Documento Programmatico sulla Sicurezza

Istituto “Giannina Gaslini”

A norma del Decreto Legislativo 196/2003 e succ. mod.

Indice

Indice delle Tabelle

INTRODUZIONE – Impostazione del Sistema Documentale

All'interno di questa introduzione sono indicate le modalità con cui è stato impostato il presente Documento Programmatico sulla Sicurezza (di seguito indicato con DPS) e i documenti di riferimento.

Il Sistema di Gestione della Sicurezza nel trattamento dei dati personali, sensibili e giudiziari, descritto sul presente DPS e l'adozione delle misure minime previste dal codice, è coordinato dal Gruppo di lavoro Privacy costituito con delibera n. 88 del 18 maggio 2015 che ha altresì dato atto che resta in vigore il presente Documento Programmatico sulla Sicurezza.

Il Gruppo di lavoro Privacy ha il compito di:

- proporre l'aggiornamento dei documenti in materia di sicurezza, e di ogni altro adempimento previsto dalla legge al titolare e per sua disposizione, ai Responsabili;
- predisporre le linee guida e strumenti operativi volti ad assicurare una corretta applicazione della normativa vigente e dei provvedimenti del Garante di interesse per il settore pubblico e sanitario, con riferimento anche al profilo della sicurezza dei dati;
- fornire ai rappresentanti dell'Azienda il supporto giuridico dagli stessi richiesto ed in relazione anche alla predisposizioni di documenti e modulistica;
- monitorare l'applicazione delle disposizioni di legge e delle direttive impartite dall'Azienda attraverso verifiche anche periodiche ed ispezioni assicurando il necessario supporto alla Direzione Generale nei rapporti con il Garante.
- redigere il Documento Programmatico sulla Sicurezza in tutte le sue parti, che sono:
    - Elenco dei dati e dei trattamenti.
    - Analisi dei Rischi.
    - Procedure ed istruzioni operative sulla gestione delle misure minime previste.
    - Istruzioni agli incaricati ed al personale tecnico sulle misure minime di loro competenza.
    - Piani per la Business Continuity.
    - Piani per la Formazione del personale.

- Requisiti richiesti nei contratti con terze parti.

Codifica e conservazione dei Documenti

Tutti i documenti contenuti nel DPS sono contraddistinti da una sigla che identifica la tipologia del documento (modello, procedure ed istruzioni) associata ad un singolo numero che li identifica in maniera univoca.

La sigla viene attribuita secondo il seguente schema:

ALL sta ad indicare che si tratta di un documento contenente informazioni integrative

PRO sta ad indicare che si tratta di un documento che descrive una procedura

IST è un documento relativo alle eventuali istruzioni operative relative ad una specifica procedura

MOD sta ad indicare i modelli di documenti necessari al rapporto con gli interessati al trattamento dei dati

XXX è un numero composto da 3 cifre che contraddistingue la procedura il modello o le istruzioni operative.

Eventuali documenti già in uso nell'istituto potranno essere allegati col loro nome.

Il numero di revisione del documento è riportato in alto a destra dell'intestazione di ogni pagina del DPS.

Prima dell'emissione formale la revisione è 1.0.

Le successive revisioni saranno contrassegnate da un numero progressivo.

Il DPS e tutta la documentazione che lo compone (politiche, procedure, istruzioni, informativa, consensi ecc..) sono conservati all'interno di una cartella (configurata in sola lettura) sulla Intranet dell' Istituto G. Gaslini all'indirizzo http://intranet/default.aspx

A questi documenti deve poter accedere tutto il personale interessato alle gestioni di dati che rientrano nel campo di applicazione del DPS.

Viene deliberato dal CDA e pubblicato all'albo pretorio unitamente alla delibera che lo approva.

Approvazione e revisione della documentazione

Le revisioni a cui sarà soggetto il presente DPS sono curate dal Gruppo di lavoro Privacy (descritto sopra), essendo composto da persone con idonee competenze dal punto di vista normativo, organizzativo e tecnologico. Le revisioni del DPS sono effettuate qualora si renda necessario adeguare le misure di sicurezza a seguito delle mutate esigenze organizzative tecnologiche e strutturali, queste saranno così approvate dall'organo deliberante.

Le revisioni delle istruzioni operative sono proposte dal Gruppo di lavoro Privacy.

Nelle tabelle seguenti, sono riportati gli aggiornamenti a cui è stato sottoposto questo documento con la descrizione delle principali modifiche apportate.

Numero Rev.	Data Rev.	Modifiche apportate	Revisionato da	Approvato con Delibera
1.0	17/03/2006	Prima stesura DPS		
2.0	01/03/2011	Revisione		
3.9	14/12/2015	Revisione		

Tabella 1: Aggiornamenti del DPsS dell' Istituto G. Gaslini

Numero Rev.	Data Rev.	Modifiche apportate	Note
1.0	17/03/2006	Redazione DPS	
2.0	01/03/2011	Aggiornamento riferimenti normative Revisione dei trattamenti effettuati dalle UU.OO. Revisione dell'analisi dei rischi	
3.9	14/12/2015	Riferimenti normativi trattamenti aggiornamento UU.OO.	

Tabella 2: Principali revisioni del documento

CAPITOLO 1 - Struttura ed Organizzazione dell'Istituto

In questa sezione sono elencati i trattamenti che gestiscono dati personali, sensibili e giudiziari, i processi che caratterizzano l'operatività dell'Istituto, e i compiti e le responsabilità delle figure coinvolte, ovvero il Titolare dei trattamenti, il o i Responsabili dei trattamenti, e gli Incaricati dei trattamenti stessi.

SEZIONE 1.1 – Il contesto normativo di riferimento

Principali Riferimenti Legislativi

- Legge 31 dicembre 1996, n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".

- Decreto legislativo 28 luglio 1997, n. 255 "Disposizioni integrative e correttive della L. 31 dicembre 1996, n. 675, in materia di notificazione dei trattamenti di dati personali, a norma dell'art. 1, comma 1, lettera f), L. 31 dicembre 1996, n. 676".

- Decreto legislativo 13 maggio 1998, n. 171 "Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica".

- Decreto legislativo 26 febbraio 1999, n. 51 "Disposizioni integrative e correttive della L. 31 dicembre 1996, n. 675, concernenti il personale dell'Ufficio del Garante per la protezione dei dati personali".

- DPR 28 luglio 1999, n. 318 "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 5, comma 2, della L. 31 dicembre 1996, n. 675".

- Legge 3 novembre 2000, n. 325 “Disposizioni inerenti all’adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall’art. 15 della L: 31 dicembre 1996, n. 675”.

- Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” aggiornato in base ai seguenti provvedimenti:
  - 29/12/2003 Il DECRETO-LEGGE 24 dicembre 2003, n. 354 (in G.U. 29/12/2003, n.300) , convertito con modificazioni dalla L. 26 febbraio 2004, n. 45 (in G.U. 27/2/2004, n. 48)
  - 24/02/2004 Il DECRETO LEGISLATIVO 22 gennaio 2004, n. 42 (in SO n.28, relativo alla G.U. 24/02/2004, n.45) 31/03/2004
  - Il DECRETO-LEGGE 29 marzo 2004, n. 81 (in G.U. 31/03/2004, n.76) , convertito con modificazioni dalla L. 26 maggio 2004, n. 138 (in G.U. 29/5/2004, n. 125) ha disposto (con l'art. 2-quinquies, comma 1 lettera c)) l'introduzione del comma 2-bis dopo il comma 2 all'art. 89.
  - 31/03/2004 Il DECRETO-LEGGE 29 marzo 2004, n. 81 (in G.U. 31/03/2004, n.76) , convertito con modificazioni dalla L. 26 maggio 2004, n. 138 (in G.U. 29/5/2004, n. 125) ha disposto (con l'art. 2-quinquies, comma 1 lettera d)) l'abrogazione della lettera e) comma 1 dell'art. 181.
  - 31/03/2004 Il DECRETO-LEGGE 29 marzo 2004, n. 81 (in G.U. 31/03/2004, n.76) , convertito con modificazioni dalla L. 26 maggio 2004, n. 138 (in G.U. 29/5/2004, n. 125) ha disposto (con l'art. 2-quinquies, comma 1 lettera a)) l'introduzione del comma 1-bis dopo il comma 1 all'art. 37.
  - 31/03/2004 Il DECRETO-LEGGE 29 marzo 2004, n. 81 (in G.U. 31/03/2004, n.76) , convertito con modificazioni dalla L. 26 maggio 2004, n. 138 (in G.U. 29/5/2004, n. 125) ha disposto (con l'art. 2-quinquies comma 1, lettera b)) l'introduzione del comma 2-bis dopo il comma 2 all'art. 83.
  - 25/06/2004 Il DECRETO-LEGGE 24 giugno 2004, n. 158 (in G.U. 25/06/2004, n.147) , convertito con modificazioni dalla L. 27 luglio 2004, n. 188 (in G.U. 30/7/2004, n. 177) ha disposto (con l'art. 3, comma 1 lettera c)) la modifica dell'art. 181 comma 1, lettera a).

- 25/06/2004 Il DECRETO-LEGGE 24 giugno 2004, n. 158 (in G.U. 25/06/2004, n.147) , convertito con modificazioni dalla L. 27 luglio 2004, n. 188 (in G.U. 30/7/2004, n. 177) ha disposto (con l'art. 3, comma 1 lettere a) e b)) la modifica dell'art. 180, commi 1 e 3.
- 10/11/2004 Il DECRETO-LEGGE 9 novembre 2004, n. 266 (in G.U. 10/11/2004, n.264) , convertito con modificazioni dalla L. 27 dicembre 2004, n. 306, (in G.U. 27 dicembre 2004, n. 302) ha disposto (con l'art. 6, comma 1 lettere a) e b)) la modifica dell'art. 180, commi 1 e 3.
- 31/12/2004 Il DECRETO-LEGGE 30 dicembre 2004, n. 314 (in G.U. 31/12/2004, n.306) , convertito con modificazioni dalla L. 1 marzo 2005, n. 26 (in G.U. 2/03/2005, n. 50) ha disposto (con l'art. 6-bis, comma 1 lettere a) e b)) la modifica dell'art. 180 commi 1 e 3.
- 27/07/2005 Il DECRETO-LEGGE 27 luglio 2005, n. 144 (in G.U. 27/07/2005, n.173) , convertito, con modificazioni dalla L. 31 luglio 2005, n. 155 (in G.U. 1/8/2005, n. 177) ha disposto (con l'art. 6, comma 3 lettere a) e b)) la modifica dell'art. 132 comma 1; (con l'art. 6, comma 3 lettere c) e d)) la modifica dell'art. 132, comma 2; (con l'art. 6, comma 3 lettera e)) la modifica dell'art. 132 comma 3; (con l'art. 6, comma 3 lettera f) l'introduzione del comma 4-bis dopo il comma 4 all'art. 132.
- 13/10/2005 Il DECRETO LEGISLATIVO 7 settembre 2005, n. 209 (in SO n.163, relativo alla G.U. 13/10/2005, n.239) ha disposto (con l' art. 352, comma 1) la modifica dell'art. 120, comma 3.
- 30/11/2005 Il DECRETO-LEGGE 30 novembre 2005, n. 245 (in G.U. 30/11/2005, n.279) , convertito con modificazioni dalla L. 27 gennaio 2006, n. 21 (in G.U. 28/01/2006, n. 23) ha disposto (con l'art. 8-bis, comma 2) la modifica dell'art. 181, comma 1 lettera a).
- 30/12/2005 Il DECRETO-LEGGE 30 dicembre 2005, n. 273 (in G.U. 30/12/2005, n.303) , convertito con modificazioni dalla L. 23 febbraio 2006, n. 51 (in S.O. n. 47/L, relativo alla G.U. 28/2/2006, n. 49) ha disposto (con l'art. 10, comma 1 lettera a)) la modifica dell'art. 180 commi 1 e 3
- 30/12/2005 Il DECRETO-LEGGE 30 dicembre 2005, n. 273 (in G.U. 30/12/2005, n.303) , convertito con modificazioni dalla L. 23 febbraio 2006,

n. 51 (in S.O. n. 47/L, relativo alla G.U. 28/2/2006, n. 49) ha disposto (con l'art. 10, comma 1 lettera b)) la modifica dell'art. 181 comma 1 lettera a).

- 13/05/2006 Il DECRETO-LEGGE 12 maggio 2006, n. 173 (in G.U. 13/05/2006, n.110) , convertito con modificazioni dalla L. 12 luglio 2006, n. 228 (in G.U. 12/7/2006, n. 160) ha disposto (con l'art. 1, comma 1) la modifica dell'art. 181, comma 1 lettera a).
- 28/12/2006 Il DECRETO-LEGGE 28 dicembre 2006, n. 300 (in G.U. 28/12/2006, n.300) , convertito con modificazioni con L. 26 febbraio 2007, n. 17 (in S.O. n. 48/L, relativo alla G.U. 26/2/2007, n. 47) ha disposto (con l'art. 6) la modifica dell'art. 181, comma 1 lettera a).
- 31/12/2007 Il DECRETO-LEGGE 31 dicembre 2007, n. 248 (in G.U. 31/12/2007, n.302) Il D.L. 31 dicembre 2007, n. 248 (in G.U. 31/12/2007, n. 302) convertito con modificazioni con L. 28 febbraio 2008, n. 31 (in S.O. n. 47/L, relativo alla G.U. 29/2/2008, n. 51) ha disposto (con l'art. 47-quater) la modifica dell'art. 153.
- 04/04/2008 La LEGGE 18 marzo 2008, n. 48 (in SO n.79, relativo alla G.U. 04/04/2008, n.80) ha disposto (con l'art. 10, comma 1) l'introduzione dei commi 4-ter, 4-quater, 4-quinquies dopo il comma 4-bis.
- 18/06/2008 Il DECRETO LEGISLATIVO 30 maggio 2008, n. 109 (in G.U. 18/06/2008, n.141) ha disposto (con l'art. 4) la modifica dell'art. 154 comma 1 lettera a).
- 18/06/2008 Il DECRETO LEGISLATIVO 30 maggio 2008, n. 109 (in G.U. 18/06/2008, n.141) ha disposto (con l'art. 2, comma 1 lettera a)) la modifica dell' art. 132 coma 1; (con l'art. 2, comma 1 lettera b)) l'introduzione del comma 1-bis dopo il comma 1;(con l'art. 2, comma 1 lettera c)) l'abrogazione dei commi 2, 4 e 4-bis dell'art. 132; (con l'art. 2, comma 1 lettera d) la modifica dell'art. 132, comma 5; (con l'art. 2, comma 2) la soppressione delle lettere b) e c) comma 5 dell'art. 132; (con l'art. 2, comma 3) la modifica del comma 5 lettera d) dell'art. 132.
- 18/06/2008 Il DECRETO LEGISLATIVO 30 maggio 2008, n. 109 (in G.U. 18/06/2008, n.141) ha disposto (con l'art. 5) l'introduzione dell'art. 162-bis.

- 18/06/2008 Il DECRETO LEGISLATIVO 30 maggio 2008, n. 109 (in G.U. 18/06/2008, n.141) ha disposto (con l'art. 6, comma 3) la modifica dell'art. 132 comma 1-bis.
- 25/06/2008 Il DECRETO-LEGGE 25 giugno 2008, n. 112 (in SO n.152, relativo alla G.U. 25/06/2008, n.147) Il D.L. 25 giugno 2008, n. 112 (in S.O. n. 152, relativo alla G.U. 25/6/2008, n. 147) convertito, con modificazioni, dalla L. 6 agosto 2008, n. 133 (in S.O. n. 196, relativo alla G.U. 21/8/2008, n. 195) ha disposto (con l'art. 29) la modifica degli artt. 34, 36, 38 e 44.
- 02/10/2008 Il DECRETO-LEGGE 2 ottobre 2008, n. 151 (in G.U. 02/10/2008, n.231) , convertito con modificazioni dalla L. 28 novembre 2008, n. 186 (in G.U. 1/12/2008, n. 281), nel modificare l'art. 6, comma 3 del D.Lgs. 30 maggio 2008, n. 109 (in G.U. 18/6/2008, n. 141), ha conseguentemente disposto (con l'art. 1, comma 1, lettera a)) la modifica dell'art. 132, comma 1-bis.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 3 lettera a)) la modifica dell'art. 162, comma 1; (con l'art.44, comma 3 lettera b)) la modifica dell'art. 162, comma 2; (con l'art. 44, comma 3 lettera c)) l'introduzione dei commi 2-bis e 2-ter dopo il comma 2 dell'art. 162.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni dalla L. 27 febbraio 2009, n. 14 (in S.O. n. 28, relativo alla G.U. 28/2/2009, n. 49), ha disposto (con l'art. 44, comma 1-bis) la modifica dell'art. 23.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 2) la modifica dell'art. 161.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 4) la modifica dell'art. 162-bis, comma 1.

- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni dalla L. 27 febbraio 2009, n. 14 (in S.O. n. 28, relativo alla G.U. 28/2/2009, n. 49), ha disposto (con l'art. 44, comma 1-bis) la modifica dell'art. 13.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 6) la modifica dell'art. 164, comma 1.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 5) la modifica dell'art. 163, comma 1.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 8) la modifica dell'art. 165, comma 1.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 9 lettera a)) la modifica dell'art. 169, comma 1; (con l'art. 44, comma 9 lettera b)) la modifica dell'art. 169, comma 2.
- 31/12/2008 Il DECRETO-LEGGE 30 dicembre 2008, n. 207 (in G.U. 31/12/2008, n.304) , convertito con modificazioni con L. 27 febbraio 2009, n. 14 (in S.O. n. 28/L, relativo alla G.U. 28/2/2009, n. 49) ha disposto (con l'art. 44, comma 7) l'introduzione dell'art. 164-bis.
- 05/03/2009 La LEGGE 4 marzo 2009, n. 15 (in G.U. 05/03/2009, n.53) ha disposto (con l'art. 4, comma 9) la modifica dell'art. 1, comma 1.
- 25/09/2009 Il DECRETO-LEGGE 25 settembre 2009, n. 135 (in G.U. 25/09/2009, n.223) ,convertito con modificazioni dalla L. 20 novembre 2009, n. 166 (in S.O. n. 215/L relativo alla G.U. 24/11/2009, n. 274) ha disposto (con l'art. 20-bis comma 1 lettera a)) la modifica dell'art. 130 comma 3, (con l'art. 20-bis comma 1 lettera b)) l'introduzione dei commi 3-bis, 3-ter, 3-quater

dopo il comma 3; (con l'art. 20-bis comma 2) la modifica dell'art. 130, comma 3-bis.

- 25/09/2009 Il DECRETO-LEGGE 25 settembre 2009, n. 135 (in G.U. 25/09/2009, n.223) ,convertito con modificazioni dalla L. 20 novembre 2009, n. 166 (in S.O. n. 215/L relativo alla G.U. 24/11/2009, n. 274) ha disposto (con l'art. 20-bis comma 1 lettera c) la modifica dell'art. 162 comma 2-bis e l'introduzione del comma 2-quater dopo il comma 2-ter.
- 25/09/2009 Il DECRETO-LEGGE 25 settembre 2009, n. 135 (in G.U. 25/09/2009, n.223) , convertito con modificazioni dalla L. 20 novembre 2009, n. 166 (in S.O. n. 215, relativo alla G.U. 24/11/2009, n. 274), nel modificare l'art. 44, comma 1-bis del D.L. 30 dicembre 2008, n. 207, convertito con modificazioni dalla L. 27 febbraio 2009, n. 14 (in S.O. n. 28, relativo alla G.U. 28/2/2009, n. 49), ha conseguentemente disposto (con l'art. 20-bis, comma 3) la modifica dell'art. 13.
- 25/09/2009 Il DECRETO-LEGGE 25 settembre 2009, n. 135 (in G.U. 25/09/2009, n.223) , convertito con modificazioni dalla L. 20 novembre 2009, n. 166 (in S.O. n. 215, relativo alla G.U. 24/11/2009, n. 274), nel modificare l'art. 44, comma 1-bis del D.L. 30 dicembre 2008, n. 207, convertito con modificazioni dalla L. 27 febbraio 2009, n. 14 (in S.O. n. 28, relativo alla G.U. 28/2/2009, n. 49), ha conseguentemente disposto (con l'art. 20-bis, comma 3) la modifica dell'art. 23.
- 29/07/2010 La LEGGE 29 luglio 2010, n. 120 (in SO n.171, relativo alla G.U. 29/07/2010, n.175) ha disposto (con l'art. 58, comma 1, lettera a)) la modifica dell'art. 74, comma 1;(con l'art. 58, comma 1, lettera b)) la modifica dell'art. 74, comma 2.
- 09/11/2010 La LEGGE 4 novembre 2010, n. 183 (in SO n.243, relativo alla G.U. 09/11/2010, n.262) ha disposto (con l'art. 14, comma 1, lettera b)) l'introduzione del comma 3-bis all'art. 19.
- 09/11/2010 La LEGGE 4 novembre 2010, n. 183 (in SO n.243, relativo alla G.U. 09/11/2010, n.262) ha disposto (con l'art. 1, comma 1, lettera a)) la modifica dell'art. 1, comma 1.
- 13/05/2011 Il DECRETO-LEGGE 13 maggio 2011, n. 70 (in G.U. 13/05/2011, n.110) , convertito con modificazioni dalla L. 12 luglio 2011, n.

106 (in G.U. 12/07/2011, n. 160), ha disposto (con l'art. 6, comma 2, lettera a)) la modifica dell'art. 24, comma 1, lettera g) e l'introduzione delle lettere i-bis) e i-ter) all'art. 24, comma 1.

- 13/05/2011 Il DECRETO-LEGGE 13 maggio 2011, n. 70 (in G.U. 13/05/2011, n.110) , convertito con modificazioni dalla L. 12 luglio 2011, n. 106 (in G.U. 12/07/2011, n. 160), ha disposto (con l'art. 6, comma 2, lettera a)) l'introduzione della lettera b-bis) all'art. 26, comma 3.
- 13/05/2011 Il DECRETO-LEGGE 13 maggio 2011, n. 70 (in G.U. 13/05/2011, n.110) , convertito con modificazioni dalla L. 12 luglio 2011, n. 106 (in G.U. 12/07/2011, n. 160), ha disposto (con l'art. 6, comma 2, lettera a)) l'introduzione del comma 3-bis all'art. 5.
- 13/05/2011 Il DECRETO-LEGGE 13 maggio 2011, n. 70 (in G.U. 13/05/2011, n.110) , convertito con modificazioni dalla L. 12 luglio 2011, n. 106 (in G.U. 12/07/2011, n. 160), ha disposto (con l'art. 6, comma 2, lettera a)) la modifica dell'art. 130, comma 3-bis.
- 13/05/2011 Il DECRETO-LEGGE 13 maggio 2011, n. 70 (in G.U. 13/05/2011, n.110) , convertito con modificazioni dalla L. 12 luglio 2011, n. 106 (in G.U. 12/07/2011, n. 160), ha disposto (con l'art. 6, comma 2, lettera a)) l'introduzione del comma 5-bis all'art. 13.
- 13/05/2011 Il DECRETO-LEGGE 13 maggio 2011, n. 70 (in G.U. 13/05/2011, n.110) , convertito con modificazioni dalla L. 12 luglio 2011, n. 106 (in G.U. 12/07/2011, n. 160), ha disposto (con l'art. 6, comma 2, lettera a)) la modifica dell'art. 34, comma 1-bis e l'introduzione del comma 1-ter all'art. 34.
- 21/09/2011 Il DECRETO LEGISLATIVO 1 settembre 2011, n. 150 (in G.U. 21/09/2011, n.220) ha disposto (con l'art. 36, commi 1 e 2) la modifica dell'art. 152, commi 1,1-bis, 2,3,4,5,6,7,8,9,10,11,12,13 e 14.
- 21/09/2011 Il DECRETO LEGISLATIVO 1 settembre 2011, n. 150 (in G.U. 21/09/2011, n.220) ha disposto (con l'art. 34, comma 9, lettera a)) la modifica dell'art. 152, comma 1; (con l'art. 34, comma 9, lettera b)) l'introduzione del comma 1-bis all'art. 152;(con l'art. 34, comma 9, lettera c)) l'abrogazione dei commi 2,3,4,5,6,7,8,9,10,11,12,13 e 14 dell'art. 152.

- 06/12/2011 Il DECRETO-LEGGE 6 dicembre 2011, n. 201 (in SO n.251, relativo alla G.U. 06/12/2011, n.284) , convertito con modificazioni dalla L. 22 dicembre 2011, n. 214 (in S.O. n. 276, relativo alla G.U. 27/12/2011 n. 300), ha disposto (con l'art. 40, comma 2, lettera d)) la modifica dell'art. 9, comma 4.
- 06/12/2011 Il DECRETO-LEGGE 6 dicembre 2011, n. 201 (in SO n.251, relativo alla G.U. 06/12/2011, n.284) , convertito con modificazioni dalla L. 22 dicembre 2011, n. 214 (in S.O. n. 276, relativo alla G.U. 27/12/2011 n. 300), ha disposto (con l'art. 40, comma 2, lettera c)) l'abrogazione del comma 3-bis dell'art. 5.
- 06/12/2011 Il DECRETO-LEGGE 6 dicembre 2011, n. 201 (in SO n.251, relativo alla G.U. 06/12/2011, n.284) , convertito con modificazioni dalla L. 22 dicembre 2011, n. 214 (in S.O. n. 276, relativo alla G.U. 27/12/2011 n. 300), ha disposto (con l'art. 40, comma 2, lettera a)) la modifica dell'art. 4, comma 1, lettera b); (con l'art. 40, comma 2, lettera b)) la modifica dell'art. 4, comma 1, lettera i).
- 06/12/2011 Il DECRETO-LEGGE 6 dicembre 2011, n. 201 (in SO n.251, relativo alla G.U. 06/12/2011, n.284) , convertito con modificazioni dalla L. 22 dicembre 2011, n. 214 (in S.O. n. 276, relativo alla G.U. 27/12/2011 n. 300), ha disposto (con l'art. 40, comma 2, lettera e)) la soppressione della lettera h) del comma 1 dell'art. 43.
- 09/02/2012 Il DECRETO-LEGGE 9 febbraio 2012, n. 5 (in SO n.27, relativo alla G.U. 09/02/2012, n.33) , convertito con modificazioni dalla L. 4 aprile 2012, n. 35 (in SO n. 69, relativo alla G.U. 06/04/2012, n. 82), ha disposto (con l'art. 45, comma 1, lettera a)) l'introduzione del comma 1-bis all'art. 21.
- 09/02/2012 Il DECRETO-LEGGE 9 febbraio 2012, n. 5 (in SO n.27, relativo alla G.U. 09/02/2012, n.33) , convertito con modificazioni dalla L. 4 aprile 2012, n. 35 (in SO n. 69, relativo alla G.U. 06/04/2012, n. 82), ha disposto (con l'art. 45, comma 1, lettera c)) la soppressione della lettera g) dell'art. 34, comma 1, e l' abrogazione del comma 1-bis dell'art. 34.
- 09/02/2012 Il DECRETO-LEGGE 9 febbraio 2012, n. 5 (in SO n.27, relativo alla G.U. 09/02/2012, n.33) , convertito con modificazioni dalla L. 4 aprile

2012, n. 35 (in SO n. 69, relativo alla G.U. 06/04/2012, n. 82), ha disposto (con l'art. 45, comma 1, lettera b)) la modifica dell'art. 27, comma 1.

- 09/02/2012 Il DECRETO-LEGGE 9 febbraio 2012, n. 5 (in SO n.27, relativo alla G.U. 09/02/2012, n.33) , convertito con modificazioni dalla L. 4 aprile 2012, n. 35 (in SO n. 69, relativo alla G.U. 06/04/2012, n. 82), ha disposto (con l'art. 45, comma 1, lettera d)) la modifica dell'Allegato B.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 10) la modifica dell'art. 164-bis, comma 1.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'art. 127, commi 1, 2, 3 e 4.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'art. 126, commi 1 e 3.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, coma 11) la modifica dell'art. 168, comma 1.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 9) l'introduzione dell'art. 162-ter.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 5, lettera a)) la modifica dell'art. 122, comma 1; (con l'art. 1, comma 5, lettera b)) la modifica dell'art. 122, comma 2; (con l'art. 1, comma 5, lettera c)) l'introduzione del comma 2-bis all'art. 122; (con l'art. 1, comma 12) la modifica della rubrica dell'art. 122.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'art. 129, comma 2.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 3) l'introduzione dell'art. 32-bis.

- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 1, lettera a)) la modifica dell'art. 4, comma 2, lettere b), c), d) e i); (con l'art. 1, comma 1, lettera b)) l'introduzione della lettera g-bis) al comma 3 dell'art. 4; (con l'art. 1, comma 12) la modifica dell'art. 4, comma 2, lettere a) e f).
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 4) la modifica dell'art. 121, comma 1.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'art. 128, comma 1.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'art. 125, commi 1, 2, 3 e 4.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 2, lettera a)) la modifica della rubrica dell'art. 32; (con l'art. 1, comma 2, lettera b)) la modifica dell'art. 32, comma 1; (con l'art. 1, comma 2, lettera c)) l'introduzione dei commi 1-bis e 1-ter all'art. 32; (con l'art. 1, comma 2, lettera d)) la modifica dell'art. 32, comma 3.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 8) l'introduzione dell'art. 132-bis.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'art. 131, commi 1 e 2.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 7, lettera a)) la modifica dell'art. 130, comma 1; (con l'art. 1, comma 7, lettera b)) la modifica dell'art. 130, comma 5.

- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'art. 124, commi 1, 3 e 4.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 12) la modifica dell'Allegato C.
- 31/05/2012 Il DECRETO LEGISLATIVO 28 maggio 2012, n. 69 (in G.U. 31/05/2012, n.126) ha disposto (con l'art. 1, comma 6) la modifica dell'art. 123, comma 3;(con l'art. 1, comma 12) la modifica dell'art. 123, commmi 2, 3 e 4.
- 05/04/2013 Il DECRETO LEGISLATIVO 14 marzo 2013, n. 33 (in G.U. 05/04/2013, n.80) ha disposto (con l'art. 53, comma 1, lettera e)) l'abrogazione del comma 3-bis dell'art. 19.
- 27/12/2013 La LEGGE 27 dicembre 2013, n. 147 (in SO n.87, relativo alla G.U. 27/12/2013, n.302) ha disposto (con l'art. 1, comma 1) la modifica dell'art. 156, comma 2.
- 19/02/2015 Il DECRETO-LEGGE 18 febbraio 2015, n. 7 (in G.U. 19/02/2015, n.41) , convertito con modificazioni dalla L. 17 aprile 2015, n. 43 (in G.U. 20/04/2015, n. 91), ha disposto (con l'art. 4-bis, commi 1 e 3) la modifica dell'art. 132, comma 1.

19/02/2015 Il DECRETO-LEGGE 18 febbraio 2015, n. 7 (in G.U. 19/02/2015, n.41) , convertito con modificazioni dalla L. 17 aprile 2015, n. 43 (in G.U. 20/04/2015, n. 91), ha disposto (con l'art. 7, comma 1) la modifica dell'art. 53.

Principali riferimenti autorizzativi

- Autorizzazione generale n. 1/2014 al trattamento dei dati sensibili nei rapporti di lavoro 11 dicembre 2014
- Autorizzazione generale n. 2/2014 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - 11 dicembre 2014

- Autorizzazione n. 7/2014 - Autorizzazione al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici - 11 dicembre 2014
- Autorizzazione generale n. 9/2014 al trattamento dei dati personali effettuato per scopi di ricerca scientifica - 11 dicembre 2014
- Autorizzazione generale n. 8/2014 al trattamento dei dati genetici - 11 dicembre 2014
- Autorizzazione n. 9/2014 - Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica - 11 dicembre 2014

Il contesto normativo

Il quadro normativo italiano sulla privacy non si limita al Codice ed ai suoi allegati perché il Garante per la protezione dei dati personali può adottare **provvedimenti** che assumono valore normativo. Inoltre, spesso il Garante, attraverso il suo sito, pubblica linee guida, modelli o anticipa contenuti su iniziative legislative in corso.

L'elenco completo[1] dei provvedimenti è disponibile presso il sito del Garante. Il Garante per la protezione dei dati personali ha predisposto sul proprio sito una sezione che raccoglie documenti di interesse in materia di protezione dei dati personali e presenta i convegni, le iniziative di formazione e sensibilizzazione promosse dal Garante o le iniziative e gli eventi cui partecipa l'Autorità[2].

Di seguito sono riportati, in ordine cronologico alcuni dei provvedimenti e delle "pubblicazioni" più importanti sulla Sicurezza rimandando al sito del garante per ogni approfondimento e aggiornamento.

Data	Argomento
2 luglio 2015	**Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche -** (Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015)
4 giugno 2015	**Dossier sanitario elettronico**: più tutele per i pazienti Il Garante Privacy adotta le nuove linee guida: consenso informato, accessi tracciati, immediata comunicazione dei data breach,

[1] http://www.garanteprivacy.it/home/provvedimenti-normativa/provvedimenti
[2] http://www.garanteprivacy.it/web/guest/home/attivita-e-documenti

Data	Argomento
	(Pubblicato sulla Gazzetta Ufficiale n. 164 del 17 luglio 2015)
14 marzo 2013	**Decreto legislativo 14 marzo 2013, n. 33.** Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni
28 maggio 2012	**Decreto legislativo 28 maggio 2012 , n. 69** Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 (..) (Gazzetta Ufficiale n. 126 del 31 maggio 2012)
25 giugno 2009	**Modifiche** del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di **amministratore di sistema** e proroga dei termini per il loro adempimento - 25 giugno 2009[3]
12 marzo 2009	Prescrizioni ai titolari di **banche dati** costituite **sulla base di elenchi telefonici** formati prima del 1° agosto 2005 a seguito della deroga introdotta dall'art. 44 d.l. n. 207/2008 - 12 marzo 2009[4]
30 dicembre 2008	Inasprimento delle sanzioni privacy[5] D.L. n. 207 del 30 dicembre 2008 (articolo 44)
24 dicembre 2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle **funzioni di amministratore di sistema**
27 novembre 2008	Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali
13 ottobre 2008	Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali[6]

[3] http://www.garanteprivacy.it/garante/doc.jsp?ID=1626595
[4] http://www.garanteprivacy.it/garante/doc.jsp?ID=1598808
[5] G.U. n. 300 del 24 dicembre 2008

Data	Argomento
gennaio 2008	Sicurezza dei dati di traffico telefonico e telematico[7]
luglio 2007	Privacy e pubblico impiego: le linee guida del Garante
marzo 2007	Linee guida del Garante per posta elettronica e internet

Tabella 3: Aggiornamenti della normativa privacy

Gli adempimenti per le funzioni di "amministratore di sistema"

Sulla Gazzetta Ufficiale n. 300 del **24 dicembre 2008** è pubblicato il testo del **provvedimento del 27 novembre 2008** del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"[8].
Il Garante ha rilevato l'esigenza di intraprendere una specifica attività rispetto ai soggetti preposti ad attività riconducibili alle mansioni tipiche dei cosiddetti "**amministratori di sistema**" nonché di coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati, evidenziandone la rilevanza rispetto ai trattamenti di dati personali anche allo scopo di promuovere presso i relativi titolari e nel pubblico la consapevolezza della delicatezza di tali peculiari mansioni nella "Società dell'informazione" e dei rischi a esse associati.
Di conseguenza il Garante impone nuovi adempimenti ai titolari di trattamenti effettuati (anche parzialmente) con strumenti elettronici. I nuovi adempimenti **non riguardano** i titolari destinatari delle recenti "semplificazioni" sugli obblighi privacy.
Le misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici sono le seguenti:

1. **Valutazione delle caratteristiche soggettive.** L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. Anche quando le funzioni di

[6] http://www.garanteprivacy.it/garante/doc.jsp?ID=1571960
[7] http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111
[8] http://www.garanteprivacy.it/garante/doc.jsp?ID=1580831

amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

2. **Designazioni individuali.** La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

3. **Elenco degli amministratori di sistema.** Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati nel presente **Documento Programmatico sulla Sicurezza** da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante. Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in Gazzetta Ufficiale 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore. Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

4. **Verifica delle attività.** L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari

del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

5. **Registrazione degli accessi.** Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

6. **Tempi di adozione delle misure e degli accorgimenti.** Per tutti i titolari dei trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, le misure e gli accorgimenti (…) devono essere introdotti al più presto e comunque entro, e non oltre, il termine che è congruo stabilire, in **centoventi giorni** dalla medesima data. Per tutti gli altri trattamenti con inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

Il **26 giugno 2009** il Garante per la protezione dei dati personali, attraverso un "comunicato stampa"[9] ha integrato e **parzialmente modificato** il provvedimento relativo agli "amministratori di sistema", recependo alcune indicazioni pervenute, anche da associazioni di categoria, nel corso della consultazione pubblica conclusasi il 31 maggio. Con le nuove disposizioni[10] il Garante intende facilitare il corretto adempimento alle prescrizioni impartite, mantenendo comunque elevato il livello di protezione dei dati personali e le garanzie per i cittadini.
L'autorità, in particolare, **ha consentito che gli adempimenti** connessi all'individuazione degli amministratori di sistema e alla tenuta dei relativi elenchi **possano essere effettuati,**

[9] http://www.garanteprivacy.it/garante/doc.jsp?ID=1626716
[10] http://www.garanteprivacy.it/garante/doc.jsp?ID=1626595

oltre che dai titolari, anche dai responsabili del trattamento. Ciò allo scopo di rendere tali obblighi più agevoli per quelle realtà aziendali nelle quali determinati servizi informatici vengono svolti da società esterne.

In questo contesto, l'Istituto ha provveduto:

- alla redazione dell'elenco degli Amministratori di sistema, includendo sia il personale interno che il nominativo delle società esterne che operano in qualità di outsourcer per i sistemi in ambito;
- alla nomina formale degli Amministratori (lettera controfirmata per accettazione dell'incarico);
- all'identificazione dei sistemi in ambito (apparati di rete/sicurezza, sistemi server, database server).

Successivamente ha implementato la soluzione tecnologica necessaria per la raccolta e la conservazione dei log di accesso per garantirne completezza, integrità e inalterabilità. Ha predisposto il processo di verifica annuale in modo tale che sia possibile controllare la rispondenza delle misure organizzative, tecniche e di sicurezza implementate rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

SEZIONE 1.2 - Elenco dei trattamenti di dati personali

I trattamenti di dati personali posti in essere dall'Istituto Giannina Gaslini sono contenuti nell'allegato elenco e sono riportati, per ogni Livello di assistenza individuato in base al DCPM 29/11/01, nelle tabelle seguenti. Sono riportate anche tabelle relative ai trattamenti di dati nell'ambito di strutture operative non sanitarie. Oltre a queste informazioni, vengono riportate altre informazioni comunque rilevanti secondo quanto indicato negli articoli 33, 34, 35 e 36 del Codice, e per quanto riguarda le misure minime di sicurezza. Queste informazioni sono relative a: gli strumenti utilizzati nei trattamenti ed i supporti impiegati per la conservazione dei dati.

Finalità del trattamento

I dati personali, nell'ambito delle attività svolte e delle prestazioni fornite dall'Istituto, sono trattati esclusivamente per le seguenti finalità:

- Tutela della salute;

- Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione;
- Assistenza socio-sanitaria;
- Ricerca scientifico-sanitaria;
- Raccolta conservazione e distribuzione di materiali biologici (Biobanche genetiche)
- Formazione;
- Gestione del personale e dei collaboratori esterni;
- Amministrativo e contabili;
- Supporto sistema informatico;
- Informazione su servizi e attività dell'ente anche con possibilità di profilazione.

Unità Operativa Complessa – Anatomia Patologica f.f. Dott.ssa Sementa Angela		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Attività generale globale:Diagnostica citologica,Diagnostica istologica e Riscontri autoptici. Attività clinica e aree di eccellenza: Anatomia e Istologia Patologica. Gestione cartelle cliniche.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (Procedura informatica fornita dalla società Dedalus con dati su database database Oracle centralizzato. Utilizzo di archivi informatici locali) Supporti cartacei	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete aziendale

Unità Operativa Complessa – Anestesia e rianimazione neonatale pediatrica Dott. Tuo Pietro		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Visite anestesiologica in regime day-surgery e ricovero ordinario; anestesia in Sala Operatoria e decorso post operatorio; anestesia/sedazione per procedure in regime di day surgery; analgesia del parto; assistenza del neonato in Sala Parto e in Sala Operatoria. Servizio terapia del dolore. Gestione cartelle cliniche.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Cardiochirurgia Prof. Zannini Lucio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Diagnosi e della cura dei bambini con cardiopatie congenite o acquisite in età pediatrica. Interventi al cuore e corregge le malformazioni vascolari congenite o acquisite. Ricerca clinica su vari aspetti della circolazione extracorporea e della protezione miocardica Gestione cartelle cliniche. Gestione sala operatoria. Gestione andamento saturazione del Paziente
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Database Cardiologico interno "Cardiobase" Software di gestione cateterismo Cardiaco (Pedcat) ed ecografica (XCelera) Supporti cartacei	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Cardiologia Dott. Marasini Maurizio Francesco		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Diagnosi e della cura dei bambini con cardiopatie congenite o acquisite in età pediatrica. Interventi al cuore e corregge le malformazioni vascolari congenite o acquisite. Ricerca clinica su vari aspetti della circolazione extracorporea e della protezione miocardica Gestione cartelle cliniche. Gestione sala operatoria. Gestione andamento saturazione del Paziente
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Database Cardiologico interno "Cardiobase" Software di gestione cateterismo Cardiaco (Pedcat) ed ecografica (XCelera) Supporti cartacei	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Chirurgia f.f. Prof Mattioli Girolamo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Chirurgia Generale, Chirurgia Toracica, Urologia, Chirurgia Oncologica, Trauma center e chirurgia d'urgenza, Chirurgia Neonatale, Chirurgia Mini-invasiva, Day Surgery, Attività di Day Hospital e Attività Ambulatoriale. Gestione cartelle cliniche cartace e Gestione dati pazienti informatizzata.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Clinica Pediatrica f.f. Dott. Del Buono Silvio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Visite ambulatoriali, day hospital e ricovero ordinario per: Prevenzione, diagnosi e alla cura delle alterazioni della crescita e dello sviluppo, obesità, patologie allergiche alimentari e respiratorie; diagnosi e cura, in tema di diabetologia, fibrosi cistica, errori congeniti del metabolismo, adolescentologia e patologia dello sviluppo. Gestione cartelle cliniche.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Dermatologia Dott. Occella Corrado		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione Day Hospital, visite ambulatoriali. Laserterapia, fototerapia, Chirurgia dermatologica, Dermatoscopia, Diagnostica micologica, Diagnostica allergologica, Videodermatoscopia in epiluminescenza. Trattamento degli emangiomi infantili e malformazioni vascolari.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Ematologia f.f. Dott. Dufour Carlo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Assistenza e cura ai bambini per: Tumori solidi e linfomi; malattie del sangue; Trattamento delle coagulopatie emorragiche, piastrinopenie immuni croniche e acute e trombofilie; Trapianto di Cellule Staminali Emopoietiche; Studio di alterazioni citogenetiche; Individuazione di indicatori citogenetici prognostici, studio di riarrangiamenti cromosomici e relativi coinvolgimenti. Ricerca negli stessi settori. Day Hospital di ematologia-oncologia pediatrica; Assistenza domiciliare
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Banca dati pazienti emofiliaci. Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Utilizzo ed accesso alla Cartella Oncologica (Oncosys) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Oncologia f.f. Dott. Garaventa Alberto		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Assistenza e cura ai bambini per: Tumori solidi e linfomi; malattie del sangue; Trattamento delle coagulopatie emorragiche, piastrinopenie immuni croniche e acute e trombofilie; Trapianto di Cellule Staminali Emopoietiche; Studio di alterazioni citogenetiche; Individuazione di indicatori citogenetici prognostici, studio di riarrangiamenti cromosomici e relativi coinvolgimenti. Ricerca negli stessi settori. Day Hospital di ematologia-oncologia pediatrica; Assistenza domiciliare
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di database centralizzati; gestione di database locali) Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Utilizzo ed accesso alla Cartella Oncologica (Oncosys) Banca dati pazienti emofiliaci. Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa– Farmacia f.f. Dott.ssa Barabino Paola		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione magazzino farmacia (OASI) Visione dati pazienti con procedura GST Assistenza farmaceutica territoriale ed ospedaliera, Sperimentazione clinica dei medicinali, Farmacovigilanza e rilevazioni reazioni avverse a vaccino, Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'attività l'assistenza ai neuropatici cronici in trattamento dialitico
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione OASI per la gestione di database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Oncologica (Oncosys) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Immunologia e medicina trasfusionale Dott. Tripodi Gino		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Esecuzione esami di laboratorio per pazienti interni ed esterni . Prestazioni ambulatoriali di assistenza. Gestione prodotti trasfusionali. Gestione donatori di sangue.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione Emonet per la gestione di specifico database centralizzato per l'area trasfusionale; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Laboratorio analisi f.f. Dott. Tripodi Gino		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Esecuzione esami di laboratorio per pazienti interni ed esterni . Prestazioni ambulatoriali di assistenza.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione NBBS e Concerto Anatomia patologica e laboratorio di analisi) per la gestione di specifici database centralizzati; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Genetica Medica Prof. Ravazzolo Roberto		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Ricerca scientifico-sanitaria su malattie genetiche rare e le sue applicazioni nella diagnostica e nello sviluppo di eventuali approcci terapeutici	Identificazione di geni, messa a punto metodi diagnostici per ,alattie ereditarie monogeniche, messa a punto nuovi metodi diagnostici mediante tecnologia Next Generation Sequencing, studi di anomalie citogenetiche resposanbili di malattie rare, studi su approcci di genomica funzionale per identificare inter-relazioni tra geni e malattia
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione NBBS e Concerto Anatomia patologica e laboratorio di analisi) per la gestione di specifici database centralizzati; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Laboratorio Biologia Molecolare Dott. Varesio Luigi		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Ricerca scientifico-sanitaria	- Database BIT - Refertazione ipossia - Valutazioni esosomi
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione NBBS e Concerto Anatomia patologica e laboratorio di analisi) per la gestione di specifici database centralizzati; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei Server decicato Biobanca BIT
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	Server decicato Biobanca BIT PC in rete GRID PC in rete locale

Unità Operativa Complessa – Immunologia clinica e sperimentale Prof.ssa Bottino Cristina		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Ricerca scientifico-sanitaria Attività di ricerca preclinica	Tipizzazione dei recettori KIR Analisi fenotipica e funzionale dei Linfociti Natural Killer
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (database centralizzati e locali) Supporti cartacei	Archivi cartacei Sistemi client per i dati informatici gestiti su database locali
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☐ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	MAC non in rete

Unità Operativa Complessa – Laboratorio Cellule Staminali Post natali e terapie Cellulari f.f. Dott. Frassoni Francesco		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Ricerca scientifico-sanitaria Attività di ricerca preclinica e clinica	Colture cellule staminali. Conservazione, manipolazione genetica, terapia genica cellulare
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione NBBS e Concerto Anatomia patologica e laboratorio di analisi) per la gestione di specifici database centralizzati; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Laboratorio Oncologia Dott. Pistoia Vito		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Ricerca scientifico-sanitaria Attività di diagnostica avanzata	Utilizzo di campioni di sangue periferico di soggetti normali o di pazienti pediatrici, nonché di tessuto tumorale pediatrico, a scopo di ricerca. Esecuzione test CGH/SNP array per neuroblastoma su campioni nazionali. Diagnostica immunofenotipica dei linfomi pediatrici e delle immunodeficienze primitive su casistica Gaslini
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura MODULAB) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Malattie infettive f.f. Dott. Castagnola Elio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione ricoveri. Gestione ambulatorio e Day Hospital: Patologie infettive acute e croniche Infezioni batteriche, micotiche o virali, in pazienti immunocompromessi; Trattamenti innovativi delle infezioni nei bambini sottoposti a chemioterapia o trapianto di midollo osseo o con immunodeficit primitivo; Epatiti acute; Infezione e malattia tubercolare; Counselling infettivologico a donne con infezione in gravidanza; Vaccinazioni.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa –Neurologia Pediatrica e Mal. Muscolari Prof. Minetti Carlo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Malattie neuromuscolari e neurodegenerative in particolare: distrofie muscolari, atrofie muscolari spinali, miopatie congenite, miopatie metaboliche, encefalomiopatie mitocondriali, miopatie infiammatorie, leucodistrofie genetico-metaboliche, neurofibromatosi, epilessie idiopatiche di origine genetica. Gestione laboratorio. Gestione biopsie muscolari. Gestione cartelle cliniche .
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Nefrologia, Dialisi e Trapianto Dott. Ghiggeri Marco		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Diagnostica e terapia delle nefropatie acquisite e congenite dell'età pediatrica; inquadramento e terapia chirurgica/endoscopica delle malformazioni delle vie Urinarie; servizio di ultrasonografia dell'apparato urinario; dialisi; assistenza pre e post trapianto. Gestione cartelle cliniche cartacee Gestione dati per trapianti.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Neurochirurgia Dott. Cama Armando		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione ricoveri, ambulatori Trattamenti per : Patologie Malformative del midollo spinale;Idrocefalo; Epilessie farmacoresistenti e la Chirurgia dell'Epilessia. Ambulatorio Multidisciplinare per le Patologie Neurovascolari. Ambulatorio Multidisciplinare per la Neuro-oncologia. Ambulatorio per Consulenze Genetiche. Gestione Cartelle Cliniche.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Neuropsichiatria Infantile Prof.ssa Veneselli Edvige		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione attività sociosanitaria a favore di fasce deboli di popolazione, Assistenza socio-sanitaria per la tutela della salute materno-infantile. Ambulatorio generale; Ambulatori di II livello: sindromi epilettiche dell'età evolutiva; Paralisi cerebrali infantili Cefalee dell'età evolutiva; Autismo e Disturbi della comunicazione; Disturbi del sonno; Follow-up neonati con problemi neurologici, Enuresi; Disturbi Infantili del comportamento. Ambulatori malattie rare. Day Hospital dopo visita neurologica e psichiatrica ambulatoriale o dopo ricovero. Ricovero ordinario per diagnosi ed alla terapia delle patologie neurologiche e psichiatriche dell'età evolutiva.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Neuroradiologia Prof. Rossi Andrea		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Attività diagnostica delle patologie del sistema nervoso centrale (encefalo e midollo spinale) e del suo contenente basata prevalentemente sull'utilizzo della Risonanza Magnetica (RM) e della Tomografia Computerizzata (TC). Attività di terapia interventistica (angiografia interventistica) endovascolare e percutanea delle malformazioni vascolari del distretto endocranico, cervico-facciale e rachideo.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione RIS/PACS Caresteram per la gestione di specifici database centralizzati di dati e immagini; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Oculistica Dott. Capris Paolo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Diagnosi e chirurgia dello strabismo; Chirurgia della cataratta congenita ed impianto di cristallino artificiale; Diagnosi e cura dei glaucomi congeniti ed infantili con particolare riferimento ai casi refrattari (impianto di valvole drenanti); Chirurgia della ptosi palpebrale e delle patologie orbitarie; Immunologia oculare, diagnosi e terapia delle uveiti; Centro per il controllo ed il trattamento della retinopatia del pretermine; Neuroftalmologia; Angiografia retinica; Ecografia oculare e Pachimetria corneale; Elettrofisiologia, potenziali visivi evocati, elettroretinografia, elettrooculografia; Esame del campo visivo; Laser terapia delle affezioni del segmento anteriore e posteriore.
Incaricati ai trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei. .	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Odontostomatologia e Ortodonzia pediatrica Dott. Laffi Nicola		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	L'U.O. effettua interventi di igiene orale, di prevenzione e di ortodonzia sui bambini ricoverati in ospedale e su bambini esterni al Gaslini. I medici dell'U.O. eseguono anche interventi chirurgici (per es. estrazioni dentali) nella sala operatoria di Otorinolaringoiatria. I medici dell'U.O. correggono le malocclusioni dentomaxillo facciali con interventi di ortodonzia e con apparecchi fissi e mobili.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei. .	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Ortopedia Dott. Boero Silvio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Trattamento chirurgico ed ortopedico delle malattie e delle disabilità in settori di rilevanza multidisciplinare; Trattamento delle deformità congenite. Chirurgia vertebrale per gravi deformità. Allungamento chirurgico degli arti. Chirurgia della mano e microchirurgia ortopedica. Chirurgia del piede. Chirurgia reumatologica. Trattamento chirurgico e conservativo nelle malattie dello sviluppo. Chirurgia mini-invasiva ed osteosintesi a minima. Termoablazione con radiofrequenza nelle neoplasie ossee benigne. Prevenzione e trattamento delle lesioni ortopediche sport-correlate. Gestione cartella clinica.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Strumenti elettronici (utilizzo applicazione RIS/PACS Caresteram per la gestione di specifici database centralizzati di dati e immagini. Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Ostetricia e Ginecologia f.f. Dott. Adriano Marco		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Screening e diagnosi prenatale delle malformazioni congenite e delle anomalie cromosomiche. Screening e monitoraggio della gravidanza complicata da patologia. Screening del diabete gestazionale. Ginecologia-difetti riproduttivi. Diagnosi precoce infettivologica ed oncologica della patologia del tratto genitale distale. Ambulatori.Gestione ricoveri. Gestione Day Hospital. Gestione cartelle cliniche.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazioni GST/AURORA e ASTRAIA per la gestione di specifici database centralizzati di dati e immagini; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Otorinolaringoiatria Dott. Tarantino Vincenzo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione Day Hospital e one day surgery Gestione ricoveri Prevenzione, diagnosi e trattamento della sordità infantile e dei disturbi del linguaggio. Screening audiologico neonatale. Potenziali evocati uditivi ad alta frequenza. Inquadramento multidisciplinare del bambino ipoacusico. Trattamento medico e chirurgico della patologia otologica. Diagnosi e cura dei disturbi dell'equilibrio e della postura. Diagnostica e trattamento della patologia adenoidea e tonsillare della patologia delle ghiandole salivari, della patologia laringea e tracheale e della patologia del collo.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Patologia Neonatale Dott.. Ramenghi Luca Antonio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	L'assistenza intensiva riguarda tutte le patologie dell'epoca neonatale e in particolare la prematurità di ogni grado, il distress respiratorio, la sepsi, la patologia chirurgica e cardiaca, l'asfissia grave e il neonato di peso molto basso. Nell'ambito dell'assistenza respiratoria il neonato viene assistito dalla sala parto alla Terapia Intensiva Neonatale con l'applicazione delle più attuali tecniche di ventilazione. E' attivo un sistema di Trasporto Neonatale
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Pediatria II Reumatologia Prof. Martini Alberto		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	L'attività assistenziale si caratterizza per la diagnosi e la cura delle malattie reumatiche (artrite idiopatica giovanile, lupus eritematoso sistemico, dermatomiosite, sclerodermia, vasculiti ecc.), delle febbri ricorrenti su base genetica e di altre malattie autoinfiammatorie (febbre familiare mediterranea, S. da iperIgD, TRAPS, CINCA ecc.). Gestione biobanca Gestione campioni biologici e dati clinici
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Pediatria III a indirizzo Gastroenterologico con endoscopia digestiva Dott. Barabino Arrigo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione reparto di degenza, Day Hospital, ambulatorio, consulenze interne ed esterne e servizio di endoscopia digestiva. L'attività clinica riguarda tutta la patologia gastrointestinale del bambino ordinaria e superspecialistica. Gestione del pre e post-trapianto epatico. Endoscopia digestiva diagnostica ed operativa. Gestione della nutrizione clinica del paziente neuroleso (in collaborazione con l'UO di Chirurgia dell'Istituto Diagnostica specialistica. Gli interventi terapeutici riguardano la terapia medica, la nutrizione clinica artificiale, diete selettive e, in casi specifici, la terapia chirurgica digestiva effettuata dalla U.O.di Chirurgia dell'Istituto. Gestione biobanca Gestione campioni biologici e dati clinici.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**

Unità Operativa Complessa – Pediatria ad indirizzo pneumologico e allergologico f.f. Dott. Sacco Oliviero		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	Prevenzione, diagnosi e cura di malattie primitive, congenite ed acquisite delle vie aeree, del polmone, della pleura e delle strutture toraciche e complicanze a carico dell'apparato respiratorio osservate in corso di patologie di altri organi od apparati.

Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Incaricati ai Trattamenti	Banche dati utilizzate	Modalità e luoghi di conservazione
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Pronto Soccorso e Medicina d'Urgenza Pediatrica f.f. Dott. Renna Salvatore		
Tipologia dei dati	**Finalità dei trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Acquisizione delle informazioni personali e sullo stato di salute (sensibili) del paziente per la compilazione della cartella clinica. Gestione del ricovero. Acquisizione di informazioni per la prenotazione del ricovero e produzione documenti per l'esecuzione di esami clinici. Gestione del Day Hospital.Servizio di informazioni relative ai trattamenti sanitari relativi ad utenti esterni ala struttura attraverso il sito dell'associazione AIMAR.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro Psicologia Clinica Ricondotta alla UOC Neuropsichiatria infantile Prof.ssa Veneselli Edvige		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Valutazione dello sviluppo cognitivo e psicodiagnostica per specifiche problematiche o aree di disagio in età evolutiva. Disadattamento e adattamento nelle malattie croniche pediatriche. Assistenza psicologica ed attività di consulenza ai reparti di degenze e day-hospital per problematiche psicologiche preesistenti o reattive alla condizione di malattia, problematiche di adattamento e compliance allo stato di malattia e/o alla ospedalizzazione nel paziente e/o familiari. Disturbi somatoformi in età evolutiva. Disturbi dell'identità di genere. Disturbi specifici ell'apprendimento e dell'adattamento scolastico. Disturbi del comportamento alimentare in età evolutiva. Assistenza psicologica (counseling) alle gestanti.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Radiologia f.f. Dott. Magnano Gian Michele		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Prenotazione, accettazione, esecuzione, refertazione, distribuzione e archiviazione delle procedure radiologiche di: radiologia, tomografia computerizzata, ultrasonografia, risonanza magnetica, angiografia diagnostica e interventistica nel paziente in età pediatrica Consegna referti e duplicazione materiale radiologico. Consulenza radiologica.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA e RIS/PACS per la gestione di specifici database centralizzati; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei. Pellicole per immagini
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Medicina Fisica e Riabilitazione Dott. Moretti Paolo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	INTERVENTO RI-ABILITATIVO IN AMBITO NEUROLOGICO PER: Bambini e adolescenti con paralisi cerebrale infantile in ricovero o in DH presso l'UO di Neuropsichiatria o nell'ambito del gruppo interdisciplinare delle PCI. Bambini ed adolescenti in ricovero per intervento neurochirurgico (neoplasie del SNC, neoplasie midollari, patologie del midollo, idrocefalia, traumi cranici) o in ricovero per patologie oncologiche ed ematologiche (tumori ossei, trapianto di midollo, neoplasie varie).
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Laboratorio di Neurogenetica e Neuroscienze Dott. Zara Federico		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Test genetici su DNA (attività diagnostica) Analisi genetiche su DNA per correlazioni genotipo-fenotipo (attività di ricerca) Analisi su cellule per studio meccanismi fisiopatologici di malattie neurologiche e muscolari (attività di ricerca)
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di Diagnostica ginecopatologica e Patologia feto – perinatale Prof. Ezio Fulcheri		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	1. Diagnostica della abortività spontanea del primo trimestre. 2. Diagnostica della patologia placentare delle alte prematurità. 3. Diagnostica placentare generale. 4. Diagnostica ginecopatologica. 5. Diagnostica citologica ginecologica. 6. Diagnostica delle malformazioni fetali su escisso o biopsiato. 7. Diagnostica autoptica delle malformazioni fetali. 8. Diagnostica autoptica delle morti fetali tardive. 9. Diagnostica autoptica delle morti improvvise fetali e neonatali. 10. Diagnostica della malattia trofoblastica gestazionale.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Uitlizzo SW "Obstetric and gynaecological database" di Astraia gmbh	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei.
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di Diagn. Genetica e biochimica mal. metaboliche Dott.ssa Filocamo Mirella		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Ricerca scientifico-sanitaria Banca dati genetici Dossier Sanitario Elettronico (DSE)	Preparazione campioni per analisi biochimiche, enzimatiche, molecolari e per conservazione nella Biobanca Genetica
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione, comunicazione dati a terzi	PC in rete locale

UOSD – Centro di endocrinologia clinica e sperimentale Dott. Maghnie Mohamad		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Ricoveri ordinari e in regime di Day Hospital, visite ambulatoriali, DXA e consulenze per patologie endocrinologiche: deficit di GH, deficit ipofisari multipli, diabete insipido, ipotiroidismo primario/ipotiroidismo congenito, ioptiroidismo centrale, ipertiroidismo, Tiroiditi, noduli tiroidei, osteoporosi primaria e secondaria, osteogenesi imperfetta, rachitismo, ipocalcemie congenite o acquisite, pubertà precoce, ipogonadismo centrale o primario, insufficienza surrenalica, patologie endocrine nei pazienti oncologici, basse stature, displasie scheletriche, sindrome di Prader Willi, obesità genetica, obesità severa semplice, sindrome ROHHADNET. Cronosomatie (S Turner, Sindrome di Turner e altre cromosomopatie), Sindrome metabolica, Sindrome adrenogenitale, ambiguità dei genitali, malattie rare con endocrinopatie (S Di Georges, Noonan, Silver Russell…)
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia (Metafora) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**

Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di reumatologia Prof. Ravelli Angelo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Iniezioni intra-articolari di steroidi Infusione di farmaci biologici (canakinumab e tocilizumab)
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia (Metafora) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro Trapianto Midollo Osseo Dott. Lanino Edoardo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Chemioterapia alte dosi Trapianto staminali emopoietiche midollari, periferiche e cordonali in patologie congenite ed acquisite, neoplastiche e non. Trattamento delle complicanze infettive e immunomediate post trapianto. Prelievo di midollo osseo o staminali periferiche da donatori sani
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia (Metafora) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro Nutrizionale Dott. Fiore Paolo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Valutazione dello stato di nutrizione Valutazione della spesa energetica basale Nutrizione clinica Indagine alimentare Educazione alimentare e dietoterapia
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo SW per gestione profili dietologici dei pazienti Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro Malattie Rare Dott. Di Rocco Maja		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Ricovero ordinario, day hospital, visita ambulatoriale, consulenze per interni, per: Malattie rare di origine genetica. Somministrazione di terapie enzimatiche sostitutive ed altri farmaci orfani.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia (Metafora) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di Dialisi Dott. Verrina Enrico Eugenio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Emodialisi in bicarbonato Emodiafiltrazione “on-line” Dialisi peritoneale Terapia sostitutiva renale continua (presso UTI) Medicazione foro cutaneo di uscita di catetere venoso centrale (CVC) o catetere peritoneale (CP) Infusione di farmaci in CVC o CP
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell’unità operativa	Strumenti elettronici (utilizzo procedura Armonia (Metafora) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro Angiomi Dott.ssa Vercellino Nadia		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Diagnosi, cura e trattamento delle anomalie vascolari attraverso visite ambulatoriali, ricoveri ordinari e Day Hospital, e interventi chirurgici.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia (Metafora) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di chirurgia mini-invasiva e robotica Dott. Mattioli Girolamo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Sia in regime di Day Surgery, Day Hospital, Ambulatoriale e ricovero ordinario, per patologie chirurgiche urgenti o programmate in pazienti pediatrici. Le competenze sono generali e specialistiche: chirurgia generale pediatrica, chirurgia toracica, urologica, oncologica, digestiva, chirurgia neonatale. Inoltre vengono trattate tutte le urgenze in generale di competenza viscerale e le ustioni. Inoltre ci sono gruppi di lavoro per la diagnostica e trattamento malattie rare. In dettaglio ci si occupa di ricerca clinica per migliorare la qualità dei risultati con particolare attenzione al concetto di "ospedale senza dolore" e mini-invasività.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**

Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di Neuroradiologia e radiologia intervenzionale Dott. Gandolfo Carlo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Trattamento endovascolare di patologie malformative vascolari di ogni distretto corporeo (ad esclusione del distretto cardio-polmonare). Trattamento percutaneo di patologie malformative vascolari di ogni distretto corporeo(ad esclusione del distretto cardio-polmonare). Biopsie ETG/Fluoro/TC guidate di ogni distretto corporeo Terapie infiltrative di localizzazioni articolari di patologie reumatologiche (ETG guidate). Posizionamento di cateteri vascolari a media e lunga permanenza. Diagnostica ECO-COLOR-DOPPLER Trattamento endovascolare e percutaneo di patologie tumorali, propedeutico a intervento chirurgico/neurochirurgico
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo SW RIS e PACS per la gestione delle immagini diagnostiche. Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**

Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro traslazionale di Miologia e patologie neurodegenerative Dott. Bruno Claudio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Terapia enzimatica sostitutiva Trial terapeutici con farmaci sperimentali fase II/III Terapie infusionali
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di assistenza domiciliare ematoncologica e continuità delle cure Dott. Dallorso Sandro		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Follow-up clinico ematologico post dimissione. Gestione e training accessi vascolari a permanenza. Somministrazione di chemioterapia, antibioticoterapia e nutrizione parenterale. Gestione dei sintomi correlati ai trattamenti e del dolore cronico. Cure palliative. Gestione paziente terminale.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**

Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Chirurgia ricostruttiva e della mano Dott. Senes Filippo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Interventi di chirurgia ricostruttiva e della mano - Chirurgia Ortopedica -visite ambulatoriali -ricoveri Day Hospital -ricoveri Ordinari -Day surgery -Sala Gessi
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**

Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Neuroncologia Dott.ssa Garrè Maria Luisa		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Trattamenti antiblastici con chemioterapia, radioterapia, trattamenti multimodali, trattamenti sperimentali con farmaci fase I e II. Terapie di supporto a complicanze. Trattamento trasfusionale. Terapie palliative
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**

Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Utilizzo ed accesso alla cartella oncologica (Oncosys). Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di Anestesiologia, Terapia del dolore acuto e procedurale Dott. Montobbio Giovanni		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**

Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Valutazione anestesiologica preoperatoria Anestesia generale e loco regionale Sedazione procedurale Terapia del dolore acuto e procedurale Partoanalgesia
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Team Interdipartimentale delle Vie Aeree Dott.Torre Michele		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Diagnostica di malformazioni o patologie acquisite delle vie aeree Trattamenti endoscopici di tali anomalie (dilatazioni, posizionamento di stent, trattamenti laser) Trattamenti ricostruttivi di laringe, trachea, bronchi (ricostruzioni laringotracheali, resezioni cricotracheali, tracheoplastiche)
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Centro di Rianimazione Neonatale e Pediatrica Dott. Moscatelli Andrea		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**

Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Terapia intensiva del neonato e del bambino critico. Monitoraggio avanzato dei parametri vitali. Supporto delle disfunzioni d'organo tramite ventilazione meccanica. Trattamenti extracorporei (ECMO e CRRT). Monitoraggio multiparametrico delle gravi disfunzioni neurologiche. Diagnostica avanzata delle vie aeree. Trasporto del neonato e del bambino critico. Terapia intensiva cardiovascolare
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Area Critica Medica Dott. Renna Salvatore		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Gestione semiintensiva dei pazienti con insufficienza d'organo. Sedazione procedurale minima. Ossigeno terapia ad alti flussi. Studi multicentrici.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo)Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

UOSD – Pronto Soccorso e OBI Dott.ssa Piccotti Emanuela		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Dossier Sanitario Elettronico (DSE)	Accettazione e valutazione medico-infermieristica Stabilizzazione e monitoraggio dei pazienti critici Infusione di fluidi e farmaci Suture e medicazioni di ferite/ustioni Sedazione procedurale minima
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

U.O.S.D. Centro di Medicina Fetale e perinatale **Prof. Paladini Dario**		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	**Diagnostica**: ecografia I, II e III trimestre. Ecocardiografia fetale, Neurosonografia Fetale. Amniocentesi, villocentesi **Chirurgia**: Laserablazione anastomosi placentari, Trasfusione intra-uterina, posizionamento shunt toraco-amniotico, amniodrenaggio, valvuloplastica in utero
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

U.O.S.D. CENTRO DI EMOSTASI E TROMBOSI Dott. Molinari Claudio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Tutela della salute Attuazione di interventi di prevenzione, di promozione della salute, di diagnosi, cura e riabilitazione Assistenza socio-sanitaria Ricerca scientifico-sanitaria Dossier Sanitario Elettronico (DSE)	infusione di fattori della coagulazione emoderivati, infusione di fattori della coagulazione ricombinanti, iniezione di ormoni sintetici, infusione di immunoglobuline emoderivati.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo procedura Armonia e Concerto (Anatomia Patologica e Laboratorio di Analisi) per la gestione di specifici database centralizzati; gestione di database locali) Strumenti elettronici (utilizzo procedura MODULAB) per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Gestione Risorse e Servizi Logistici Dott.ssa Picco Rosella		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☒	Amministrativo contabili Gestione del personale e dei collaboratori esterni	Gestione contratti/appalti (PRO011) Acquisto apparecchiature Acquisto beni e servizi diversi
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione OASI sistema ERP aziendale; gestione di database locali). Utilizzo SW di gestione protocollo elettronico aziendale Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Affari Generali e Legali Avv. Berri Carlo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☒	Amministrativo contabili Gestione del personale e dei collaboratori esterni	Raccolta dati clinici per gestione sinistri Gestione contratti e convenzioni Gestione lasciti ed eredità Gestione patrimonio immobiliare dell'Istituto Gestione cause e vertenze
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione OASI sistema ERP aziendale; gestione di database locali). Utilizzo SW di gestione protocollo elettronico aziendale Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Servizi Tecnici Ing. Tufaro Gaetano		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☐ Giudiziari ☐	Amministrativo contabili Gestione del personale e dei collaboratori esterni	Gestione Contratti (servizi, appalti, lavori pubblici) Gestione anagrafica fornitori, ditte appaltatrici
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione OASI sistema ERP aziendale; gestione di database locali). Utilizzo SW di gestione protocollo elettronico aziendale Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Gestione e Valorizzazione del Personale Dott. Bolognesi Alberto		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☒	Amministrativo contabili Gestione del personale	Gestione del rapporto di lavoro con il personale dipendente Gestione previdenziale, Gestione concorsi, Gestione Formazione Obbligatoria
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione ALISEO per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo SW di gestione Protocollo Elettronico Aziendale Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Centro Controllo Direzionale e Servizio Qualità Dott. Rosati Ubaldo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Amministrativo contabile	Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria Trattamento statistico dati aziendali
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione RAGES per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo SW di gestione Procollo Elettronico Aziendale Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Unità Operativa Complessa – Sistema Informativo Aziendale Dott. Lightwood Simone		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☒	Supporto informatico alle UU.OO.	Supporto alle UU.OO. per la conservazione e la disponibilità operativa dei dati informatici. Implementazione e gestione dei sistemi di sicurezza informatici. Supervisione alle procedure operative per l'utilizzo del sistema informatico dell'Istituto
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (database centralizzati). Strumenti elettronici (utilizzo applicazione OASI sistema ERP aziendale; gestione di database locali). Utilizzo SW di gestione Procollo Elettronico Aziendale Supporti cartacei	Sistemi server e client per i dati informatici gestiti su database centralizzati e locali Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale Connessioni remote via Internet

Unità Operativa Complessa – Bilancio, Contabilità e Finanza Dott.ssa Moncini Stefania		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Amministrativo contabili	Gestione Bilancio, Budget, Cassa Tesoreria, Ambulatori ed Accettazione, Rapporti Economici con i dipendenti, Fornitori e Clienti, Cessione C redito, Cespiti, Eredità e Legati e Fondi di Reparto
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (utilizzo applicazione; OASI sistema ERP aziendale; gestione di database locali). Utilizzo SW di gestione Procollo Elettronico Aziendale Supporti cartacei.	Sistemi server cluster installati in appositi ambienti controllati e climatizzati. PC client per i dati informatici gestiti su database locali. Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Direzione Generale Dott. Petralia Paolo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☒	Amministrativo contabile	Procedimenti amministrativi e gestionali di rilevanza per l'Istituto.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (OASI ERP aziendale) Utilizzo SW di gestione Procollo Elettronico Aziendale Supporti cartacei	Sistemi server e client per i dati informatici gestiti su database centralizzati e locali Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Direzione Scientifica f.f. Prof. Ramenghi Luca Antonio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☐	Amministrativo contabile	Gestione amministrativa e organizzativa della ricerca, Gestione del rapporto con i ricercatori Gestione rapporti con altri istituti di ricerca e università
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (OASI ERP aziendale) Utilizzo SW di gestione Procollo Elettronico Aziendale Supporti cartacei	Sistemi server e client per i dati informatici gestiti su database centralizzati e locali Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Direzione Sanitaria Dott. Del Buono Silvio		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☒	Amministrativo contabile	Gestione amministrativa del personale sanitario e operativa dei reparti sanitari. Procedure Medico-Legali
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (OASI ERP aziendale) Utilizzo applicazione GST/AURORA per la gestione di specifici database centralizzati; gestione di database locali). Utilizzo ed accesso alla Cartella Clinica Elettronica ed al Dossier Paziente (sistema Galileo) Utilizzo SW di gestione Procollo Elettronico Aziendale Supporti cartacei	Sistemi server e client per i dati informatici gestiti su database centralizzati e locali Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

Direzione Amministrativa Dott. Faravelli Paolo		
Tipologia dei dati	**Finalità dei Trattamenti**	**Principali trattamenti**
Personali ☒ Sensibili ☒ Giudiziari ☒	Amministrativo contabile Gestione del personale	Procedimenti amministrativi di rilevanza per la direzione.
Incaricati ai Trattamenti	**Banche dati utilizzate**	**Modalità e luoghi di conservazione**
Tutto il personale che opera nell'unità operativa	Strumenti elettronici (OASI ERP aziendale) Utilizzo SW di gestione Procollo Elettronico Aziendale Supporti cartacei	Sistemi server e client per i dati informatici gestiti su database centralizzati e locali Archivi cartacei
Modalità del trattamento	**Operazioni**	**Caratteristiche IT**
Automatizzato ☒ Manuale ☒	Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione, comunicazione	PC in rete locale

SEZIONE 1.2 - Compiti e Responsabilità

Questa sezione descrive le responsabilità attribuite ad ogni figura prevista dalla normativa, associando ad ognuna di esse i diversi soggetti organizzativi dell' Istituto G. Gaslini , che svolgono i trattamenti sui dati (comma 2 articolo 19 del Disciplinare Tecnico).
Per ogni soggetto organizzativo considerato è stato indicato il ruolo e la funzione svolta.
La lista degli incaricati è stata fatta coincidere con tutto il personale operativo presente nei settori dell' Istituto G. Gaslini, questo perché per motivi organizzativi tutto il personale è autorizzato a trattare dati personali e sensibili, in relazione alle proprie mansioni.
Nei casi in cui siano necessarie modalità diverse, è previsto un sistema di autorizzazione (come richiesto dagli articoli 12, 13 e 14 del Disciplinare Tecnico) per la configurazione di particolari profili di accesso.

Titolare del trattamento: Istituto G. Gaslini nella persona del suo Legale Rappresentante.
Responsabile dei Trattamenti: Ai sensi della delibera del CdA n. 88 del 18.5.2015 sono preposti dal titolare al trattamento di dati personali i responsabili delle U.O.C. e delle U.O.S.D. In particolare si tratta dei responsabili delle seguenti Unità operative complesse e Strutture Semplici Dipartimentali:

Unità Operativa Semplice Dipartimentale – Epidemiologia Biostatistica e Comitati
Unità Operativa Complessa – Centro Controllo Direzionale e Servizio Qualità
Unità Operativa Complessa – Sistema Informativo Aziendale
Unità Operativa Complessa – Affari generali e Legali
Unità Operativa Complessa – Gestione e Valorizzazione del Personale
Unità Operativa Complessa – Bilancio Contabilità e Finanze
Unità Operativa Complessa – Gestione Risorse e Servizi Logistici
Unità Operativa Complessa – Servizi Tecnici
Unità Operativa Complessa – Farmacia
Unità Operativa Complessa – Genetica Medica
Unità Operativa Complessa – Laboratorio Analisi
Unità Operativa Complessa – Immunologia Clinica e Sperimentale
Unità Operativa Complessa – Laboratorio di Oncologia
Unità Operativa Complessa – Laboratorio di Biologia Molecolare
Unità Operativa Complessa – Laboratorio Cellule Staminali post natali e terapie cellulari
Unità Operativa Complessa – Immunoematologia e Medicina Trasfusionale
Unità Operativa Complessa – Anatomia Patologica
Unità Operativa Semplice Dipartimentale – Centro di Diagnostica genetica e biochimica delle malattie metaboliche
Unità Operativa Semplice Dipartimentale – Centro di Diagnostica ginecopatologica e patologia feto-perinatale

Unità Operativa Semplice Dipartimentale – Laboratorio di Neurogenetica e Neuroscienze
Unità Operativa Complessa – Clinica Pediatrica
Unità Operativa Complessa – Nefrologia Dialisi e Trapianto
Unità Operativa Complessa – Pediatria III a indirizzo gastroenterologico con endoscopia digestiva
Unità Operativa Complessa – Malattie Infettive
Unità Operativa Complessa – Pediatria ad indirizzo pneumologico e allergologico
Unità Operativa Complessa – Dermatologia
Unità Operativa Complessa – Pediatria II Reumatologia
Unità Operativa Complessa – Ematologia
Unità Operativa Complessa – Oncologia
Unità Operativa Semplice Dipartimentale – Centro di Endocrinologia clinica e sperimentale
Unità Operativa Semplice Dipartimentale – Centro Nutrizionale
Unità Operativa Semplice Dipartimentale – Centro Malattie Rare
Unità Operativa Semplice Dipartimentale – Centro di Reumatologia
Unità Operativa Semplice Dipartimentale – Centro Trapianto Midollo Osseo
Unità Operativa Semplice Dipartimentale – Centro di Emostasi e Trombosi
Unità Operativa Semplice Dipartimentale – Centro di Dialisi
Unità Operativa Complessa – Cardiochirurgia
Unità Operativa Complessa – Cardiologia
Unità Operativa Complessa – Chirurgia
Unità Operativa Complessa – Radiologia
Unità Operativa Semplice Dipartimentale – Centro Angiomi
Unità Operativa Semplice Dipartimentale – Centro di chirurgia mini-invasiva e robotica
Unità Operativa Semplice Dipartimentale – Centro di Neuroradiologia e radiologia intervenzionale
Unità Operativa Complessa – Neurochirurgia
Unità Operativa Complessa – Neurologia Pediatrica e Malattie Muscolari
Unità Operativa Complessa – Ortopedia
Unità Operativa Complessa – Neuropsichiatria Infantile
Unità Operativa Complessa – Oculistica
Unità Operativa Complessa – Medicina Fisica e Riabilitazione
Unità Operativa Complessa – Otorinolaringoiatria
Unità Operativa Complessa – Neuroradiologia
Unità Operativa Semplice Dipartimentale – Centro Traslazionale di Miologia e patologie neurodegenerative
Unità Operativa Semplice Dipartimentale – Centro di Neuro-Oncologia
Unità Operativa Semplice Dipartimentale – Centro di Assistenza domiciliare ematoncologica e continuità delle cure
Unità Operativa Semplice Dipartimentale – Centro di Psicologia Clinica
Unità Operativa Semplice Dipartimentale – Chirurgia ricostruttiva e della mano
Unità Operativa Semplice Dipartimentale – Odontostomatologia e ortodonzia pediatrica
Unità Operativa Semplice Dipartimentale – Laboratorio di Neurogenetica e Neuroscienze
Unità Operativa Complessa – Ostetricia e Ginecologia
Unità Operativa Complessa – Anestesia e Rianimazione neonatale pediatrica
Unità Operativa Complessa – Patologia Neonatale
Unità Operativa Semplice Dipartimentale – Centro di Medicina Fetale e perinatale
Unità Operativa Semplice Dipartimentale – Team Interdipartimentale delle Vie Aeree

Unità Operativa Semplice Dipartimentale – Centro di Anestesiologia. Terapia del dolore acuto e procedurale
Unità Operativa Semplice Dipartimentale – Centro di Rianimazione Neonatale e Pediatrica
Unità Operativa Complessa – Pronto Soccorso e Medicina d'urgenza Pediatrica
Unità Operativa Semplice Dipartimentale – Area Critica Medica
Unità Operativa Semplice Dipartimentale – Pronto Soccorso e OBI
Unità Operativa Semplice Dipartimentale – Centro di Psicologia Clinica

I responsabili dei trattamenti presso le direzioni dell'Istituto, sono nominati i direttori stessi. In particolare si tratta delle seguenti direzioni:

Direzione Generale
Direzione Scientifica
Direzione Sanitaria
Direzione Amministrativa

Il Responsabile del Trattamento ha il compito di verificare, all'interno della sua U.O.C , U.O.S.D. o direzione, che i dati oggetto dello specifico trattamento siano pertinenti, corretti e non superflui rispetto le finalità preposte e siano correttamente conservati per il tempo previsto. Deve impartire specifiche istruzioni agli incaricati del trattamento dei dati, sulla corretta gestione e conservazione dei dati per garantirne l'integrità e la sicurezza. Deve inoltre verificare la corretta applicazione delle informative precedenti le richieste di consenso del trattamento dei dati.

Gruppo di Lavoro Privacy: Individuato con deliberazione del CdA n. 88 del 18.5.2015
Ha il compito (insieme al Referente dei Sistemi Informativi) di proporre l'aggiornamento dei documenti in materia di sicurezza, e di ogni altro adempimento previsto dalla Legge al titolare e, per sua disposizione ai Responsabili; di predisporre le linee guida e strumenti operativi volti ad assicurare una corretta applicazione della normativa vigente e dei provvedimenti del Garante di interesse per il settore pubblico e sanitario, con riferimento anche al profilo della sicurezza dei dati; di fornire ai Rappresentati dell'Azienda il supporto giuridico dagli stessi richiesto ed in relazione anche alla predisposizione di documenti e modulistica: di monitorare l'applicazione delle disposizioni di legge e delle direttive impartite dall'Azienda attraverso verifiche anche periodiche ed ispezioni assicurando il necessario supporto alla Direzione Generale nei rapporti con il Garante. Il gruppo è composto da: Dott.ssa Beatrice Chiozza, Dott. Ubaldo Rosati, Sig.a Alessandra Traverso, Dr. Simone Lightwood, Avv. Dr. Carlo Berri, Avv. Dott.ssa Patrizia Fabrizi, Sig. Stefano Castagnola

Responsabile dei Sistemi Informativi: individuato nella persona di Dr. Simone Lightwood che ha:

- la responsabilità della gestione del Sistema Informativo dell'Istituto Giannina Gaslini;
- la responsabilità dell'implementazione delle misure tecniche relative alla gestione della sicurezza del Sistema Informativo.

In particolare è responsabile: della gestione delle copie di backup (creazione, custodia, ripristino) di tutto l' Istituto G. Gaslini, dell'analisi e della custodia dei log di accesso (agli applicativi, alla rete, ecc.), delle corrette configurazioni delle risorse hardware e software.
Altresì ha la responsabilità (insieme al Responsabile della Privacy) della redazione, e della verifica dell'adozione, di tutte le politiche e procedure necessarie a garantire l'effettiva adozione delle misure di sicurezza per quanto concerne gli aspetti informatici.

Incaricati del trattamento: sono individuati come incaricati del trattamento tutti coloro che svolgono operazioni sui dati personali,sensibili e giudiziari, secondo quanto riportato nei rispettivi mansionari (interni all'Istituto e/o definiti dai contratti collettivi nazionali del lavoro). Gli incaricati agiscono secondo le modalità previste da specifici contratti/accordi/convenzioni.
Per gli incaricati che devono eseguire particolari operazioni di trattamento sono configurati ed autorizzati dei profili di accesso che permettono di accedere ai dati con modalità diverse rispetto al resto del personale.
Tutti gli incaricati che eseguono operazioni di raccolta dei dati hanno la responsabilità di comunicare le specifiche informative (a seconda del tipo di dati raccolti) agli interessati. Altresì hanno la responsabilità di farsi rilasciare, dagli interessati, il consenso al trattamento, in base alle modalità previste dalle normative vigenti.

Per un maggior dettaglio sulle operazioni svolte dagli incaricati si rimanda a quanto stabilito per i ruoli e le mansioni svolte previsto dai contratti/accordi/convenzioni collettivi o individuali.

CAPITOLO 2 - Analisi dei Rischi

Ai sensi del comma 3 dell'articolo 19 del Disciplinare Tecnico, in questa sezione è riportata l'analisi dei rischi che incombono sui dati (personali, sensibili e giudiziari) oggetto di trattamento.
L'individuazione delle minacce che incombono sui dati è necessaria per poter implementare quelle misure a prevenzione dei rischi legati ai dati ed alle informazioni, che sono stati suddivisi in maniera generale in:

- Rischi di distribuzione o perdita, anche accidentale, dei dati, con particolare riguardo a quelli sensibili e giudiziari.
- Rischi connessi all'integrità dei dati.
- Rischi di accesso non autorizzato ai dati.
- Rischi di trattamento non consentito o non conforme alle finalità della raccolta.
- Rischi connessi all'utilizzo di reti di telecomunicazioni, anche disponibili al pubblico.
- Rischi connessi al reimpiego dei supporti di memorizzazione.
- Rischi connessi alla conservazione della documentazione relativa al trattamento.
- Rischi connessi all'utilizzo di archivi e contenitori di sicurezza.
- Rischi derivanti dalla mancata o insufficiente formazione del personale.

Quindi sulla base di quanto riportato nel capitolo 1.2 (tipi di dati trattati, operazioni di trattamento svolte, strumenti utilizzati e supporti di memorizzazione), e sulla base della situazione in essere dell' Istituto G. Gaslini, si è condotta un'Analisi dei Rischi, basata sull'esposizione alle minacce (riportate nella tabella 2) che incombono sulle proprietà dei dati, che sono: riservatezza, integrità e disponibilità.
L'analisi dei rischi condotta ha permesso di selezionare le misure minime da implementare, per garantire quella tutela dei dati personali prevista dalla normativa nazionale in tema di privacy.
Le misure minime sono riportate nel capitolo 3 del presente documento.

Minacce considerate	Rilevata esposizione		Cause dell'esposizione
Terremoti	SI ☐	NO ☒	Non si sono mai verificati episodi sismici rilevanti
Inondazioni - allagamenti	SI ☐	NO ☒	Mai nel recente passato
Fulmini	SI ☐	NO ☒	Mai nel recente passato
Fuoco	SI ☒	NO ☐	L'Istituto è in regola con le norme antincendio (L.81) e i danni sono stati contenuti in quanto le precauzioni adottate hanno consentito un rapido intervento antincendio e al fatto che che grazie alla dematerializzazione non vi erano dati in formato cartaceo. I dati archiviati nei server non sono stati danneggiati
Malfunzionamento alimentazione elettrica	SI ☒	NO ☐	Il cluster dei database principali ha le alimentazioni ridondate e in generale i server contenenti dati e i server di applicazione critiche sono sotto gruppi di continuità e gruppi elettrogeni. Non si può escludere il verificarsi di questa minaccia: la tendenza è quella di ridondare i sistemi per evitare interruzioni di servizio
Perdita di dati per errore su banche dati	SI ☒	NO ☐	La minaccia può considerarsi di livello basso, date le protezioni in atto (controllo accessi e controlli sull'integrità dei dati) e l'alto livello di affidabilità raggiunto dal sistema operativo di gestione dei DB utilizzato e delle procedure di backup messe in atto
Accesso fisico di persone non autorizzate	SI ☒	NO ☐	L'accesso libero alle aree dell'Istituto e la presenza continua di persone esterne rende questa minaccia particolarmente insidiosa. L'accesso alle zone riservate è veicolato attraverso badge (sala CED) o chiavi.
Accesso logico di utenti non autorizzati	SI ☒	NO ☐	Anche in presenza di sistemi di adeguati sistemi di sicurezza perimetrale (rif. DOC001 Allegato Tecnico), non si può escludere a priori questa minaccia. I sistemi di controllo sono aggiornati giornalmente per il riconoscimento delle minacce esterne (virus, malware, ecc)
Accesso ai dati sensibili da parte di persone non autorizzate	SI ☒	NO ☐	L'accesso ai dati informatici gestiti con sistemi centralizzati è consentito con specifiche procedure di riconoscimento e autorizzazione. Per quanto riguarda i dati cartacei (cartelle cliniche) è responsabilità degli utilizzatori garantirne la riservatezza e l'appropriata archiviazione. L'esposizione al rischio in questo secondo caso è maggiore che per i dati informatici
Malfunzionamento Server	SI ☐	NO ☒	La minaccia è da considerarsi di livello basso. I server funzionano in modalità bilanciamento di carico tra più sistemi differenti, ed sono presenti contratti di supporto con i fornitori con tempi di intervento entro le 4 ore (24X7)
Malfunzionamento Hardware	SI ☒	NO ☐	La minaccia, seppur con bassa probabilità di accadimento, non può essere esclusa. Le apparecchiature più critiche (vedi server del punto precedente) hanno garantiti tempi di ripristino più veloci rispetto ai PC dell'utenza.
Malfunzionamento Software	SI ☒	NO ☐	La struttura IT in grado di intervenire sui malfunzionamenti software. Sono attivi contratti di

Minacce considerate	Rilevata esposizione		Cause dell'esposizione
			assistenza con tutti i fornitori di software, sia applicativo che di sistema. La complessità del Sistema Informativo dell'Istituto fa comunque permanere un certo grado di esposizione alla minaccia .
Uso di client da parte di utenti non autorizzati	SI ☒	NO ☐	Pur in presenza di politiche di autorizzazione all'accesso sulla rete dell'Istituto, permane ancora un basso livello di esposizione alla minaccia.
Uso software da parte di utenti non autorizzati	SI ☒	NO ☐	Il livello di esposizione alla minaccia è da considerarsi molto basso, grazie alla politica di profilazione degli accessi a fronte della corretta conservazione delle credenziali da parte dell'utenza autorizzata. Non è autorizzata l'installazione (comunque impedita per policies di configurazione) di software non licenziato dall'Istituto.
Uso non autorizzato dei supporti di memorizzazione	SI ☒	NO ☐	Per questa minaccia non sono state ancora adottate contromisure specifiche (politiche di utilizzo dei supporti). Resta problematico impedire di fatto l'utilizzo di floppy, CD ROM, chiavette USB e altri strumenti mobili di memorizzazione.
Deterioramento dei supporti di memorizzazione	SI ☒	NO ☐	La struttura IT garantisce un adeguato livello di sicurezza con i sistemi e le procedure di backup utilizzate con costante sostituzione dei supporti rimovibili utilizzati per le attività di backup (e contestuale distruzione dei supporti dismessi).
Uso improprio di risorse	SI ☒	NO ☐	Anche se il personale è informato sui comportamenti corretti da adottare, non si può escludere l'esposizione a questa minaccia.
Software maligno	SI ☒	NO ☐	I sistemi di prevenzione dal software malevole (antivirus) sono continuamente aggiornati on-line con i loro produttori. Ogni PC della rete viene a sua volta aggiornato da un server centrale. Rimane un livello di esposizione molto basso alla minaccia.
Intercettazione del traffico di rete	SI ☒	NO ☐	Il livello di esposizione è molto basso, date le contromisure attuate a livello tecnologico (cfr. Allegato Tecnico)
Danno intenzionale	SI ☒	NO ☐	L'esposizione a questa minaccia è strettamente correlata al livello di consapevolezza degli utenti circa gli obblighi derivanti dai loro compiti.
Furto	SI ☒	NO ☐	Anche in presenza di impianti di allarme, la continua presenza di pubblico fa permanere la possibilità di accadimento di questa minaccia specialmente nelle postazioni operative (reparti).
Errori degli utenti	SI ☒	NO ☐	L'esposizione a questa minaccia è strettamente correlata al livello di consapevolezza degli utenti circa gli obblighi derivanti dai loro compiti.

Tabella 4: Minacce considerate per l'Analisi dei Rischi

Minacce considerate	Gravità delle conseguenze		
Accesso fisico di persone non autorizzate	☒ Alta	☐ Media	☐ Bassa
Accesso ai dati sensibili da parte di persone non autorizzate	☒ Alta	☐ Media	☐ Bassa
Uso improprio di risorse	☐ Alta	☒ Media	☐ Bassa
Accesso logico di utenti non autorizzati	☐ Alta	☒ Media	☐ Bassa
Uso non autorizzato dei supporti di memorizzazione	☐ Alta	☒ Media	☐ Bassa
Errori degli utenti	☐ Alta	☒ Media	☐ Bassa
Furto	☐ Alta	☒ Media	☐ Bassa
Malfunzionamento Software	☐ Alta	☒ Media	☐ Bassa
Terremoti	☐ Alta	☐ Media	☒ Bassa
Inondazioni - allagamenti	☐ Alta	☐ Media	☒ Bassa
Fulmini	☐ Alta	☐ Media	☒ Bassa
Fuoco	☐ Alta	☒ Media	☐ Bassa
Malfunzionamento alimentazione elettrica	☐ Alta	☐ Media	☒ Bassa
Perdita di dati per errore su banche dati	☐ Alta	☐ Media	☒ Bassa
Malfunzionamento Server	☐ Alta	☐ Media	☒ Bassa
Malfunzionamento Hardware	☐ Alta	☐ Media	☒ Bassa
Uso client da parte di utenti non autorizzati	☐ Alta	☐ Media	☒ Bassa
Uso software da parte di utenti non autorizzati	☐ Alta	☐ Media	☒ Bassa
Deterioramento dei supporti di memorizzazione	☐ Alta	☐ Media	☒ Bassa
Software maligno	☐ Alta	☐ Media	☒ Bassa
Intercettazione traffico di rete	☐ Alta	☐ Media	☒ Bassa
Danno intenzionale	☐ Alta	☐ Media	☒ Bassa

Tabella 5: Livello di gravità conseguente al realizzarsi delle Minacce

CAPITOLO 3 - Regolamento per l'attuazione di misure minime ed idonee di sicurezza

Ai sensi del titolo V, articoli 31, 33, 34, 35 e 36 Dlgs 196/2003, in questo capitolo sono riportate le modalità adottate dall'Istituto per proteggere i dati personali, sensibili e giudiziari in suo possesso, soddisfacendo i requisiti richiesti dalla normativa in materia di misure minime e idonee.
Le istruzioni contenute nella sezione si possono raggruppare nelle seguenti classi:

- Istruzioni per la sicurezza fisica
- Istruzioni specifiche per tutti i tipi di dati personali trattati con strumenti elettronici
- Istruzioni specifiche per i dati sensibili e giudiziari trattati con strumenti elettronici
- Istruzioni specifiche per tutti i tipi di dati (personali, sensibili e giudiziari) trattati senza strumento elettronico

Tutte le misure di sicurezza sono riportate in 12 procedure, descritte in allegato al presente documento, numerate da PRO001 a PRO011.

SEZIONE 3.1 – Istruzioni per la sicurezza fisica

La protezione fisica oggetto di questa sezione, riguarda la gestione degli accessi ai locali dell'Istituto e degli accessi alle aree e ai locali dove sono trattati e conservati i dati, in qualsiasi modo questo avvenga.
Le misure nello specifico sono:

- Misure a protezione degli edifici, per evitare accessi fisici non autorizzati;
- Controlli per l'identificazione delle persone che entrano ed escono dagli edifici;
- Controlli sugli accessi ai locali, contenenti dati personali (indipendentemente dal supporto di conservazione), in modo da evitare che in assenza del personale possano accedervi utenti non autorizzati;
- Controlli sugli accessi ai locali, contenenti dati sensibili (indipendentemente dal supporto di conservazione), in modo da evitare, che in assenza di personale autorizzato possano accedervi utenti non autorizzati.

Le misure sopra elencate sono state formalizzate all'interno delle procedure:

- PRO001 – Procedura per la gestione degli accessi fisici
- PRO004 – Procedura per la gestione del posto di lavoro e degli accessi agli uffici.

All'interno di queste procedure sono state riportate le misure in dettaglio, insieme alle responsabilità ed ai compiti del personale addetto ad effettuare i controlli sopra citati.

SEZIONE 3.2 – Istruzioni specifiche per tutti i tipi di dati personali trattati con strumenti elettronici

Istruzioni per il personale tecnico

Per evitare accessi non autorizzati (da parte di utenti esterni all'Istituto, e da parte del personale non autorizzato) il personale tecnico è tenuto ad implementare un sistema di autenticazione per l'accesso al sistema informativo.
Il personale tecnico ha la responsabilità di configurare i profili di accesso degli incaricati, sulla base delle sole operazioni di trattamento che sono autorizzati a svolgere.
Il personale tecnico è tenuto a configurare i profili di accesso sempre prima che all'incaricato siano assegnate le credenziali per l'autenticazione.
Il personale tecnico deve impostare il sistema di gestione delle password, affinché siano gli incaricati del trattamento i responsabili della selezione e della modifica delle stesse.
Questo per renderli gli unici detentori delle proprie credenziali di accesso, e quindi gli unici responsabili delle operazioni effettuate.
Il personale tecnico può verificare (anche con controlli automatizzati) la durata di validità delle password, invitando gli incaricati del trattamento a modificarla quando scaduta.
Il personale tecnico può verificare (anche con controlli automatizzati) il periodo di inutilizzo degli account, e dopo sei mesi di inutilizzo provvede a cancellarli, per evitare che possano essere sfruttati per accessi non autorizzati.
Gli unici account esclusi da questo controllo sono quelli adibiti alla gestione tecnica del sistema informativo.
Il personale tecnico può condurre verifiche periodiche sui log di accesso, per accertare che non vi siano stati accessi non autorizzati (ad esempio verificando il numero di password invalidate dal sistema informativo). Altresì ha la responsabilità di proteggere i dati relativi ai log di accesso.
Il personale tecnico su segnalazione degli enti interessati, o comunque almeno annualmente, può verificare / modificare tutti i profili di accesso autorizzati, per accertarsi che sussistano i motivi della loro creazione.

Queste misure sono contenute nelle procedure:

- PRO002 – Procedura per l' autenticazione degli accessi informatici
- PRO003 – Procedura per la gestione dei profili di accesso.

Il personale tecnico è tenuto ad istallare un software di rilevazione dei virus, su ogni apparecchiatura (client e server) del sistema informativo.
Il personale tecnico è tenuto a gestire il download degli aggiornamenti del software antivirus, nel caso questo venga gestito in modo centralizzato.
Gli aggiornamenti di tale software devono avvenire almeno ogni sei mesi.
Il personale tecnico deve garantire la presenza degli ultimi aggiornamenti dei sistemi operativi volti a correggere le vulnerabilità dei programmi in uso presso l'Azienda, compatibilmente con l'architettura software in essere.

Queste misure sono contenute nella procedura:
- PRO005 – Procedura per la protezione da software maligno.

Il personale tecnico è tenuto a svolgere regolarmente i backup dei dati, ed è responsabile della loro custodia.

Queste misure sono contenute nella procedura:

- PRO006 – Procedura per la gestione dei backup.

Nel caso di assenze prolungate degli incaricati del trattamento, il personale tecnico è tenuto ad assicurare la disponibilità dell'accesso ai dati senza che il sistema di gestione delle password sia compromesso (quindi senza invalidare la responsabilità univoca degli utenti).

Il personale tecnico ha il compito di garantire l'accesso ad Internet e alla Posta elettronica secondo quanto disposto dalle procedure:
- PRO001 - Procedura per la gestione degli accessi fisici,
- PRO002 - Procedura per l' autenticazione degli accessi informatici
- PRO004 - Procedura per la gestione del posto di lavoro e dell'accesso agli uffici

Istruzioni per gli incaricati del trattamento

In ottemperanza a quanto disposto dall'art. 30 del Dlgs 196/2003 e dai punti da 1 a 11 del Disciplinare Tecnico, gli incaricati hanno la responsabilità di seguire quanto previsto dalle procedure:
- PRO002 – Procedura per l' autenticazione degli accessi informatici
- PRO004 – Procedura per la gestione del posto di lavoro e dell'accesso agli uffici
- PRO008 – Procedura per la gestione dei supporti removibili
- PRO009 – Procedura per la conservazione e gestione dei documenti cartacei
- PRO010 – Procedura per la continuità dei servizi
- PRO011 – Procedura per la gestione dei requisiti di sicurezza nei contratti

.

SEZIONE 3.3 – Istruzioni specifiche per i dati sensibili e giudiziari trattati con strumenti elettronici

Nel caso di trattamenti di dati sensibili e/o giudiziari, valgono le istruzioni riportate nella sezione 3.2 inerenti i dati personali, ed in aggiunta vanno considerati i seguenti punti:

Istruzioni per il personale tecnico

Il personale tecnico deve implementare un sistema di sicurezza (Firewall) contro gli accessi non autorizzati ai dati.
Il personale tecnico ha la responsabilità di documentare formalmente le configurazioni adottate, in modo da poterle facilmente ripristinare in caso di problemi.

La gestione del firewall è illustrata dalla procedura:
- PRO007 – Procedura per la gestione degli accessi logici.

Istruzioni per gli incaricati del trattamento

Quando i dati sensibili e/o giudiziari devono essere registrati su supporti removibili di memorizzazione, gli incaricati del trattamento sono tenuti a seguire regole di utilizzo che

garantiscano sia l'integrità dei dati, sia che utenti non autorizzati possano venirne a conoscenza.

Queste regole sono contenute nella procedura:
- PRO008 – Procedura per la gestione dei supporti removibili

SEZIONE 3.4 – Istruzioni specifiche per tutti i tipi di dati (personali, sensibili e giudiziari) trattati senza strumento elettronico

In ottemperanza a quanto disposto dall'art. 35 del Dlgs 196/2003 e dal Disciplinare Tecnico (punti da 26 a 29), è stata predisposta una formale procedura operativa che descrive le modalità di controllo e di custodia dei documenti contenenti dati personali e le modalità di accesso e di consultazione degli archivi cartacei.
Tale procedura, riportata in allegato, è denominata:
- PRO009 – Procedura per la conservazione e gestione dei documenti cartacei.

CAPITOLO 4 - Piano per la Continuità del Servizio

Ai sensi del comma 5 dell'articolo 19 del Disciplinare Tecnico e del successivo articolo 23, in questo capitolo vengono descritti i piani per la Continuità del Servizio, studiati per assicurare il ripristino della disponibilità dei dati personali trattati dall'Azienda, in seguito ad una perdita degli stessi, causata da eventi dannosi.

Tale piano viene revisionato annualmente parallelamente all'aggiornamento del presente Documento Programmatico sulla Sicurezza.

Il Piano per la Continuità del Servizio che è stato predisposto è contenuto nella procedura:

- PRO010 – Procedura per la continuità dei servizi.

CAPITOLO 5 - Piano per la formazione degli incaricati

Ai sensi del comma 6 dell'articolo 19 del Disciplinare Tecnico, in questo capitolo viene descritto il Piano per la Formazione del Personale, predisposto dall'Istituto.

A partire dal 2016 è prevista la realizzazione di un piano formazione i cui dipendenti coinvolti sono:

- Gli incaricati.
- Il personale tecnico.
- Il Gruppo di lavoro Privacy.
- Il Referente per i Sistemi Informativi.
- Il Referente per la Sicurezza.

Il piano prevede la formazione degli utenti sui temi della sicurezza delle informazioni, ed in particolare su:

- Le nuove normative e direttive introdotte in materia di privacy.
- I rischi che incombono sulle risorse e sui dati dell'Azienda (informazioni emerse dall'analisi dei rischi).
- Le misure tecnologiche implementate (tipo di misure, modalità di gestione e di utilizzo).
- Le misure organizzative implementate (politiche e procedure operative) che riguardano:
  - Le modalità da seguire nei trattamenti gestiti da strumenti elettronici.
  - Le modalità da seguire nei trattamenti gestiti senza l'ausilio degli strumenti elettronici.
  - Le modalità da seguire per rendere effettiva l'introduzione delle misure tecniche.
- Le responsabilità degli incaricati e del personale tecnico, dettagliate in ciascuna procedura implementata.

CAPITOLO 6 - Contratti con le Terze Parti

Ai sensi del comma 7 dell'articolo 19 del Disciplinare Tecnico, in questo capitolo vengono descritti i requisiti da tenere in considerazione per quanto riguarda il trattamento dei dati personali in tutti i contratti che L' Istituto Giannina Gaslini deciderà di stipulare con Società esterne.

Tali requisiti sono descritti nella procedura:

- PRO011 - Procedura per la gestione dei requisiti di sicurezza nei contratti.

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

“PRO001”

Procedura per la gestione degli accessi fisici

Documento a disposizione di tutto il personale

1.0	17/03/2006	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 SCOPO

La presente procedura ha lo scopo di descrivere gli aspetti legati al Codice sulla Privacy nella regolamentazione degli accessi fisici alle strutture dell'Istituto G. Gaslini durante e al di fuori degli orari di lavoro. Gli aspetti di carattere generale e legati alla sicurezza sul luogo di lavoro sono descritti da documenti e procedure relativi agli adempimenti previsti nel D.lgs. 9 aprile 2008, n. 81 e riportati nella sezione Riferimenti.
È necessario regolamentare l'accesso delle persone ai locali che ospitano apparecchiature ed uffici, al fine di prevenire:

- atti di sabotaggio;
- furti;
- accesso a informazioni riservate;
- danneggiamenti, anche involontari, alle apparecchiature o al servizio, da parte di personale estraneo;
- infortuni al personale, interno ed esterno, e/o ai visitatori.

Tra i locali protetti assume massima importanza il CED, che ospita le apparecchiature di elaborazione e trasmissione dati.

2 CAMPO DI APPLICAZIONE

La presente procedura si applica a tutto il personale dell'Istituto e in generale a tutte le persone che per qualsivoglia motivo debbano avere accesso alle strutture aziendali. La presente procedura regola l'accesso a partire dall'esterno dell'Istituto (suolo pubblico) fino alle aree di pertinenza dei singoli incaricati (in pratica nelle aree comuni dell'Istituto quali ad esempio viali, scale, corridoi).

3 RESPONSABILITA'

Il controllo degli accessi alle aree dell'Istituto durante l'orario di lavoro, è responsabilità del personale addetto alla portineria e agli accessi carrai, secondo quanto di loro competenza.
Il controllo degli accessi alle aree aziendali al di fuori degli orari di lavoro è garantito dai sistemi di sicurezza descritti nella sezione 4.
Tutto il personale ha la responsabilità di monitorare e controllare gli accessi fisici ai locali di loro pertinenza, e di assicurarsi che i terzi accedano secondo le regole definite nella presente procedura e dalla Direzione Sanitaria. Il controllo degli accessi

all'interno delle aree di pertinenza dei singoli incaricati è descritto nella procedura PRO004 – Gestione del posto di lavoro e dell'accesso agli uffici.
La responsabilità della corretta applicazione della presente procedura ricade:

- Sul responsabile del personale di portineria per quanto riguarda l'accesso dall'esterno;
- Sui responsabili per i trattamenti per quanto riguarda il controllo all'interno dei reparti.

4 MODALITA' ESECUTIVE

4.1 Accesso da Via Gerolamo Gaslini

L'Istituto dispone di un accesso carraio principale utilizzato da dipendenti, visitatori e terzi sito in via Gerolamo Gaslini.
L'accesso per i veicoli avviene attraverso un ingresso a sbarra presidiato dal personale di portineria; l'accesso per i pedoni avviene attraverso due distinti ingressi aperti durante l'orario di lavoro. Il primo riservato al personale dipendente che accede tramite tornello, apribile con badge presenze, l'altro senza barriere, presidiato da operatore, per il pubblico.

4.2 Accesso da via Redipuglia

Esistono altri due ingressi da via Redipuglia utilizzati da dipendenti, visitatori e terzi.
L'accesso per i veicoli avviene attraverso un ingresso a sbarra presidiato dal personale di portineria; l'accesso per i pedoni avviene attraverso un apposito varco presidiato.

4.3 Norme generali

Gli accessi veicolari, gli orari di apertura degli ingressi, gli strumenti di controllo degli accessi e la gestione dei parcheggi regolamentati con delibera 39 del 16/04/2004.

4.4 Modalità di controllo all'interno dei reparti

L'accesso ai reparti è consentito al pubblico durante gli orari di visita e per le necessità di servizio, compatibilmente con la capacità di accoglienza del reparto

stesso. La riservatezza nel rapporto con i pazienti e i visitatori è garantita nel rispetto di quanto previsto dall'art. 83 del D.Lgs. 196/2003.
Data la natura dell'attività svolta dall'Istituto, i singoli incaricati devono prestare particolare attenzione onde evitare che persone non autorizzate accedano ad aree riservate o circolino al di fuori degli orari consentiti.
Gli aspetti di sicurezza legati alla gestione del posto di lavoro sono descritti dalla procedura PRO-004.

4.5 Responsabilità dei controlli

Per tutte le aree ove sono trattati dati personali la responsabilità del controllo è dei singoli incaricati.
E' responsabilità degli incaricati segnalare prontamente tutte le situazioni anomale al Responsabile dei trattamenti competente.
E' responsabilità del Responsabile dei trattamenti competente raccogliere e gestire le segnalazioni di incidente per affrontarle e risolverle in opportuna sede.

5 RIFERIMENTI

Dlgs 196/2003 – Disciplinare Tecnico punti 19, 29.
Procedura PRO004 – Procedura per la gestione del posto di lavoro e dell'accesso agli uffici

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

“PRO002”
Procedura di autenticazione informatica

Documento a disposizione di tutto il personale

1.0	15/09/05	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 SCOPO

La presente procedura ha lo scopo di definire i criteri da seguire per la gestione e l'utilizzo di un sistema di autenticazione informatica secondo quanto prescritto dal Dlgs 196/2003 "Codice in materia di protezione dei dati personali" (Disciplinare Tecnico punti da 1 a 11).

2 CAMPO DI APPLICAZIONE

A tutto il personale dell'Istituto incaricato del trattamento dei dati personali mediante strumenti elettronici (Personal Computer).

3 RESPONSABILITÀ

La Direzione Sanitaria ha la responsabilità di autorizzare la creazione, modifica e cancellazione dei nuovi utenti e delle relative credenziali di autenticazione sugli applicativi di area.

La responsabilità della creazione di nuovi utenti (account) per gli incaricati, di modificare i privilegi di accesso di un utente e di cancellare gli account non più necessari è del Referente per i Sistemi Informativi.

Il personale incaricato di gestire gli accessi al Sistema Informativo (Referente per i sistemi informativi e suoi collaboratori) è responsabile della loro creazione, cancellazione e revisione, oltre che dell'assegnazione delle password temporanee. E' altresì responsabile della comunicazione all'incaricato di tutta la documentazione eventualmente prevista dalla procedura e dell'account stesso.

I singoli incaricati hanno la responsabilità di gestire le loro password, modificando al primo accesso la password temporanea assegnatagli, con una definitiva scelta da loro.

Gli incaricati hanno la responsabilità di scegliere ed utilizzare le proprie password secondo quanto descritto nella seguente procedura.

Gli incaricati sono informati del fatto che l'accesso ai sistemi e agli applicativi è autorizzato esclusivamente per ragioni di servizio. Gli applicativi devono essere utilizzati esclusivamente per gli scopi inerenti al loro impiego, anche per quanto riguarda i dati che tali applicativi possono trattare. Si ricorda che il Codice sulla protezione dei dati personali non consente il trattamento di dati non pertinenti allo scopo che ci si prefigge (principio di necessità, art. 3).
Il personale tecnico, per esigenze di servizio, deve possedere i privilegi di amministratore di tutte le postazioni di lavoro.

4 MODALITÀ ESECUTIVE

4.1 Registrazione delle credenziali di autenticazione

4.1.1 Applicativi di Area Sanitaria (escluso dipartimentali)

Quando si rende necessario creare una nuova credenziale di autenticazione (login e password) per un nuovo incaricato al trattamento di dati personali della Gestione Sanitaria Territoriale o quando si rende necessario la modifica dei diritti di accesso di un incaricato già registrato, la U.O. interessata farà richiesta via mail, alla Direzione Sanitaria.
La D.S. autorizza l'intervento inviando una conferma via mail al SIA.
Il personale tecnico provvederà a creare, modificare o eliminare l'account secondo specifiche. Nel caso della creazione di un nuovo utente viene assegnata una password temporanea, da modificarsi al primo accesso.
L'ID utente non deve in alcun modo indicare il livello di privilegio assegnato all'utente.
Le modalità per la definizioni dei privilegi devono tener conto del ruolo che l'incaricato dovrà svolgere, nel caso di nuovo incaricato la definizione dei privilegi deve essere fatta in collaborazione con il Direzione di appartenenza dell'incaricato, nel caso invece di modifica deve essere presa in esame la precedente dichiarazione scritta che deve sempre essere aggiornata; nel caso in cui questa non fosse definita occorre procedere alla sua creazione.
Ai sensi del punto 6 del Disciplinare Tecnico, gli account utilizzati non sono riutilizzati per altri incaricati, nemmeno in tempi diversi.
La richiesta iniziale e tutte le successive comunicazioni sono archiviate presso i Sistemi Informativi.

4.1.2 Accesso ad internet e posta elettronica

Quando si rende necessario creare una nuova credenziale di autenticazione (login e password) per l'accesso ad Internet e alla posta elettronica o quando si rende necessario la modifica dei diritti di accesso di un incaricato già registrato, la U.O. interessata farà richiesta via mail, alla Direzione dei Sistemi Informativi.
Il personale tecnico provvederà a creare, modificare o eliminare l'account secondo specifiche. Nel caso della creazione di un nuovo utente è assegnata una password emporanea, da modificarsi al primo accesso.
L'ID utente non deve in alcun modo indicare il livello di privilegio assegnato all'utente.
Al termine dell'intervento, per quanto riguarda la posta elettronica l'incaricato firma per ricevuta la richiesta di attivazione, per quanto riguarda l'accesso ad Internet l'incaricato firma il MOD008 02
Ai sensi del punto 6 del Disciplinare Tecnico, gli account utilizzati non sono riutilizzati per altri incaricati, nemmeno in tempi diversi.
La richiesta iniziale e tutte le successive comunicazioni sono archiviate presso i Sistemi Informativi.

4.1.3 Accesso agli applicativi di area amministrativa

Quando si rende necessario creare una nuova credenziale di autenticazione (login e password) per l'utilizzo degli applicativi ERP e HR (gestione amministrativa e delle risorse umane) o quando si rende necessario la modifica dei diritti di accesso di un incaricato già registrato, la U.O. interessata farà richiesta via mail, alla Direzione dei sistemi informativi.
Il personale tecnico provvederà a creare, modificare o eliminare l'account secondo specifiche. Nel caso della creazione di un nuovo utente è assegnata una password temporanea, da modificarsi al primo accesso.
L'ID utente non deve in alcun modo indicare il livello di privilegio assegnato all'utente.
Ai sensi del punto 6 del Disciplinare Tecnico, gli account utilizzati non sono riutilizzati per altri incaricati, nemmeno in tempi diversi.
La richiesta iniziale e tutte le successive comunicazioni sono archiviate presso i Sistemi Informativi.

4.2 Selezione e uso della Password

Per quanto riguarda la gestione delle password, questa viene affidata ai singoli incaricati, come prescritto dal Dlgs 196/2003.
All'incaricato è assegnata dai tecnici una password temporanea che il sistema chiede di cambiare all'atto del primo accesso. L'incaricato dovrà creare la password secondo quanto indicato nei punti successivi.

4.2.1 Selezione

Le password che un incaricato deve creare, devono soddisfare le seguenti misure minime (punto 5 del Disciplinare Tecnico):

- ✓ La password deve avere una lunghezza minima di otto caratteri; laddove lo strumento elettronico non lo consenta, la lunghezza deve essere pari al massimo consentito.
- ✓ La password non deve essere divulgata, né custodita in modo improprio, per evitare la possibilità di utilizzo da parte di terzi non autorizzati.
- ✓ Le password non devono contenere riferimenti agevolmente riconducibili all'incaricato: nomi propri, date di nascita, ecc NON sono password ammesse. Una password di qualità, infatti, non deve basarsi su nomi di persone, animali, oggetti, o comunque ricavabili da un dizionario, anche di lingua straniera.
- ✓ Le password possono essere di tipo alfanumerico, ovvero utilizzare caratteri, cifre e simboli.
- ✓ Il codice di identificazione (login) non può essere utilizzato per incaricati diversi.
- ✓ La durata delle password di accesso al dominio dell'Istituto e conseguentemente agli applicativi aziendali accessibili dallo stesso è stabilita in 90 giorni, per tutti gli incaricati.

4.3 Disattivazione/cancellazione delle credenziali di autenticazione

La disattivazione delle credenziali è di responsabilità dei sistemi informativi, che agiscono su richiesta della U.O interessata o della Direzione sanitaria (nel caso di applicazioni di area sanitaria non dipartimentali) . Le credenziali devono essere disattivate contestualmente alla richiesta nei seguenti casi (punti 7 e 8 del Disciplinare Tecnico):

- ✓ Nel caso incaricati che cessano il rapporto di lavoro;
- ✓ Nel caso in cui l'incaricato in possesso della credenziale perda la qualità che gli consente l'accesso ai dati personali (cambio di mansione, ecc.).

La cancellazione fisica dell'account è effettuata dai sistemi informativi periodicamente, di solito una volta l'anno, dopo aver provveduto all'archiviazione dei dati aziendali di proprietà dell'account.

4.4 Accesso alla postazione di lavoro in caso di prolungata assenza dell'incaricato

La seguente procedura ha lo scopo di ottemperare al punto 10 del Disciplinare Tecnico.

In caso di necessità, per assenza prolungata dell'incaricato o comunque per sua irreperibilità, di accesso alle risorse protette da password, il referente dei sistemi informativi può forzare l'accesso cancellando la password dell'utente. L'operazione, come tutte le operazioni di modifica di profilo, deve essere richiesta dalla Direzione interessata via mail. I sistemi informativi inviano all'incaricato assente una mail informativa.

Al ritorno, l'incaricato assente avrà l'obbligo di sostituire immediatamente la propria password.

La particolare architettura del sistema informativo, delle basi dati e delle politiche di accesso agli applicativi rendono comunque remota la necessità assoluta di dover operare da una determinata postazione o con uno specifico utente.

5 RIFERIMENTI

Dlgs 196/2003, Disciplinare Tecnico, punti da 1 a 11

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

“PRO003”

Procedura per la gestione dei profili di accesso

Documento a disposizione di tutto il personale

1.0	17/03/2006	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 SCOPO

La presente procedura ha lo scopo di stabilire le modalità di gestione dei diritti di accesso ai sistemi e ai programmi utilizzati da dagli incaricati in conformità al Dlgs 196/2003.

2 CAMPO DI APPLICAZIONE

La presente procedura si applica al personale dei sistemi informativi per la parte tecnica, e a tutto il personale dell'Istituto incaricato del trattamento dei dati personali mediante strumenti elettronici (Personal Computer) per la parte esecutiva.

3 RESPONSABILITÀ

Il Disciplinare Tecnico stabilisce che qualora gli incaricati svolgano mansioni differenti debba essere implementato un sistema di autorizzazione, ovvero la definizione di profili di accesso da associare ad ogni singolo incaricato in modo da identificare con corrispondenza univoca una funzione aziendale e un profilo utente.

La definizione dei profili utente viene stabilita dalle U.O interessate.

Nella definizione dei profili utente si include anche l'abilitazione alla navigazione Internet e la posta elettronica.

Il personale dei Sistemi Informativi è responsabile della loro creazione, cancellazione e revisione. E' altresì responsabile della comunicazione all'utente di tutta la documentazione prevista, quando necessario.

4 MODALITÀ ESECUTIVE

L'accesso agli applicativi deve essere gestito con modalità che consentano la definizione di profili di accesso differenziati per incaricati con mansioni differenti.
L'accesso agli applicativi deve essere limitato – ove consentito dall'applicativo stesso – alle sole informazioni e funzioni richieste per lo svolgimento delle attività che sono assegnate all'incaricato.
Ove è reso possibile dal software applicativo, devono essere specificate le funzioni e i dati a cui deve essere concesso l'accesso e la modalità (sola lettura, sia lettura che scrittura, solo dati dei clienti, ecc).
Per esigenze di servizio, esistono alcune postazioni di lavoro utilizzate a rotazione continua con un utente generico.

4.1 Modalità di creazione di nuovi profili

Si veda quanto disposto nella procedura PRO002 – Procedura di autenticazione informatica.

4.2 Disattivazione e cancellazione degli account di accesso

La disattivazione viene effettuata dai Sistemi Informativi contestualmente alla richiesta via mail che viene inoltrata dalla Direzione competente. La cancellazione viene effettuata sempre dai Sistemi Informativi periodicamente, di norma una volta l'anno nel corso delle normali operazioni di manutenzione dei sistemi.

4.3 Riesame dei diritti di accesso

Nella gestione degli accessi, ha molta importanza la verifica periodica di tutti i diritti e di tutti i privilegi di accesso accordati, al fine di evitare gli accessi non autorizzati a dati o funzionalità.
La revisione viene fatta periodicamente, almeno ogni anno.
Al fine di garantire la corretta attribuzione dei profili di accesso e di evitare che alcuni utenti abbiano in uso profili non attinenti ai loro incarichi è necessario che le Direzioni competenti comunichino tempestivamente ai Sistemi Informativi tutte le variazioni (assunzioni, dimissioni, cambi di mansione), in modo che siano riflesse nel minore tempo possibile sui profili di accesso. Si fa presente che la presenza di profili utente

non congrui o non più attivi costituisce un grave rischio per la sicurezza del sistema informativo, oltre ad una violazione delle misure minime.

5 RIFERIMENTI

Dlgs 196/2003, Disciplinare Tecnico punti da 12 a 14

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

"PRO004"

Procedura per la gestione del posto di lavoro e dell'accesso agli uffici

Documento a disposizione di tutto il personale

1.0	17/03/2006	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 PREMESSA

Un comportamento corretto dell'utente è una misura di sicurezza fondamentale per ridurre i rischi di perdita o di divulgazione non autorizzata dei dati personali. L'uso corretto delle apparecchiature in dotazione e la corretta conservazione dei documenti (cartacei e in formato elettronico) riducono drasticamente questi rischi.

2 SCOPO

Lo scopo della presente procedura è quello di gestire il posto di lavoro e l'accesso agli uffici e alle aree ad accesso controllato per prevenire possibili furti, danni e divulgazione di dati personali, sensibili e giudiziari.

3 CAMPO DI APPLICAZIONE

La procedura si applica a tutto il personale dell'Istituto incaricato del trattamento dei dati personali.

4 RESPONSABILITÀ

Tutti gli incaricati al trattamento dei dati personali, sensibili e giudiziari sono tenuti ad osservare quanto specificato nella presente procedura e nella lettera di incarico, e a segnalare tutte le violazioni alle disposizioni specificate al responsabile dei trattamenti.

Tutti gli incaricati al trattamento hanno la responsabilità di utilizzare gli strumenti aziendali solo per gli scopi per i quali sono destinati. I trattamenti di dati personali, sensibili e giudiziari sono consentiti solo nel rispetto di quanto disposto dal Codice, particolarmente per quanto riguarda l'art. 3 (Principio di Necessità).

5 MODALITÀ ESECUTIVE

I dati personali, sensibili e giudiziari e gli strumenti di elaborazione dati devono essere adeguatamente protetti da modifiche, furti, e divulgazione non autorizzata.

E' buona norma mantenere la postazione di lavoro (scrivania) quanto più possibile ordinata e sgombra da documenti, che potrebbero essere smarriti, o letti da persone non autorizzate. I documenti contenenti dati sensibili e/o giudiziari devono essere conservati sotto chiave quando non sono utilizzati e soprattutto fuori dall'orario di lavoro.
In caso di allontanamento momentaneo dalla postazione di lavoro l'accesso a terzi non autorizzati deve essere impedito.

I personal computer devono essere bloccati quando non sono sorvegliati e utilizzati. Per bloccare l'accesso al computer si utilizzano le apposite funzioni del sistema operativo (con i sistemi Windows basta premere i tasti Ctrl+Alt+Canc). È buona norma in tutti i casi in cui ci si allontana dal posto di lavoro uscire dagli applicativi che gestiscono dati personali.

All'accensione del personal computer per poter accedere alle risorse locali e di rete è necessario utilizzare delle credenziali di autenticazione, così come dettagliato nella procedura PRO002.

Le apparecchiature in dotazione agli incaricati e i dati da loro gestiti sono un bene aziendale di valore rilevante. Gli incaricati sono tenuti a utilizzare gli strumenti elettronici esclusivamente per fini legati all'attività lavorativa. Ogni modifica hardware e software deve essere notificata ai sistemi informativi e in generale non è consentito modificare in alcun modo la configurazione delle postazioni di lavoro, se non per scopi legati all'attività lavorativa. Si fa presente che l'installazione di software non autorizzato comporta rischi di malfunzionamenti legati all'incompatibilità con altri applicativi o con i sistemi operativi e può configurare un illecito penale nel caso in cui il software installato non fosse regolarmente licenziato.

L'Azienda mette a disposizione dei servizi che ne necessitano stampanti personali o di reparto per la stampa di documenti riservati, o comunque contenenti dati sensibili. L'uso delle stampanti di sistema o di corridoio dovrebbe essere riservato solo per stampe di dati comuni. E' buona norma, in ogni caso, non lasciare incustodite per lungo tempo le stampe prodotte.

L'impiego dei PC portatili al di fuori dell'Istituto è consentito solamente per ragioni di servizio (comando, missione o simili). E' assolutamente proibito l'utilizzo dei portatili

per ragioni personali. Per quanto riguarda l'impiego dei computer portatili si veda anche quanto disposto dalla procedura PRO004 - Procedura per la gestione del posto di lavoro e degli accessi agli uffici.

Allo stesso modo l'uso di fax e di fotocopiatrici in modo non presidiato può essere causa di violazione della riservatezza. L'invio, la ricezione e la riproduzione di documenti, specialmente se contenenti dati sensibili o giudiziari dovrebbe essere eseguito presidiando lo strumento.

Per la memorizzazione dei documenti sono disponibili arre riservate sui dischi dei server in rete installati presso la sala macchine del SIA aziendale. Queste aree sono assegnate su richiesta autorizzata. La mancata osservanza di queste regole crea potenziali rischi di divulgazione non autorizzata di dati. E' buona norma non memorizzare documenti in aree disco diverse da quelle assegnate, opportunamente protette da intrusioni non autorizzate e regolarmente salvate con i sistemi automatici di backup previsti. E' da evitare la definizione di aree condivise.

Tutti i dati aziendali debbano essere memorizzati in originale sui dischi di rete. Sui dischi locali è consentita solo la memorizzazione di copie per scopi di lavoro, e comunque nel rispetto delle misure minime di sicurezza.

L'uso di Internet e della posta elettronica da parte degli utenti del Sistema informativo Aziendale ha un costo considerevole in termini di banda necessaria e spese per le operazioni di manutenzione e amministrazione, per questo motivo l'accesso ai servizi di rete in generale e ad Internet nel caso specifico viene fornito agli utenti che ne hanno necessità per supportare la loro attività di lavoro. Si fa inoltre notare che anche la posta elettronica è da considerarsi a tutti gli effetti uno strumento che l'Azienda mette a disposizione degli incaricati per lo svolgimento del loro lavoro: non è quindi da considerarsi, in nessun caso, una proprietà del singolo incaricato.

Obblighi da osservare:

- L'accesso ad Internet e alla posta elettronica avviene attraverso una procedura di autenticazione (utente e password).
- È consentito l'uso di Internet per esclusivi motivi di lavoro.

- E' vietato l'uso della casella di posta aziendale per uso personale.
- È vietato l'accesso ai siti inappropriati e non strettamente connessi con l'attività lavorativa. Si fa presente che è attiva in azienda una politica di deny che proibisce l'accesso a certe categorie di siti.
- È vietato in generale l'uso di risorse informatiche aziendali per svolgere attività illegali o per svolgere attività commerciali non autorizzate.
- È vietato il download di software se non con autorizzazione dell'Azienda. Il download del software è una delle cause principali di contagio da virus e può causare malfunzionamenti qualora modifichi la configurazione del client sul quale viene installato. Inoltre il software scaricato da Internet può essere soggetto a particolari condizioni di licenza il cui uso è spesso concesso nell'ambito personale e non all'interno di una realtà aziendale .

La violazione alle norme sopra citate può essere perseguita a norma di contratto e di legge. E' facoltà dall'Azienda, qualora lo ritenga necessario, effettuare controlli sia sul traffico internet generato dagli utenti, sia sul contenuto delle caselle di posta elettronica degli incaricati nel rispetto di quanto indicato nelle linee guida del Garante per posta elettronica e internet (Gazzetta Ufficiale n. 58 del 10 marzo 2007).

La comunicazione via telefono di dati sensibili o giudiziari è vietata a persone non identificabili. Qualsiasi richiesta di dati sensibili o giudiziari da parte di persone, enti, istituzioni esterne deve essere autorizzata e documentata in forma scritta. In ogni caso, la divulgazione di dati sensibili o giudiziari all'interno dell'Azienda deve avvenire solo dietro autorizzazione della Direzione Generale e per fondati motivi.

Le aree aziendali sono suddivise in tre categorie in relazione alla loro riservatezza:

- **Aree comuni**: sono tutte quelle aree non presidiate dove è possibile accedere senza passare da controlli. Sono da considerare tali i corridoi, le scale e tutte le aree esterne ai reparti ed ai padiglioni viali e parcheggi compresi.
- **Aree riservate** : locali in cui viene svolta l'attività sia amministrativa (uffici), sia sanitaria (reparti). Sono aree normalmente presidiate con accesso regolamentato.
- **Aree ad accesso limitato**: locali in cui l'accesso è controllato (porte chiuse, accesso via badge, ecc.) e limitato agli utenti autorizzati o accompagnati da

personale autorizzato rientrano. Rientrano in questa categoria le Sale Operatorie e la sala macchine del SIA.

6 RIFERIMENTI

PRO002 Autenticazione Informatica

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

“PRO005”

Procedura per la protezione da software maligno

Documento a disposizione di tutto il personale

1.0	17/03/2006	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 SCOPO

La presente procedura ha lo scopo di definire le contromisure necessarie a proteggere l'infrastruttura di rete Aziendale dalle minacce provenienti da software maligno secondo quanto indicato dal Dlgs 196/2003 (Disciplinare Tecnico punto 16).

2 CAMPO DI APPLICAZIONE

La procedura si applica ai Sistemi informativi per la parte di gestione centralizzata, e a tutti gli utenti dotati di personal computer per la parte di corretto utilizzo del sistema.
L'introduzione delle reti locali e di Internet ha prodotto, come immediata conseguenza, la moltiplicazione del numero di canali attraverso i quali può avvenire la diffusione di programmi maliziosi (malicious software) in grado di sfruttare vulnerabilità del software, al fine di alterare e utilizzare in maniera illegittima le risorse informatiche, con un aumento del rischio per l'operatività, l'immagine aziendale e potenziali conseguenze legali.
Tra i programmi maliziosi il virus informatico è la minaccia più ricorrente ed efficace, che può dar luogo a danni rilevanti, con conseguenze di gravità variabili, quali il rallentamento o blocco nell'operatività corrente, la perdita di tempo e produttività, la negazione del servizio agli utenti, la compromissione o perdita dei dati e gli accessi non autorizzati a risorse aziendali.

2.1 Definizione di virus

La definizione giuridica di virus dell'art.615 quinquies C.P. è "…un programma informatico …avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei
dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento" .
Nella G.U. del 22.03.2002, n.69, il virus viene definito come: "una procedura automatica autoriproducente che, quando eseguita, effettua più copie di se stessa; a loro volta le copie si moltiplicano con metodo analogo e così via".

3 REGOLE PER LA PROTEZIONE DA VIRUS

Di seguito sono elencate le principali regole:

- tutti i server ed i personal computer dell'Istituto devono essere dotati di programmi antivirus aggiornati all'ultima versione disponibile rilasciata dal fornitore del prodotto;
- tutti i personal computer dell'Istituto devono essere dotati di programma antispyware aggiornato all'ultima versione disponibile rilasciata dal fornitore del prodotto.
- sui personal computer l'attivazione dei prodotti di antivirus e antispyware deve essere eseguita automaticamente alla ripartenza;
- sui server l'esecuzione dell'antivirus deve essere eseguita con cadenza periodica, non superiore alle 24 ore;
- qualora ci sia la verificata effettiva necessità di dover aprire un oggetto informatico di provenienza esterna non certificata si dovrà inviare il file al personale di SIA per poter essere controllato con appositi strumenti;
- E' proibito:
    - l'uso di software gratuito (o shareware) prelevato da siti internet non attendibili o in allegato a riviste o libri;
    - il prelievo di file BBS o da servizi commerciali in linea o da banche dati.

4 TERMINOLOGIA

4.1 Programmi maliziosi

I programmi maliziosi (malicious software) sfruttano vulnerabilità intrinseche del software, al fine di alterare e utilizzare in maniera illegittima le risorse del sistema che lo ospita. Per attivarsi necessitano di un programma che li ospita oppure possono agire come programmi autonomi; per diffondersi replicano il proprio codice automaticamente o necessitano di essere impiantati sulle postazioni.

L'analisi delle modalità di funzionamento dei malicious software conduce alla classificazione in:

- Malware: contrazione di malicious software che indica tipologie di applicazioni concepite per provocare danni: virus, cavalli di troia e worm.

- Spyware: software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete ecc.) ma anche dati personali, trasmettendoli tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata. Il tutto senza il consenso dell'utente.
- Payload: effetto contenuto nel malware, di gravità variabile.
- Virus: programma in grado di incapsulare il proprio codice, effettuando repliche di se stesso in un programma e/o file di dati che lo ospita; l'esecuzione del programma o l'accesso al file produce la duplicazione e diffusione del virus. I virus informatici si differenziano, a loro volta, in funzione delle modalità con cui agiscono e delle proprietà dannose, in:
    - parassita: sottoclasse comprendente gran parte dei virus comuni, la cui natura prevede l'infezione del maggior numero di file eseguibili dal sistema ospite;
    - residente in memoria: virus informatico costituito da blocchi di codice inseriti in programmi residenti nella memoria principale (RAM) del sistema ospite; infetta i programmi eseguiti, fino alla loro rimozione dalla RAM.
- Boot sector/Master Boot Record infector: virus informatico che infetta i settori di avvio dei dischetti removibili (boot sector) o dischi rigidi (Master Boot Record); è caricato in memoria nella fase di avvio del computer (bootstrap), prima del caricamento del sistema operativo, ed usa servizi del BIOS per l'infezione.
- File infector: virus informatico che infetta file eseguibili, modificandone la struttura interna per essere eseguito; può alterare i file, preservandone le funzioni o rendere i file irrecuperabili (overwriting virus). Una particolare tipologia, i companion virus, non modifica la struttura interna del file infetto, ma crea copie del file con stesso nome ed estensione diversa; per eseguire le copie il virus sfrutta priorità assegnate da alcuni sistemi operativi a estensioni di file ed usate quando i programmi sono eseguiti specificandone il nome ed omettendo l'estensione.

- Macro virus: virus informatico che infetta le macro usate da file o applicazioni per automatizzare l'esecuzione di attività; è scritto generalmente in linguaggio Visual Basic o in WordBasic.
- Multipartito: virus informatico concepito per infettare sia gli archivi che i settori di avvio.
- Polimorfo: virus informatico che rende difficoltosa la rilevazione da parte dell'Antivirus usando specifiche tecniche per cambiare continuamente parti del suo codice; mediante un algoritmo, cifra gran parte del proprio codice e muta di continuo la restante parte in chiaro, costituita dalle istruzioni necessarie a decifrare la parte principale del virus, per poi cedergli il controllo.
- Retrovirus: virus informatico che attacca l'Antivirus tentando di neutralizzarlo.
- Script virus: virus scritto in linguaggio di tipo "script" (ad es. Visual Basic Script).
- Invisibile (stealth) virus: virus informatico "furtivo" che utilizza tecniche atte a eludere il controllo Antivirus, es. infetta file senza aumentarne la lunghezza oppure agisce perturbando le richieste di interruzione (interrupt) interne al computer.
- Zoo virus: virus presente solo nei laboratori di ricerca, non diffuso tra gli utenti.
- Worm: programma indipendente in grado di autoreplicarsi e di diffondere repliche del proprio codice su altri sistemi in varie modalità; nella fase di riproduzione e diffusione produce azioni ed effetti dannosi e/o indesiderati sul sistema che lo ospita.
- Cavalli di Troia (Trojan horse): programma o parte di programma che effettua operazioni diverse da quelle ritenute dall'utente; differentemente dai virus non è autoreplicante.
- Hoax: termine usato per indicare i messaggi di posta elettronica che diffondono false notizie sui virus, causando effetti negativi. L'allarme invita a non aprire il file allegato ad un certo messaggio, perché potrebbe contenere un pericoloso virus, e raccomanda di diffondere la

notizia al maggior numero di persone possibili. La veridicità avviene facendo transitare i messaggi con indirizzi di note aziende informatiche, affinchè il ricevente abbia l'impressione che il messaggio provenga da fonte ufficiale.

- Joke: programma innocuo che simula il payload di un programma ingannevole (es. formattazione del disco, visualizzazione della caduta di lettere sullo schermo).
- Backdoor/Trapdoor: meccanismo, generalmente usato in fase di sviluppo di un programma, che consente l'accesso a informazioni e servizi offerti dal programma in modalità non standard (es. porte non documentate), aggirando le procedure di autenticazione e controllo.

4.2 Ciclo di vita di un virus informatico

Il ciclo di vita di un virus è organizzato generalmente in quattro fasi:

- incubazione: fase in cui il virus rimane inerme, in attesa di un evento scatenante;
- propagazione: fase in cui il virus produce copie di se stesso e le inserisce nei programmi, affinché ogni copia passi subito in fase di propagazione;
- attivazione: fase in cui il virus viene attivato, con eventi scatenanti molteplici, al fine di compiere le funzioni per cui è stato ideato;
- esecuzione: fase in cui il virus porta a termine il proprio compito.

4.3 Antivirus

L'Antivirus è un software utilizzato come meccanismo di difesa e di controllo, che consente di prevenire la diffusione di infezioni, rilevare ed eliminare virus/worm informatici e cavalli di Troia noti. L'antivirus prevede la scansione euristica (indicata con nomenclatura diversa, es. sandbox, bloodhound,ecc...), applicabile in casi specifici, per rilevare eventuali virus nuovi, basandosi sui meccanismi di virus conosciuti.

4.4 Antispyware

Software che cerca nel computer tracce di programmi che installano dati o programmi a nostra insaputa per sapere quello che facciamo viene fatto con il pc. Al momento sono indispensabili come i firewall e gli antivirus.

5 RESPONSABILITÀ

Il personale dei Sistemi Informativi ha la responsabilità della scelta dei software antivirus, della sua installazione e gestione operativa, della verifica periodica dell'efficacia dei software antivirus e dell'aggiornamento dei file di dati dei software antivirus.
Gli incaricati hanno la responsabilità di non manomettere le configurazioni impostate dal personale dei Sistemi Informativi e di segnalare tempestivamente funzionamenti anomali dei propri sistemi al personale responsabile della gestione del sistema.

6 MODALITÀ ESECUTIVE

L'infrastruttura di rete Aziendale deve essere adeguatamente protetta contro le minacce da software maligno.
Le contromisure che seguono considerano gli aspetti atti a prevenire, individuare e rimuovere la presenza di software maligno.

6.1 Prevenzione

Tutti gli incaricati riceveranno una formazione sui rischi legati al software maligno e sul corretto utilizzo degli strumenti di scansione.

L'incaricato si impegna a non modificare per nessun motivo la configurazione del sistema antivirus della sua macchina.
Gli incaricati non devono creare, eseguire, inoltrare o introdurre nessun tipo di codice maligno. Gli incaricati che violano tale norma possono essere soggetti ad azioni disciplinari fermo restando la possibilità di segnalare alla competente Autorità Giudiziaria ogni possibile violazione costituente reato.

Tutti i computer connessi alla rete aziendale sono protetti dal software maligno attraverso idonei strumenti. Gli strumenti di cui l'Azienda si è dotata comprendono:
Il sistema antivirus comprende

- prodotto antivirus per client
- prodotto antivirus per server
- prodotto antivirus (agent) per sistemi di posta elettronica.

L'efficacia dell'antivirus viene periodicamente verificata attraverso l'analisi dei tempi di fermo macchina e delle perdite di dati causate dal software maligno in un'ottica di medio periodo dal personale dei sistemi informativi.

L'aggiornamento dei software antivirus deve essere gestito in modo centralizzato e distribuito automaticamente su tutte le macchine presenti in rete ogni volta che l'utente si collega alla rete.

6.2 Individuazione

Gli incaricati devono informare in modo tempestivo il personale tecnico se sospettano la presenza di codice maligno sui propri sistemi (ad esempio hanno osservato comportamenti inusuali di un'applicazione o cambiamenti di configurazione dei propri sistemi).
In caso di infezione, il sistema è configurato in modo da eseguire le seguenti operazioni sui file infetti nel seguente ordine:

- Cleaning: il file viene pulito e reso riutilizzabile;
- Quarantine: il file viene posto in un folder riservato non accessibile;

6.3 Rimozione

Fermo restando quanto detto al paragrafo precedente, in caso di inefficacia dei sistemi antivirus, il sistema sospettato di essere infetto da un virus non ancora conosciuto sarà immediatamente isolato dal resto della rete.
Il sistema non sarà riconnesso alla rete fino a quando non sarà possibile garantirne il perfetto funzionamento.

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

"PRO006"

Procedura per la gestione dei backup

Documento riservato ai Sistemi Informativi

1.0	17/03/2006	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 SCOPO

La presente procedura ha lo scopo di definire le modalità e le responsabilità per la corretta esecuzione dei salvataggi delle banche dati e degli archivi dell'Istituto contenenti dati personali, in accordo col dettato del Dlgs 196/2003.

2 CAMPO DI APPLICAZIONE

La presente procedura si applica a tutti gli utenti del sistema informativo per la parte di loro pertinenza (richiesta di ripristino e policy di archiviazione dei dati da sottoporre a backup) e i sistemi informativi per la corretta gestione degli strumenti di backup.

3 RESPONSABILITA'

Per i dati memorizzati su sistemi centralizzati normalmente installati nel data center (CED). Il Referente per i Sistemi Informativi ha la responsabilità della corretta esecuzione dei salvataggi, della gestione e della conservazione dei supporti rimovibili e del ripristino dei dati a fronte di malfunzionamenti o perdite degli stessi.Per queste operazioni si avvale del personale tecnico del SIA.
Gli incaricati hanno il compito di verificare la correttezza dei dati di loro competenza e di avvertire tempestivamente il SIA qualora si verificassero situazioni anomale.
Per quanto riguarda i sistemi dipartimentali gestiti cioè autonomamente presso i locali delle UU.OO. , la responsabilità del corretto e sistematico salvataggio dei dati è del responsabile dell'unita stessa.

4 MODALITA' ESECUTIVE

Secondo quanto previsto dal Disciplinare Tecnico (punto 18), le banche dati e gli archivi contenenti dati personali devono essere salvati con cadenza almeno settimanale.

4.1 Dati sottoposti a salvataggio nella sala macchine del SIA (Server Centrali)

Sono salvati con procedura automatica i DataBase Oracle e SQL utilizzati dalle diverse procedure, File server, documenti legati ad applicazioni (protocollo) e documenti memorizzati sulle aree riservate residenti sui dischi di rete ed assegnate

agli utente che ne hanno fatto richiesta. I dati sottoposti a salvataggio sono quelli residenti sui server aziendali, con la frequenza stabilita nel paragrafo 4.2. Le attuali policy di backup non prevedono salvataggi dei dati memorizzati sui dischi locali se non in casi straordinari. Si rammenta che la memorizzazione di dati aziendali sulle risorse locali è a rischio e pericolo dell'incaricato.

4.2 Effettuazione dei salvataggi

Il salvataggio dei dati utente (documenti, database) memorizzati sui server sono salvati su base giornaliera.
In particolare, la policy di salvataggio prevede un backup incrementale al giorno e un salvataggio completo una volta alla settimana.
I supporti utilizzati sono cartucce a nastro: la cartuccia viene riempita completamente (in media 5 salvataggi su un nastro) e poi conservata in un armadio. Vengono conservati gli ultimi 2 anni di backup.
I supporti non vengono ruotati, ma sostituiti con nuovi.
Il personale del SIA verifica quotidianamente attraverso i log generati dalla procedura di backup la corretta esecuzione dei salvataggi.

4.3 Conservazione dei supporti e dei log

I supporti di backup sono custoditi in armadi chiusi presso aree dislocate in altro padiglione rispetto la sala CED.
Le cassette da smaltire sono rese inservibili per evitare che persone non autorizzate possano comunque tentare di leggerne il contenuto.
I sistemi di backup utilizzati dal sistema informativo aziendale sono impostati in modo da gestire un file di log delle principali attività, tra cui l'avvio e l'arresto delle attività, gli errori rilevati e le date in cui si sono verificati.

4.4 Ripristino dei dati

I salvataggi delle base dati sono effettuati per disaster recovery. Non si può ripristinare la singola tabella. Per questo si usa un file di export giornaliero, sono mantenuti in linea i salvataggi degli ultimi 7 giorni.

In caso di perdita totale (incidente grave), si applica la procedura di disaster recovery. Per quanto riguarda i documenti e il file server non ci sono problemi, si può arrivare alla granularità desiderata.
Il ripristino dei dati viene eseguito su richiesta dell'utente attraverso comunicazione anche per via orale. I sistemi informativi valutano la richiesta ed eventualmente attivano il ripristino.
Le operazioni di ripristino vengono condotte in modo da salvaguardare i dati presenti sul sistema dei quali si richiede il ripristino con versioni precedenti. Il tutto per evitare che il ripristino danneggi altri dati. L'operazione viene ripetuta nel caso in cui i dati ripristinati non fossero coerenti con le aspettative dell'utente.

4.5 Dati contenuti su sistemi locali (client)

Sui sistemi locali non devono essere memorizzati dati sensibili.
Il back-up dei dati memorizzati nei singoli personal computer è a carico dell'utente.

Terze parti che eseguono operazioni di manutenzione, nei personal computer, agiscono esclusivamente come determinato dal proprietario dei dati, sulla base dei concetti di salvataggio.

Una copia di back-up deve essere effettuata dopo cambiamenti sostanziali dei dati, o prima di interventi di manutenzione, o aggiornamenti hardware e software.

5 RIFERIMENTI

Dlgs 196/2003 – Disciplinare Tecnico punti 18.

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

“PRO007”

Procedura per la gestione degli accessi logici

Documento riservato ai sistemi informativi

1.0	17/03/2006	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1. INTRODUZIONE.

1.1 Scopo

Lo scopo di questo documento è di definire una policy aziendale che regolamenti la gestione degli accessi alle diverse categorie di informazioni dell'Istituto.
Per poter gestire in modo adeguato l'accesso alle informazioni è necessario che l'owner della risorsa informativa che deve essere acceduta definisca i diritti di accesso in termini di profili di base e/o privilegi specifici.

2. CONTROLLO ACCESSI.

La regola della presente policy è:

"Tutto è proibito se non è espressamente permesso"

Discende dai punti di seguito riportati dalla politica della sicurezza:

1. i diritti di accesso alle informazioni ed alle risorse devono essere basati sui principi del:
    a. "need to know";
    b. "least privilege";
    c. "separation of duties";
2. tutti gli utenti devono essere identificati ed autenticati prima di poter accedere alle informazioni e/o ai sistemi.

2.1 Regole di accesso ai sistemi e alle applicazioni.

2.1.1 Sistemi di controllo accessi.

a. Deve essere installata sui sistemi un'infrastruttura hardware o software che consenta di rendere operative le specifiche di sicurezza in termini di controllo dell'accesso ai dati.

b. Il criterio di base su cui si fonda un sistema di controllo dell'accesso ai dati è l'affermazione generale sul diritto di accesso : l'accesso, a priori, non è libero, ma è accordato solo su basi specifiche a utenti, dati e scopi selezionati che dipendono dalle funzioni che l'utente è chiamato a svolgere.

c. I diritti di accesso riconosciuti su un sistema non devono permettere accessi non controllati su altri sistemi. Su ogni sistema i controlli devono essere specifici.

d. Il sistema di controllo accessi deve essere in grado di definire il diritto di accesso (privilegio), monitorare l'uso, rimuoverlo se necessario.

e. Come regola generale, se un sistema o mezzo di comunicazione coinvolto nel controllo viene meno per guasto o altro, il meccanismo di controllo deve collocarsi su un default di accesso vietato.

f. E' vietato modificare o manipolare il software di controllo accessi salvo che attraverso le exit ed i punti di personalizzazioni espressamente previsti all'origine. E' vietato altresì modificare le interfacce dei sottosistemi software con il software di controllo accessi, che devono interagire nella maniera nativa originariamente prevista.

g. E' richiesta la documentazione della implementazione dei sistemi di controllo accessi. Tale documentazione deve comprendere:

- le modalità implementate per stabilire coloro che possono accedere;
- i profili ed i privilegi specifici.

2.1.2 Profili di accesso.

La definizione fondamentale delle regole di accesso è fatta per mezzo di profili di base

Ogni profilo di accesso deve essere definito tenendo conto delle reali necessità di business.

I profili sono individuabili per categoria in base ad una serie di coordinate, ruolo, tipologia di utente, unità organizzativa di appartenenza, localizzazione geografica, appartenenza a progetti, responsabilità speciali.

Devono, inoltre, poi essere definite le tipologie utente. Per esempio:

- utenti ordinari,
- utenti di sviluppo,
- utenti di sistema,
- utenti di gestione,
- utenti di sicurezza,
- utenze di amministrazione dell'intero sistema/DB,
- utenti tecnici.

Particolare attenzione deve essere rivolta ai profili "amministratori" che devono essere strettamente controllati ed il loro numero mantenuto al minimo necessario. I loro diritti di accesso devono essere garantiti solo secondo una chiara e predefinita richiesta da parte del responsabile del sistema in oggetto.

2.1.3 Accesso Personale esterno.

Per quanto riguarda l'accesso di personale esterno i privilegi devono essere accordati di volta in volta su basi specifiche ed in funzione delle reali necessità dichiarate dal referente.

L'accesso di terze parti ai sistemi aziendali deve essere basato su un contratto. In esso si deve stabilire che il personale esterno è obbligato al rispetto delle norme e delle policy di sicurezza aziendali. Il contratto deve essere perfezionato prima che qualsiasi accesso possa essere consentito.

2.1.4 Gestione.

La registrazione delle richieste di accesso deve essere mantenuta come documentazione per un certo periodo di tempo conforme all'eventualità che possano essere necessarie indagini a riguardo.

E' indispensabile definire profili diversi tra chi amministra/ gestisce e tra chi è incaricato del controllo delle attività.

I privilegi di accesso del personale che lascia l'impiego devono essere immediatamente rimossi dal sistema.

3. CAMPO DI APPLICAZIONE.

La presente procedura si applica alla rete aziendale dell'Istituto.

4. RESPONSABILITÀ.

La responsabilità della corretta gestione dei sistemi di protezione dagli accessi logici non autorizzati è del SIA.

5. MODALITÀ ESECUTIVE.

I dati personali, sensibili e giudiziari e gli strumenti di elaborazione dati devono essere adeguatamente protetti dagli accessi logici non autorizzati.
Il sistema di protezione dagli accessi logici non autorizzati implementato in azienda è così composto:

- Sistema firewall primario (PIX): garantisce il controllo degli accessi alla rete aziendale dall'esterno bloccando tutti i tentativi di accesso. Consente l'uscita dei soli utenti provenienti da un proxy server. Esistono classi di utenze definite

che per motivi inerenti all'attività svolta non passano dal proxy (es utenze CElD), ma sono conosciute dal firewall a livello di indirizzo IP.

- Sistema firewall per la gestione degli accessi VPN: gestisce le connessioni in rete privata virtuale per gli utenti esterni che ne hanno necessità (manutentori software). I due firewall sono connessi a reti differenti.
- Gli utenti che hanno necessità di consultare la posta elettronica dall'esterno (medici, ricercatori, ecc.) vi accedono attraverso un server in DMZ, che riceve dal server di posta primario le repliche del database. Per garantire la sicurezza della rete è sempre il server di posta primario che gestisce gli aggiornamenti del database di posta.
- Per gestire alcuni accessi manutentivi di fornitori software è attiva una connessione RAS e una ISDN accessibile tramite modem e procedura di autenticazione.
- Gli utenti accedono ad internet attraverso un proxy server LINUX. Al momento non sono implementate policy di accesso particolari. Gli accessi avvengono previa autenticazione. Il proxy genera statistiche sui siti visitati, sulle ore di collegamento, ecc. a livello di IP macchina.
- Il server di posta elettronica possiede funzionalità di antispamming e antirelay.
- Non è previsto l'impiego di modem per la connessione a reti esterne dall'azienda

6. RIFERIMENTI.

Dlgs 196/2003 – Disciplinare Tecnico punto 20

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

“PRO008”

Procedura per la gestione dei supporti removibili

Documento a disposizione di tutto il personale

1.0	17/03/2006	Emissione		
2.0	01/03/2011	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1. Premessa

I supporti di memorizzazione devono essere gestiti con attenzione, in quanto rappresentano una possibile fonte di minaccia ai requisiti di riservatezza, disponibilità, integrità delle informazioni.
L'utilizzo dei supporti removibili è concesso solamente nei casi in cui, per inderogabili necessità, si debbano utilizzare dati off line (in mancanza della rete locale).
In ogni caso, non è consentito l'utilizzo di dati sensibili al di fuori dell'Istituto.
L'Istituto mette a disposizione degli incaricati al trattamento dei dati tecnologie di rete che garantiscono elevati standard di sicurezza per quanto riguarda la condivisione e l'interscambio di dati all'interno dell'Azienda. L'impiego di supporti di memorizzazione removibili per l'interscambio e la condivisione di dati deve essere limitato ai casi di reale necessità.

2. Scopo

Scopo di questo documento è quello di fornire le linee guida per la gestione sicura dei supporti di memorizzazione magnetici nel caso di loro utilizzo.

3. Area di applicazione

Il presente documento si applica a tutti supporti magnetici contenenti copie delle informazioni gestite. Rientrano quindi all'interno della categoria dei supporti oggetto di questo documenti dispositivi quali:

- nastri magnetici (DAT, DLT, ecc.);
- dischi magnetici fissi (come quelli presenti sulle stazioni di lavoro e sui server) e removibili (come i floppy disk);
- dispositivi personali di memorizzazione tascabili;
- CD ROM, CD R/W, DVD ed altri dispositivi a lettura laser;

Rientrano tra le informazioni che possono essere memorizzate su questi supporti, e che devono essere tutelate:

- dati applicativi;
- informazioni di configurazione dei sistemi, ovvero tutte le informazioni

necessarie a ripristinare le funzionalità di un sistema, esclusi i dati applicativi;
- software di base ed applicativo;
- documentazione.

4. Obiettivi

- Prevenire divulgazione non autorizzata, modifica, rimozione o distruzione di asset, e interruzioni di operatività.
- Tutte le apparecchiature contenenti supporti di memorizzazione, devono essere controllate per garantire che qualsiasi dato critico, o software con licenza, sia stato cancellato o sovrascritto in modo sicuro prima dell'eliminazione o del riutilizzo.

5. Politica di Gestione dei Supporti di Memorizzazione

Le norme contenute in questa Politica sono conformi ai seguenti principi generali:

1) devono esistere copie sufficienti delle informazioni ad assicurare la continuità dei servizi e la conservazione dei dati anche a fronte di eventi eccezionali;
2) **poiché ogni copia dell'informazione è fonte di potenziali minacce alla sicurezza (delle informazioni), devono essere prese misure per salvaguardare le informazioni da queste minacce;**
3) **tutte le operazioni di trattamento di dati personali devono essere conformi a quanto stabilito dalla legge.**

In particolare il punto 1 riguarda solo indirettamente la presente Politica, ed è riferibile principalmente al salvataggio e ripristino delle Informazioni (finalizzato alla continuità del business), per il quale si rimanda al prossimo paragrafo e, più dettagliatamente alla Procedura Operativa PRO010 (continuità dei servizi).

6. Supporti Magnetici

6.1 Salvataggio e Ripristino delle Informazioni

Guasti alle apparecchiature informatiche, errori accidentali ed attacchi deliberati possono comportare la perdita di dati importanti. Occorre, quindi, attivare delle misure per garantire la disponibilità e la continuità dei servizi, predisponendo copie di salvataggio che permettano di recuperare le informazioni che sono state danneggiate. Tali copie dovranno essere conservate su supporti di tipo opportuno in relazione al tipo di dati e di sistema, e registrate in base alla criticità delle informazioni e alla loro frequenza di aggiornamento. Per ogni tipo di salvataggio devono essere sviluppati e provati preventivamente dei metodi che consentano di ripristinare le informazioni salvate sui sistemi.

Il documento di riferimento per le modalità di salvataggio e ripristino sono le procedure PRO006 (gestione dei backup) e PRO010 (continuità dei servizi).

6.2 Etichettatura dei supporti

Tutti i supporti devono essere etichettati, al fine di consentirne il riconoscimento, la gestione e la classificazione, e in modo da evitare l'uso improprio delle informazioni in essi contenute. Nella etichetta devono essere evidenziati i riferimenti temporali, l'uso previsto dei supporti, l'origine delle informazioni ed il loro livello di classificazione; quest'ultimo dovrà essere attribuito da parte del proprietario delle informazioni e potrà essere variata solo dallo stesso.

I principi cui attenersi nella redazione delle etichette possono essere così riassunti:

- le etichette devono essere applicate, oltre che sui supporti, anche sulle loro copertine e/o contenitori;
- le etichette devono riportare la classificazione più elevata posta sulle informazioni contenute sul supporto al quale si riferiscono;
- se è determinato, ed è noto, un periodo oltre il quale delle informazioni variano il loro livello di classifica, bisogna che tale scadenza

venga riportata tra le informazioni che classificano questi dati;

- un insieme di informazioni variamente classificate può richiedere, nella sua interezza, una classificazione più elevata di quella delle sue parti; essa dovrà essere attribuita da chi aggrega le informazioni.

6.3 Custodia dei supporti (Clean Desk)

I supporti magnetici contenenti informazioni non devono essere lasciati liberamente accessibili sulle scrivanie o nei locali (*Clean Desk*). Essi devono sempre essere custoditi in archivi dotati delle funzioni necessarie a restringere l'accesso fisico solo alle persone autorizzate, ed a proteggere i supporti da alcune minacce ambientali.

Gli archivi per la conservazione dei supporti magnetici contenenti informazioni devono essere muniti di serratura. È accettabile in alternativa la conservazione in stanze nelle quali l'accesso sia controllato da operatori abilitati, e che, in assenza di tali operatori, siano chiuse a chiave.

Gli archivi devono essere ad accesso selezionato, in modo da poter consentire agli addetti l'accesso solo alle informazioni al trattamento delle quali questi siano autorizzati. In caso di difficoltà nella realizzazione di archivi ad accesso selezionato, contenenti una pluralità di informazioni, occorre realizzare più archivi, ciascuno per una specifica categoria di informazioni.

Gli archivi devono essere protetti da calore, umidità, polvere, campi elettromagnetici eccessivi e da qualunque agente che possa danneggiare i supporti in essi contenuti.

Al fine di rendere minime le probabilità di danneggiamento simultaneo delle informazioni sui sistemi e di quelle archiviate, gli archivi devono essere posti ad una distanza significativa dai sistemi ai quali si riferiscono, e comunque in una stanza diversa da quella che li ospita.

6.4 Norme di accesso agli archivi ed ai supporti

Le regole di accesso fisico agli archivi di lavoro dei supporti magnetici vengono definite dai gestori delle informazioni in esse contenute, in accordo con le procedure di sicurezza definite.

Si rammenta che l'accesso agli archivi ed ai supporti contenenti dati personali e/o sensibili deve essere consentito solo ai responsabili ed agli incaricati dei relativi trattamenti.

6.5 Accettazione di supporti dall'esterno

Allo stato attuale non è previsto l'utilizzo di supporti di provenienza esterna e già usati da altri. In ogni caso, per qualsiasi esigenza futura, sarà necessario adottare le seguenti misure di sicurezza:

- non usare sui sistemi dati e/o programmi contenuti in tali supporti senza prima averli verificati con opportuni programmi antivirus;
- non riusare supporti provenienti dall'esterno senza prima averne preventivamente cancellato i contenuti;
- non accettare software su supporti provenienti dall'esterno senza prima averne verificato la provenienza, ed accertato l'autenticità e l'integrità.

6.6 Riuso di supporti

I supporti magnetici non removibili (quali ad esempio i dischi rigidi di stazioni di lavoro o server) prima di essere assegnati ad altro uso, devono essere sottoposti a procedura di cancellazione sicura; questo ogni volta che ciò sia richiesto del proprietario dei dati su di essi trattati o dall'utente al quale il dispositivo è assegnato. È comunque obbligatorio eseguire la procedura ad ogni riassegnazione del dispositivo.

6.7 Eliminazione o esportazione di supporti

I supporti magnetici non riutilizzabili devono essere fisicamente distrutti.

La gestione dei supporti avviene in maniera tale da prevenire l'accesso non autorizzato ai dati e alle informazioni che essi contengono; oltre che copertine o contenitori, i supporti riportano la classificazione più elevata posta sulle informazioni che essi contengono; si ricorda infatti che un insieme di informazioni diversamente classificate può richiedere, nella sua interezza, una classificazione più elevata. I supporti, in generale, non dovrebbero essere portati all'esterno dell'area di utilizzo. Il trasferimento, sia all'interno che all'esterno, è senza alcun vincolo per quei supporti che contengono informazioni non classificate.

6.8 Procedura di cancellazione sicura

A causa della modalità con le quali operano, le normali procedure di cancellazione dei supporti magnetici non assicurano l'eliminazione di tutte le informazioni presenti su un supporto. I dati cancellati con gli usuali comandi

di cancellazione vengono infatti "marcati" come cancellati, ma restano fisicamente ancora sul supporto magnetico. Anche i comandi di inizializzazione e formattazione dei supporti non rimuovono fisicamente tutte le informazioni eventualmente già presenti, ma ne lasciano intatta una parte significativa.
È quindi necessario prendere speciali precauzioni nel cancellare le informazioni presenti su un supporto magnetico, predisponendo delle procedure di cancellazione sicura degli stessi. Con "cancellazione sicura" s'intende quel processo che rende impossibile, o comunque estremamente difficoltoso, il ripristino di informazioni dal supporto magnetico sul quale sono state memorizzate.

Uno dei metodi di cancellazione sicura utilizzabile prevede la sovrascrittura, con una sequenza predeterminata di caratteri, delle aree del supporto occupate dalle informazioni che si intendono cancellare. La sovrascrittura fisica di un file ne rende il recupero estremamente difficoltoso, anche se non impossibile ad un attaccante dotato delle conoscenze e della determinazione necessari. La difficoltà di tale recupero può essere ulteriormente accresciuta aumentando il numero delle sovrascritture utilizzate, ciascuna eseguita usando una diversa sequenza di caratteri, fino ad un massimo di 5-7 volte. Viene inoltre evidenziato che le informazioni originariamente contenute in un file possono venire disseminate, con l'uso, in vari punti del dispositivo che ospita tale file, in particolare in copie del file precedentemente cancellate o su files temporanei, contenuti in locazioni e con nomi diversi da quelli di partenza. Per cancellare in maniera sicura le informazioni presenti su un supporto magnetico è quindi necessario sottoporre a cancellazione non solo i files ancora presenti e contenenti le informazioni di interesse, ma l'intero dispositivo. Per ogni sistema deve quindi essere predisposta una utilità di cancellazione sicura.

In alternativa, qualora non sia possibile eseguire la cancellazione sicura dei dati laddove previsto (ad esempio, nel caso di dispositivi non riscrivibili), o ove si desideri avere la garanzia totale della impossibilità di lettura dei dati precedentemente registrati, il supporto magnetico deve essere fisicamente distrutto.

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

"PRO 009"

Procedura per la gestione dei documenti cartacei

Documento a disposizione di tutto il personale

1.0	17/03/2006	Emissione		
2.0	01/03/2010	Revisione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 SCOPO

Lo scopo della presente procedura è quello di gestire la corretta conservazione e l'accesso dei documenti cartacei contenenti dati personali, sensibili e giudiziari, in accordo con quanto disposto ex Dlgs 30 giugno 2003, n. 196 Tecnico (punti 27, 28, 29) per prevenire possibili furti, danni e divulgazione non autorizzata.

2 CAMPO DI APPLICAZIONE

La procedura si applica a tutto il personale dell'Istituto incaricato del trattamento dei dati personali.

3 RESPONSABILITÀ

Il Responsabile dei trattamenti è responsabile degli archivi cartacei di tipo storico, cioè relativi ad almeno 5 anni prima.
Tutti gli incaricati al trattamento dei dati personali sono tenuti ad osservare quanto specificato nella presente procedura, ed a segnalare tutte le violazioni alle disposizioni specificate al Responsabile dei trattamenti. Gli incaricati ai trattamenti sono altresì responsabili dei dati in forma cartacea di uso corrente, ovvero che si riferiscono all'anno in corso e all'anno precedente.

4 MODALITÀ ESECUTIVE

Per quanto riguarda la gestione della documentazione di uso individuale o comunque di propria diretta pertinenza, si rimanda a quanto previsto dalla procedura PRO004 – Procedura per la gestione del posto di lavoro e degli accessi agli uffici.
Gli archivi possono essere suddivisi in due categorie:

- Archivi di dati "correnti": contengono relativi all'anno in corso e all'anno precedente.
- Archivi di dati "storici": contengono i dati relativi a periodi precedenti.

Gli archivi correnti sono conservati negli uffici sotto la responsabilità degli incaricati.
I documenti relativi al personale (sia di tipo corrente che storico), sono conservati in armadi chiusi direttamente nell'Ufficio Personale.

Una volta l'anno, o comunque quando se ne presenti la necessità, i dati meno recenti contenuti negli archivi correnti vengono trasferiti negli archivi storici. Gli archivi storici sono aree ad accesso controllato (chiuse a chiave).

4.1 Accesso agli archivi

L'accesso ai dati degli archivi storici avviene su richiesta fatta al responsabile dell'archivio di competenza. Non sono consentiti accessi autonomi ai dati archiviati.

5 RIFERIMENTI

Disciplinare Tecnico punti 28 e 29
PRO004 - Procedura per la gestione del posto di lavoro e degli accessi agi uffici

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

"PRO010"

Procedura per la continuità dei servizi

Documento a disposizione di tutto il personale

1.0	17/03/2006	Emissione		
4.0	14/12/2015	Revisione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 SCOPO

Lo scopo della presente procedura è quello di garantire l'accesso ai dati personali in caso di distruzione, danneggiamento o malfunzionamento dei sistemi in tempi certi e comunque non superiori al limite stabilito dal Disciplinare Tecnico (punto 23).

2 CAMPO DI APPLICAZIONE

La procedura si applica a tutto il personale ed ai collaboratori dell'Istituto incaricati del trattamento dei dati personali per quanto riguarda i comportamenti da tenere, e al personale tecnico per l'individuazione e l'implementazione delle misure tecniche.

3 RESPONSABILITA'

Il Referente per i sistemi informativi ha la responsabilità di verificare, mantenere aggiornato e revisionare il piano per la continuità del servizio, in collaborazione con i responsabili dei trattamenti e di adottare le misure tecniche ritenute idonee al mantenimento della continuità del servizio.
Il personale tecnico ha la responsabilità di implementare le misure tecniche decise e di mantenere efficienti le infrastrutture tecnologiche.
Gli incaricati hanno la responsabilità di attenersi alle istruzioni operative che li riguardano e di segnalare le interruzioni di servizio e le situazioni potenzialmente pericolose al Referente per i sistemi informativi.

4 MODALITA' ESECUTIVE

Qualsiasi evento causato da fenomeni naturali o da azioni deliberate (incendi, allagamenti, ecc.) che metta a repentaglio la vitalità dell'Azienda o la vita umana del personale, è gestito dal Piano di emergenza ed evacuazione, a norma del Decreto Legislativo 626/94.
Qualsiasi evento che metta a repentaglio l'intergità e la disponibilità dei dati personali (malfunzionamenti hardware, incidenti di sicurezza, ecc.) comporta l'immediata applicazione della procedura di continuità per il servizio interessato dall'interruzione.

Premesso che l'Istituto si impegna a mettere a disposizione le risorse necessarie in termini di mezzi e persone e a lavorare in modo continuativo per ripristinare per quanto possibile tutti i sistemi di gestione dei dati personali a fronte di guasto bloccante, le misure ritenute idonee dall'Azienda al fine di garantire la continuità del servizio possono essere ricondotte ai seguenti aspetti:

- **Alimentazione elettrica**: in sala macchine sono attive unità UPS che garantiscono la continuità per il tempo necessario alla partenza dei generatori di corrente. I gruppi di continuità hanno anche la funzione di stabilizzare la corrente per eliminare i rischi derivanti dalle sovratensioni. I servizi ritenuti critici sono alimentati in caso di interruzione della rete elettrica da generatori diesel. Tutto l'impianto elettrico è segmentato per aree di servizio con interruttori differenziali autonomi.
- **Backup**: sono stati implementati sistemi di backup al fine di garantire il corretto ripristino dell'accesso ai dati in caso di malfunzionamenti o perdite accidentali. La descrizione dei sistemi per il salvataggio periodico dei dati è contenuta nella procedura PRO006 – Procedura per la gestione dei backup.
- **Centrale telefonica**: la centrale è protetta e alimentata da un gruppo di continuità dedicato che stabilizza la corrente e garantisce alcune ore di autonomia.
- **Server**: il database server Oracle è ospitato su una piattaforma hardware cluster composta da due nodi in configurazione attiva/attiva. In caso di caduta di uno dei due nodi i servizi afferenti al nodo in fault vengono migrati automaticamente sull'altro. L'interruzione dei servizi è quantificabile in circa 60 secondi. Ad ulteriore protezione i dischi fissi sono in tecnologia RAID 5. L'accessibilità alla rete su ogni nodo è garantita da una doppia scheda Ethernet. Tutti i rimanenti server aziendali dispongono in varia misura di parti ridondate (alimentatori, ventole, dischi fissi con tecnologia RAID).
- **Apparati di rete e cablaggio**: Gli apparati di rete sono alimentati da gruppi di continuità nell'area CED. Il centro stella dispone di alimentazione ridondata.
- **Contratti di assistenza tecnica**: Il database server dispone di un contratto di assistenza che garantisce la presa in carico del problema entro il successivo giorno lavorativo. Gli altri server e i client sono coperti da garanzia di 3 anni on site. A questo proposito si veda anche quanto descritto nella procedura PRO012 – Procedura per la gestione dei criteri di sicurezza nei contratti.
- **Casseforti e armadi ignifughi**: al fine di garantire la corretta conservazione di supporti elettronici è presente in sala macchine un armadio ignifugo.

- **Sistemi antincendio**: L'Istituto dispone dei sistemi antincendio previsti dalle normative vigenti. All'interno dell'Istituto è attivo un servizio antincendio di pronto intervento gestito da una società esterna.
- **Sistemi antiintrusione**: L'Azienda dispone di impianto di allarme con sensori di movimento collegato con la vigilanza;

  Si faccia riferimento inoltre a quanto specificato nella procedura PRO001 – Procedura per la gestione degli accessi fisici.
- **Protezione dei documenti in formato cartaceo**: Si veda quanto previsto dalla procedura PRO009 – Procedura per la conservazione e gestione dei documenti cartacei.
- **Postazioni di lavoro**: Le postazioni di lavoro che utilizzano software distribuiti possono essere intercambiabili, garantendo la possibilità di spostare servizi e/o uffici in altri locali.
- **SIA (Servizio Informatico Aziendale)**: Il servizio si occupa del mantenimento in efficienza del sistema informatico aziendale, del monitoraggio della qualità dei servizi erogati, della risoluzione dei fault o di escalation verso terzi, del controllo e monitoraggio dei tempi di risoluzione in caso di escalation verso terzi.

In tutti i casi in cui risultino danneggiati o comunque inagibili o inutilizzabili i sistemi e le strutture aziendali, le figure di riferimento da contattare per le opportune misure di emergenza e ripristino sono il Referente per i Sistemi Informativi per la parte informatica e i responsabili dei servizi dell'Ufficio Tecnico per le parti di loro competenza.

5 RIFERIMENTI

Dlgs 196/2003 – Disciplinare Tecnico punti 19.5 e 23
PRO001 – Procedura per la gestione degli accessi fisici.
PRO006 – Procedura per la gestione dei backup.
PRO009 – Procedura per la conservazione e gestione dei documenti cartacei.
PRO012 – Procedura per la gestione dei criteri di sicurezza nei contratti.

Istituto Giannina Gaslini – Ospedale Pediatrico IRCCS

“PRO011”

Procedura per la gestione dei requisiti di sicurezza nei contratti

Documento a disposizione di tutto il personale

4.0	14/12/2015	Emissione		
Rev.	**Data**	**Causale**	**Verifica**	**Approvazione**

INDICE

1 Introduzione

Il presente documento ha lo scopo di definire le politiche relative alla gestione dei rapporti con terze parti che l'Istituto intende applicare al proprio interno, sulla base delle prescrizioni di legge, degli impegni contrattuali, al fine di proteggere il proprio patrimonio informativo.

1.1 Obiettivi

Garantire la sicurezza delle informazioni e degli apparati di elaborazione dell'organizzazione che sono acceduti, elaborati, comunicati a, o gestiti da, terze parti.

Implementare e mantenere un adeguato livello di sicurezza delle informazioni ed un livello di servizio in linea con gli accordi stipulati con le terze parti.

2 Norme generali

Accanto alle norme comportamentali per ogni singola componente organizzativa coinvolta, nelle indicazioni di seguito elencate, si pone particolare attenzione a quegli aspetti dell'attività lavorativa che prevedano il coinvolgimento nell'accesso, utilizzo e gestione di informazioni ad opera di terze parti; soprattutto quando questo coinvolgimento può impattare sulla loro sicurezza.

3 Gestione del personale interno e di terze parti

3.1 Selezione

Durante la selezione del personale se una risorsa è destinata a ricoprire incarichi critici dal punto di vista della sicurezza devono essere previsti approfondimenti che prevedano oltre alle competenze specifiche per il ruolo da ricoprire anche le attinenze del candidato.

I dipendenti che ricoprono incarichi critici e/o che hanno necessità di accedere ad applicazioni critiche devono rispettare gli accordi di riservatezza e non divulgazione previsti dal contratto CCNL(Contratto Collettivo Nazionale di Lavoro) e dal Codice Etico.

Deve essere prevista la nomina della risorsa quale incaricato al trattamento dei dati ai fini del D.Lgs. 196/03, inoltre devono essere fornite le istruzioni relative al trattamento dei dati.
La presenza di terze parti che prestano la loro opera all'interno dell'Istituto o all'esterno, ma su dati aziendali, seppure per un periodo definito, può dare origine a vulnerabilità nel sistema di sicurezza.
Deve quindi applicarsi un adeguato livello di controllo anche al personale non dipendente e temporaneo: a tal fine devono essere esplicitate nei contratti le responsabilità in materia di sicurezza.
La Società terza si impegna a far rispettare l'obbligo della riservatezza a tutti i propri dipendenti, consulenti e collaboratori che, per ragioni d'ufficio, dovessero venire a conoscenza delle informazioni riservate; in particolare:

- devono essere definite le responsabilità circa gli aspetti sicurezza;
- devono essere specificati gli obblighi di conformità alle norme di sicurezza;
- devono essere specificati gli obblighi di conformità con i copyright;
- devono essere fornite linee guida sulle responsabilità nel trattamento d'informazioni riservate e nella custodia dei beni assegnati.

Va prevista in fase di stipula del contratto la firma di appositi accordi di riservatezza e di non divulgazione di dati ed informazioni (NDA - Non Disclosure Agreement) che prevedano eventuali penali laddove sia accertata la violazione dell'accordo.

3.2 Sensibilizzazione sui temi di Sicurezza

Tutto il personale deve essere informato e istruito sugli aspetti di sicurezza attraverso la diffusione di un preciso e definito programma di sensibilizzazione.

3.3 Contatti con gruppi di particolare interesse

Devono essere individuati specialisti, esterni o interni, focalizzati sulla sicurezza delle informazioni. La qualità della loro valutazione del rischio e la consulenza sui controlli determina l'efficacia della sicurezza dell'informazione.

3.4 Obblighi di conformità con i copyright

L'Istituto deve costantemente allineare i propri processi di software management alle norme di legge che tutelano il diritto di proprietà intellettuale.
E' necessario quindi:

- informare il personale sulle norme che regolano il copyright e rendere note le azioni
  disciplinari previste dal CCNL per il personale dipendente da imprese esercenti servizi di telecomunicazione, in caso di loro violazione;
- definire una politica di conformità con il copyright del software;
- conservare le prove della titolarità della licenza, dei dischi master e dei manuali;
- controllare che non sia superato il numero massimo di utenti abilitati dalla licenza.

3.5 Contatti con le autorità

L'Istituto mantiene le normali relazioni con le Autorità Giudiziarie, sindacali, della sicurezza sul lavoro.

4 Enti esterni

4.1 Identificazione dei rischi connessi ad enti esterni

L'Istituto ha adottato tutte le opportune misure di gestione dei servizi esterni in termini di:

- categorizzare e valutare i rischi dei fornitori e dei contratti;
- valutare e selezionare i fornitori e contratti;
- sviluppare, negoziare e concordare i contratti;
- riesame, rinnovo e cessazione del contratto;
- gestione dei fornitori e fornitore di prestazioni;
- concordare e implementazione di piani di miglioramento dei servizi e dei fornitori;
- mantenimento di contratti, termini e condizioni standard;
- gestione della risoluzione delle controversie contrattuali;
- gestione dei fornitori contrattualizzati.

4.2 Gestione dell'erogazione dei servizi di terze parti

La gestione dei fornitori e i relativi servizi, strumenti, soluzioni che forniscono è monitorata al fine di tenere allineati i servizi ricevuti con le esigenze di business e con i servizi contrattualizzati, al fini di:

- Ottenere il valore pagato dal fornitore e i contratti;
- Assicurare che i contratti e gli accordi con i fornitori siano allineati alle necessità del business e supportino e siano allineati con i target concordati nei SLR e SLA.

Devono essere previste apposite clausole riguardanti gli aspetti di sicurezza nei contratti con terze parti che prevedono accessi alle componenti IT, in particolare, devono essere inclusi nel contratto:

- la politica generale di sicurezza dell'informazione;
- la protezione dei beni, in termini di procedure, controlli e restrizioni;
- una descrizione di ciascun servizio reso accessibile;
- il livello concordato del servizio;
- le rispettive responsabilità contrattuali delle parti;
- le responsabilità rispetto alle materie legali, per es. alla normativa per la protezione dei dati alle cessioni di copyright e alla tutela di qualsiasi collaborazione lavorativa;
- accordi sul controllo di accesso, che riguardino:
    - metodi per consentire l'accesso, e il controllo e l'uso di identificatori, come documenti di identificazione degli utenti e password;
    - il processo di autorizzazione per l'accesso;
    - una lista di soggetti autorizzati all'uso dei servizi resi disponibili, e dei loro diritti e prerogative rispetto a tale uso;
    - la definizione di criteri per verificare l'adempimento, il loro controllo e registrazione;
    - il diritto di controllare e revocare l'attività degli utenti;
    - il diritto di verificare eventuali responsabilità contrattuali o di affidare tali ispezioni a terzi;
    - la fissazione di un processo per la soluzione di problemi;

- le responsabilità relative all'installazione e la manutenzione di hardware e software;
- una chiara struttura di reportistica;
- un processo chiaro e dettagliato di cambi nel management;
- qualsiasi controllo richiesto di protezione fisica e meccanismi per assicurare che questi controlli siano rispettati;
- formazione degli utenti e degli amministratori su metodi, procedure e sicurezza;
- controlli per assicurare protezione contro software malevoli.

Si deve controllare che le terze parti implementino e mantengano i controlli di sicurezza ed i livelli di servizio inclusi negli accordi.
Servizi, report e documenti forniti da terze parti devono essere monitorati, controllati e sottoposti ad audit regolarmente.
Devono essere gestiti i cambiamenti nei servizi offerti da terze parti, inclusi mantenimento e miglioramento delle politiche di sicurezza delle informazioni, procedure e controlli, tenendo conto della criticità dei sistemi e dei processi coinvolti.

5 Riferimenti

Decreto Legislativo 196/2003.
PRO001 – Accessi Fisici