



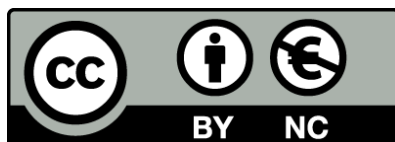
innovation-governance-compliance
ICT & Business Consulting

Antonio Cappiello

acappiello@e-tecnolink.it

Guida Pratica al Riesame del DPS

V. 1.0 del 10 febbraio 2010



Creative Commons Attribuzione - Non commerciale 2.5 Italia License
<http://creativecommons.org/licenses/by-nc/2.5/it/>



Creative Commons Attribuzione - Non commerciale 2.5 Italia License
<http://creativecommons.org/licenses/by-nc/2.5/it/>

Commons Deed



Tu sei libero:



- di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera



- di modificare quest'opera

Alle seguenti condizioni:



- **Attribuzione.** Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.



- **Non commerciale.** Non puoi usare quest'opera per fini commerciali.

- Ogni volta che usi o distribuisce quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza.
- In ogni caso, puoi concordare col titolare dei diritti utilizzi di quest'opera non consentiti da questa licenza (acappiello@e-tecnolink.it).
- Questa licenza lascia impregiudicati i diritti morali.

Limitazione di responsabilità

Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.

Questo è un riassunto in linguaggio accessibile a tutti del [Codice Legale \(la licenza integrale\)](#)¹.

¹ <http://creativecommons.org/licenses/by-nc/2.5/it/legalcode>

Presentazione

Cresce la sensibilità dell'opinione pubblica e delle istituzioni nazionali e internazionali sul tema dell'uso legittimo e sicuro delle informazioni personali raccolte a vario titolo da, ormai, una moltitudine di soggetti

L'osservanza nell'operato quotidiano delle misure minime di sicurezza adottate e descritte nel Documento Programmatico della Sicurezza, diventano sempre più oggetto di controllo da parte di numerose autorità e, in alcuni casi, **condizione essenziale per gli operatori privati** per continuare ad operare in regime di concessione, autorizzazione o convenzione

Questa opera minimalista ha lo scopo di offrire al Titolare e al Responsabile del trattamento dati una guida operativa per verificare l'aderenza del proprio DPS alla vigente normativa in materia di trattamento dei dati personali anche in seguito delle importanti novità introdotte dal Garante in tema degli amministratori di sistema e con la pubblicazione delle "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di Dossier Sanitario"

Questa opera non offre discorsi, quadri interpretativi, spiegazioni o confronti con altre legislazioni, ma unicamente tre tabelle da completare.

Nella prima tabella, **ELENCO DEI CONTROLLI**, sono elencati e suddivisi per area una serie di affermazioni che dovranno essere verificate negli aspetti formali (sono scritte da qualche parte) e negli aspetti sostanziali (c'è evidenza che si applica quanto si è scritto). Dalla verifica scaturisce un giudizio di conformità che ogni organizzazione può articolare come meglio crede, ad esempio:

- 0 = non conforme
- 1 = parzialmente conforme
- 2 = conforme

La seconda tabella, **VALUTAZIONE DEI POSSIBILI RISCHI DERIVANTI DALLE NON CONFORMITA'**, contiene un invito esplicito a valutare rischi e conseguenze a fronte delle non conformità parziali o totali individuate.

La terza tabella infine, offre un semplice strumento per pianificare le necessarie azioni di adeguamento.



*innovation-governance-compliance
ICT & Business Consulting*

<u>PRESENTAZIONE</u>	<u>3</u>
<u>RIESAME DEL DPS</u>	<u>5</u>
<u>ELENCO DEI CONTROLLI</u>	<u>6</u>
<u>VALUTAZIONE DEI POSSIBILI RISCHI DERIVANTI DALLE NON CONFORMITA'</u>	<u>21</u>
<u>INTERVENTI DI ADEGUAMENTO PREVISTI</u>	<u>23</u>

Riesame del DPS

<i>DATA</i>	
<i>NOME AZIENDA</i>	
<i>TITOLARE DEL TRATTAMENTO</i>	
<i>RESPONSABILE DEL TRATTAMENTO</i>	
<i>ALTRI RESPONSABILI DEL TRATTAMENTO</i>	
<i>RESPONSABILE DEL SISTEMA INFORMATIVO</i>	
<i>ALTRI PERTECIPANTI</i>	

ELENCO DEI CONTROLLI

<i>Gestione delle variazioni</i>			
<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
L'organizzazione monitorizza e recepisce le modifiche normative e i nuovi provvedimenti del Garante			
Le modifiche che riguardano l'organizzazione interna, i dati o le modalità di trattamento dei dati, l'inserimento di nuovo personale o la scelta di nuovi fornitori che entrano in contatto con i dati personali sono valutate anche in base alla normativa sul trattamento e protezione dei dati personali			
L'organizzazione aggiorna periodicamente l'elenco dei dati personali trattati			
Ogni modifica che impatta sul sistema di gestione dell'organizzazione e protezione dei dati personali viene opportunamente registrata			
Le misure di sicurezza vengono periodicamente riviste in base all'aggiornamento delle analisi dei rischi			
La procedura di accoglimento del nuovo personale prevede l'istruzione e informazione circa le procedure e norme di riferimento per il trattamento dei dati personali			

DPS, soggetti e incarichi			
Obiettivi di controllo	Evidenza formale	Verifica effettuata	Grado di conformità
Il DPS è stato redatto secondo le indicazioni contenute nelle guide operative messe a disposizione dal Garante ed è disponibile presso l'ufficio del Responsabile del trattamento dati			
L'organizzazione descritta nel DPS rispecchia quella attuale			
Le persone del Responsabile del trattamento e del Custode delle password, sono state formalmente designate			
<p>Per ogni Amministratore di Sistema interno è disponibile la lettera di incarico comprendente al (minimo):</p> <ul style="list-style-type: none"> • Attestazione che l'incaricato ha le caratteristiche richieste dalla legge • Elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato • Indicazioni delle verifiche almeno annuali che il Titolare svolgerà annualmente sulle attività svolte dall'amministratore di sistema • Indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed eventualmente a terzi nei modi richiesti dalla legge 			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Gli estremi identificativi delle persone fisiche nominate "Amministratore di sistema", con l'elenco delle funzioni ad esse attribuite, sono stati riportati nel DPS			
Ogni incaricato al trattamento dati ha ricevuto comunicazione scritta dei dati sensibili e dei relativi trattamenti a cui può accedere in base al proprio ruolo nell'organizzazione			
<i>Informativa, consenso, trattamento dati e amministratori di sistema</i>			
Le informative e la richiesta del consenso al trattamento dei dati personali sono complete e specificano correttamente tutte le finalità del trattamento dei dati in modo coerente rispetto all'effettivo utilizzo, così come previsto dalla legge			
Le informative e la richiesta del consenso sono consegnate sempre preventivamente rispetto al trattamento dei dati			
Sono stati predisposti inventari inerenti le categorie di dati e di soggetti interessati			
Tutti i trattamenti di dati personali effettuati (anche in parte) mediante strumenti elettronici sono censiti e sono indicati i relativi amministratori di sistema.			
Se i trattamenti sono affidati a terze parti, queste hanno comunicato al Titolare l'elenco dei relativi amministratori di sistema			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Se nel trattamento per il trattamento dei dati personali informatizzati, il Titolare si avvale di amministratori di sistemi di società esterne, queste hanno provveduto a comunicare per iscritto l' idoneità (come richiesta dalla legge) delle loro persone a svolgere il ruolo di amministratore di sistema			
Se gli amministratori di sistema operano anche indirettamente su trattamenti di dati personali che riguardano i lavoratori, è stata resa nota e conoscibile l'identità degli amministratori di sistema nell'ambito della propria organizzazione			
E' adottato un idoneo sistema per la registrazione degli accessi logici ai sistemi di elaborazione e agli archivi informatici da parte degli amministratori di sistema			
Tali registrazioni hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste			
Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo non inferiore a 6 mesi			

Misure organizzative di sicurezza			
Obiettivi di controllo	Evidenza formale	Verifica effettuata	Grado di conformità
Esiste un censimento delle aree e dei locali in cui vengono custoditi e trattati i dati con l'evidenza dello stato delle misure di protezione			
L'utilizzo e la custodia dei documenti affidati agli incaricati per lo svolgimento dei loro compiti sono regolamentati			
Sono state impartite ai dipendenti e collaboratori istruzioni scritte sull'utilizzo dei sistemi informatici, della posta elettronica e della navigazione internet e modalità di conservazione e custodia delle password			
Nel caso di trattamento di dati sensibili, gli incaricati sono stati formati ad un utilizzo corretto di tutti i supporti rimovibili presenti nell'organizzazione, illustrando eventualmente le modalità di cancellazione/formattazione degli stessi			
L'organizzazione ha predisposto una comunicazione scritta per sensibilizzare i dipendenti e collaboratori sui rischi di incorrere in reati informatici			
Sono preventivamente autorizzate le persone alle quali è consentito l'accesso agli archivi di dati sensibili, se questi non risultano protetti elettronicamente			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Sono identificati e registrati i soggetti ammessi fuori dall'orario di servizio ai luoghi in cui si svolge il trattamento di dati sensibili			
L'organizzazione ha predisposto procedure per l'accesso agli archivi e la custodia dei locali adibiti alla conservazione di dati sensibili			
La documentazione cartacea contenente dati sensibili è conservata in armadi chiusi a chiave			
Se l'organizzazione non ha affidato a terzi il servizio di riciclo e rottamazione dei PC e affini, ha adottato appropriate misure organizzative e tecniche volte a garantire la sicurezza e protezione dei dati personali			
<i>Sistemi di identificazione, autenticazione e sicurezza informatica</i>			
L'organizzazione ha attivato ed è correttamente funzionante un sistema di autenticazione per ognuno degli incaricati che utilizza strumenti elettronici per il trattamento dei dati personali			
E' stato previsto un sistema di profilazione degli utenti per accedere e trattare esclusivamente i dati previsti dal proprio ruolo			
I codici identificativi sono frequentemente aggiornati inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Nel caso delle password viene verificato che la loro lunghezza minima non sia inferiore a 8 caratteri.			
E' prevista la scadenza di validità della password utilizzata			
E' stata prevista la procedura in cui si individuano chiaramente le modalità in cui il titolare può assicurare la disponibilità dei dati in caso di prolungata assenza degli incaricati			
L'organizzazione si è dotata di un sistema di Firewall, Antivirus e Antispam			
E' previsto un aggiornamento periodico delle release di tutto il software installato con l'indicazione del responsabile dell'attività e la frequenza dell'aggiornamento			
Nell'organizzazione sono vigenti le procedure e gli strumenti per il backup e le prove di ripristino			
L'organizzazione si è dotata di procedure e misure per il ripristino dei dati entro 7 giorni da un eventuale incidente			
<i>Gestione dei rapporti con terze parti</i>			
Se l'organizzazione non svolge in proprio il servizio di riciclo e rottamazione del materiale informatico, ha conferito per iscritto l'incarico ad un terzo di riciclare e rottamare le apparecchiature informatiche autorizzando a cancellare e a non rendere più intelligibili i dati			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Il titolare, quando adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria organizzazione, per provvedere all'esecuzione riceve dal fornitore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del disciplinare tecnico			
È previsto che i soggetti esterni che effettuano attività di manutenzione o installazione non strettamente correlate all'adozione e al mantenimento delle misure minime di sicurezza, rilascino sempre un rapporto dettagliato del loro intervento a garanzia del cliente e di quanto effettuato			
I soggetti esterni a cui sono affidate attività di trattamento dei dati rilasciano idonea dichiarazione scritta dalla quale risulta che dichiarano di ottemperare agli obblighi previsti dal D.Lgs. 196			
Per eventuali trattamenti affidati a terze parti, queste hanno attestato per iscritto di aver effettuato con cadenza almeno annuale, le verifiche sui relativi amministratori di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti di dati personali previste dalle normative vigenti			

Responsabilità del titolare			
<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
E' previsto un piano formativo annuale per ogni figura prevista dal D.Lgs. 196			
L'operato degli amministratori di sistema è verificato, con cadenza almeno annuale, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti			
Il titolare del trattamento si assicura che i responsabili abbiano le caratteristiche giuste per ricoprire i ruoli designati			
Il Titolare del trattamento vigila sui Responsabili affinché rispettino le istruzioni ricevute			
Il titolare del trattamento ha predisposto un'attività periodica di Internal Audit e riesame del DPS			

Solo per Strutture che trattano dati personali di riferiti allo stato di salute			
<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
La struttura ha acquisito il consenso specifico per il trattamento di dati personali connessi all'erogazione delle prestazioni e dei servizi per svolgere attività di prevenzione, diagnosi, cura e riabilitazione			
<p>L'organizzazione ha adottato idonee misure per garantire, nell'erogazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale prevedendo:</p> <ul style="list-style-type: none"> • un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa; • non vengono l'affisse le liste di pazienti nei locali aperti al pubblico • non sono resi facilmente visibili da terzi non legittimati, i documenti riepilogativi delle condizioni cliniche dell'interessato • l'istituzione di appropriate distanze di cortesia 			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
L'organizzazione ha previsto, in conformità agli ordinamenti interni della struttura, adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà			
La struttura ha ottenuto un consenso specifico e distinto per fornire informazioni sullo stato di salute a soggetti diversi dall'interessato			
La struttura ha previsto la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale			
I dati personali idonei a rivelare lo stato di salute sono resi noti all'interessato o ai soggetti sostituiti solo per il tramite (anche in forma scritta) di un medico designato dall'interessato o dal titolare			
Nei casi in cui il titolare o il responsabile autorizza per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato, l'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento dei dati			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Il personale designato è stato istruito anche in ordine alle modalità di consegna a terzi di documenti idonei a rivelare lo stato di salute			
Solo per chi ha adottato il Fascicolo e/o Dossier Sanitario Elettronico			
Gli strumenti sono strutturati in modo che i dati amministrativi sono separati dalle informazioni sanitarie, prevedendo profili diversi di abilitazione degli aventi accesso agli stessi in funzione della differente tipologia di operazioni ad essi consentite			
La struttura richiede il consenso esplicito, autonomo e specifico anche se espresso congiuntamente a quello previsto per il trattamento dei dati ai fini di cura, per la creazione del Fascicolo o Dossier Elettronico			
La struttura ha previsto momenti distinti in cui l'interessato possa esprimere la propria volontà attraverso un consenso di carattere generale per il FSE/Dossier, e di consensi specifici ai fini della sua consultazione o meno da parte di singoli operatori			
E' prevista la possibilità di non far confluire nel FSE/Dossier alcuni specifici eventi clinici. L'oscuramento dell'evento clinico è revocabile nel tempo e avviene con modalità tali da garantire che i soggetti abilitati all'accesso non possano avvenire automaticamente a conoscenza del fatto che l'interessato ha effettuato tale scelta			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Il titolare del trattamento ha informato i soggetti abilitati che i FSE/dossier a cui hanno accesso possono non essere completi in quanto l'interessato potrebbe aver optato per il diritto di oscuramento			
L'inserimento nel FSE/Dossier elettronico delle informazioni relative ad eventi sanitari pregressi, si fonda sul consenso specifico ed informato dell'interessato			
In caso di revoca del consenso, liberamente manifestabile, il FSE/Dossier non è ulteriormente arricchito. I documenti sanitari restano disponibili per l'organismo che li ha redatti e per eventuali conservazioni per obbligo di leggi, ma non sono più condivisi			
Il titolare del trattamento ha previsto le modalità con cui consentire una facile consultazione all'interessato del FSE/Dossier, anche in merito alla facoltà riconosciuta a quest'ultimo di estrarne copia			
Se un insieme di informazioni di base sullo stato di salute sono disponibili a tutti coloro che accedono allo strumento, di questa circostanza l'interessato è edotto nell'informativa			
Il Titolare ha incaricato formalmente le persone designate al trattamento dei dati mediante FSE/Dossier informandole adeguatamente delle particolari modalità di creazione e utilizzazione di tali strumenti			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
All'atto della designazione degli incaricati, il responsabile o il titolare indica con chiarezza l'ambito delle operazioni consentite, avendo cura di specificare se gli stessi abbiano solo la possibilità di consultare o anche di integrare/aggiornare o modificare			
Il titolare ha valutato attentamente quali dati pertinenti, non eccedenti e indispensabili inserire nel FSE/dossier in relazione alle necessità di prevenzione, diagnosi, cura e riabilitazione			
Il titolare rispetta le disposizioni normative a tutela dell'anonimato della persona (vittime di violenza sessuale o pedofilia, persone sieropositive, di chi fa uso di sostanze stupefacenti, di sostanze psicotropiche e di alcool. Il titolare può decidere di non inserire tali informazioni o di inserirle a fronte di una specifica manifestazione di volontà dell'interessato, il quale potrebbe anche richiedere che tali informazioni siano consultabili solo da parte di alcuni soggetti individuati dall'interessato stesso			
Il titolare prevede l'inserimento nel FSE/Dossier di dati e informazioni prodotti da altri organismi e in tal caso è sempre chiaro ed evidente a chi accede la paternità dell'informazione, ovvero del soggetto che l'ha generata			
L'identificazione dei soggetti o delle categorie abilitate a consultare lo strumento è effettuata con chiarezza			

<i>Obiettivi di controllo</i>	<i>Evidenza formale</i>	<i>Verifica effettuata</i>	<i>Grado di conformità</i>
Lo strumento non deve essere consultabile da periti e medici legali, compagnie di assicurazione, datori di lavoro			
L'accesso è sempre consentito a chi ha creato il documento, in ogni caso l'accesso è circoscritto ai soggetti in cura e al periodo di tempo indispensabile per il percorso di cura			
All'interessato è garantita facile modalità di consultazione del proprio FSE/Dossier, nonché di ottenerne copia			
Sono utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi attraverso l'adozione di tecnologie crittografiche o che comunque rendano i dati inintelligibili a soggetti non legittimati			
Sono state adottate procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati			
Sono stati individuati i criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute o la vita sessuale dagli altri dati personali			
E' stato predisposto un sistema per tracciare gli accessi e le operazioni effettuate e un sistema di auditlog per il controllo degli accessi al DB			

VALUTAZIONE DEI POSSIBILI RISCHI DERIVANTI DALLE NON CONFORMITA'

<i>Area di controllo</i>	<i>Grado di conformità</i>	<i>Note sul grado di conformità</i>	<i>Rischi</i>	<i>Conseguenze</i>
Gestione delle variazioni				
DPS, soggetti e incarichi				
Informativa, consenso, trattamento dati e amministratori di sistema				
Misure organizzative di sicurezza				
Sistemi di identificazione, autenticazione e sicurezza informatica				
Gestione dei rapporti con terze parti				
Responsabilità del titolare				

<i>Area di controllo</i>	<i>Grado di conformità</i>	<i>Note sul grado di conformità</i>	<i>Rischi</i>	<i>Impatti</i>
Trattamento di dati sanitari				
Trattamento di dati attraverso il Fascicolo elettronico sanitario (FSE) o Dossier				

Interventi di adeguamento previsti

<i>Obiettivi di controllo</i>	<i>Note sul grado di conformità</i>	<i>Azione</i>	<i>Da realizzare entro il</i>	<i>In carico a</i>