio Relazioni col Pubblico.
8. In ogni momento l'interessato potrà esercitare i Suoi diritti nei confronti del Titolare del trattamento, ai sensi dell'articolo **8** del **d. lgs n. 196/2003**.

Acquisizione del consenso dell'interessato al trattamento dei dati personali

Acquisite le dovute informazioni fornite ai sensi dell'articolo **13 del d. lgs. n. 196/2003**, preso atto delle misure di salvaguardia della riservatezza nel trattamento dei dati personali, l'interessato presta il suo consenso al trattamento dei propri dati, per i fini indicati nell'allegata informativa

Espressione di consenso al trattamento dei dati personali

ai sensi dell'art. 23 del d. lgs 196/03

Nome……..……...

Cognome……...

Firma leggibile……data……

(L'interessato che sottoscrive presta il suo consenso alla comunicazione dei Suoi dati per le finalità indicate nell'informativa.)

Art. 7 del d. lgs. n. 196/2003: Diritti dell'interessato

In relazione al trattamento dei dati personali e sensibili l'interessato ha diritto:

a) di conoscere mediante accesso gratuito al registro di cui all'art. 31, comma 1, lettera a), l'esistenza di trattamenti di dati che possono riguardarlo;
b) di essere informato su quanto indicato dall'art. 7, comma 4, lettere a), b), e h);
c) di ottenere a cura del titolare o del responsabile, senza ritardo:

1. conferma dell'esistenza o meno dei dati personali che lo riguardano, anche se non ancora registrati e la comunicazione in forma intellegibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento;
2. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
3. l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;
4. l'attestazione che le operazioni di cui ai numeri 2) e 3) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestatamene sproporzionato rispetto al diritto tutelato;

e) di opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

f) di opporsi in tutto o in parte, al trattamento di dati personali che lo riguardano, previsto a fini di informazioni sui servizi erogati o di invio di materiale pubblicitario o per il compimento di ricerche di mercato o di comunicazione interattiva e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente tale diritto.

ATTO DI NOMINA DEGLI INCARICATI DEL TRATTAMENTO

Il sottoscritto, Responsabile del trattamento dei dati ai sensi dell'art. 29 del D.lgs 196/03, Direttore della UOSC: ..…….., Responsabile del trattamento giusta nomina conferita dal Titolare del trattamento dei dati, con il presente atto nomina, individua nei sottoelencati dipendenti, ai sensi dell'art. 30 del D.lgs 196/03, la funzione di Incaricati del trattamento dei dati:

- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,

Con il presente atto di nomina si incaricano le persone suelencate a trattare i dati personali degli utenti, dei fornitori e del personale:

- in modo lecito e secondo correttezza;
- raccogliendoli e registrandoli per gli scopi inerenti l'attività svolta da ciascuno;
- verificando, ove possibile, che siano esatti e, se necessario, aggiornati;
- verificando che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile;
- conservandoli, rispettando le misure di sicurezza predisposte dall'Azienda. In ogni operazione di trattamento dovrà essere garantita la massima riservatezza.

In caso di allontanamento anche temporaneo dal posto di lavoro, l'incaricato dovrà verificare che non vi sia possibilità, da parte di terzi, anche se dipendenti, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo o automatizzato.

Firma……data……..

ATTO DI NOMINA DEI SOSTITUTI DEL RESPONSABILE DEL TRATTAMENTO

Il sottoscritto Dott:…….
Coordinatore del Dipartimento:……..Responsabile del trattamento dei dati, ai sensi dell'art. 29 del D.lgs 196/03 e Coordinatore dipartimentale, giusta nomina conferita con delibera 761 del 29-11-2010, con il presente atto nomina, attribuisce ai sottoelencati Direttori di Struttura Operativa Complessa , ai sensi dell'art. 29 del D.lgs 196/03, l'incarico di Sostituti del Responsabile del trattamento dei dati:

- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,
- ……..,

Con il presente atto di nomina si incaricano le persone suelencate a trattare i dati personali degli utenti, dei fornitori e del personale:

- in modo lecito e secondo correttezza;
- raccogliendoli e registrandoli per gli scopi inerenti l'attività svolta da ciascuno;
- verificando, ove possibile, che siano esatti e, se necessario, aggiornati;
- verificando che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Responsabile;
- conservandoli, rispettando le misure di sicurezza predisposte dall'Azienda. In ogni operazione di trattamento dovrà essere garantita la massima riservatezza.

Firma……data……
Il Responsabile del trattamento dei dati personali (timbro e firma)

SCHEDE di RILEVAZIONE B e C STANDARIZZATE

SCHEDA B: RICOGNIZIONE BANCHE DATI

Identificativo Trattamento	scheda n°			**Pag. 1/1**
Data		**Compilata da:**		

Struttura di Riferimento del Trattamento	
Dipartimento Area sanitaria	
UOSC Amministrativa	
UOSC Sanitaria	
UOS o Ufficio	

Categoria di Interessati a cui si riferiscono i Dati				
Dipendenti	X	Pazienti	X	
Assistiti	X	Fornitori	X	
Barrare a lato con una X una o più categorie interessate; specificare(nelle caselle libere) eventuali tipi diversi				

Localizzazione Banche Dati Relativa al Trattamento	
Nome delle Banche dati	
Sede	AORN "A. Cardarelli"
Programma utilizzato	web filtering
Strumenti Software utilizzati	

Sistema di Backup delle Banche Dati	
Descrizione	salvataggio in rete mediante sistema di archiviazione robotizzato
Dispositivo	Disaster recovery
Frequenza e modo	ogni 24 ore

Addetto	Operatore Ditta LUTECH
Luogo di custodia	"Centro Stella" ubicato al pad. N piano terra
Piano di ripristino	Ripristino mediante il dispositivo di disaster recovery
UPS	Presente

Protezioni Fisiche delle Banche Dati			
Sistemi di allarme		Stanze con porte con chiavi	**X**
Sistemi antincendi	**X**	Armadi muniti di serrature	**X**
Bunkerizzazione dei locali		Scaffallature aperte	

SCHEDA TIPO C: RICOGNIZIONE MISURE ADOTTATE (Protezione Banche Dati)

Identificativo Trattamento				**Pag. 1/1**
Data		**Compilata da:**		

Struttura di Riferimento del Trattamento	
Struttura Complessa sanitaria	
Struttura Complessa amminist	
Struttura semplice (UOS)	

Descrizione e Livello Tecnologico Strumenti Utilizzati per il Trattamento					
Tipo PC/Server	PC				
N° PC		Medio	X	Attuale	

Sistema Operativo			**Lic(S/N)**
Windows 95			
Windows			

98			
Windows Millenium			
Windows 2000 Professional	X		X
Windows XP	X		X
Altro Sistema Operativo (descrivere)			
Barrare con una X il sistema operativo installato e indicare se regolarmente licenziato (S/N)			

Controllo Elettronico Accesso alla Banca Dati	
Sistema di Autenticazione	
Sistema di Autorizzazione	userid e password
Separazione e Cifratura dei dati Sensibili	

Protezione dagli Attacchi alla Banca Dati	
Firewall	Firewall perimetrale "Fortinet"
Antivirus	Sophos antivirus
Altro	web filtering

Modalità di Accesso del Sistema di Elaborazione	
Non accessibile ad altri elaboratori (Stand-alone)	X
In rete interna non accessibile al pubblico (Intranet)	X
In rete interna accessibile al pubblico (Internet)	X
Server	I server sono centralizzati nel "Centro Stella" aziendale, punto di accesso unificato della rete LAN, ubicato al pad. "N" piano terra. Il cablaggio della rete LAN è in fibra ottica e decorre dal "Centro Stella" ai Padiglioni e dai Padiglioni alle Strutture.