REGIONE TOSCANA

AZIENDA OSPEDALIERO-UNIVERSITARIA CAREGGI
Sede Legale Largo Brambilla n. 3 – 50134 Firenze

DELIBERAZIONE DEL DIRETTORE GENERALE

Numero della Deliberazione	766
Data della Deliberazione	15-11-2024
Oggetto della Deliberazione	Protocollo di intesa per la prevenzione e il contrasto dei crimini informatici sui sistemi informativi critici dell'AOU Careggi

Struttura Proponente	AFFARI GENERALI
Direttore della Struttura	MASOTTI ENRICO
Responsabile del procedimento	LUZZI LINDA

Immediata Esecutività	SI

Il DIRETTORE UO AFFARI GENERALI

Visti:

- il Decreto Legislativo 30 dicembre 1992 n. 502 "*Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421*"

- la Legge 7 agosto 1990, n. 241 *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"* ed in particolare l'art. 1, comma 1-bis, laddove stabilisce che la pubblica amministrazione, nell'adozione di atti di natura non autoritativa, agisce secondo le norme di diritto privato salvo che la legge disponga diversamente

- l'art. 15 della stessa Legge in cui si offre la possibilità alle amministrazioni pubbliche di concludere tra di loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune;

- il Decreto legislativo 31 marzo 2023, n. 36 "*Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici"* laddove si stabilisce che le disposizioni del codice non si applicano ai contratti esclusi, ai contratti attivi e ai contratti a titolo gratuito, anche qualora essi offrano opportunità di guadagno economico, anche indiretto;

- l'art. 7, comma 4 del medesimo Codice che, recependo il principio di auto organizzazione amministrativa, sancito nell'art. 2 della direttiva 2014/23/UE, stabilisce che le disposizioni del Codice non trovano applicazione agli accordi conclusi tra due o più amministrazioni pubbliche quando le finalità di collaborazione perseguono l'interesse pubblico, ovvero il miglioramento dei servizi pubblici che esse sono tenute a svolgere e non svolgono tali servizi sul mercato aperto;

Dato atto che:

- la legge 31 luglio 1997, n. 249, ha istituito l'Autorità per le garanzie nelle comunicazioni dettando norme sui sistemi delle telecomunicazioni e radiotelevisivo;
- con decreto del Ministro dell'Interno in data 19 gennaio 1999 è stato individuato il Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni;
- l'articolo 39 della legge 16 gennaio 2003, n. 3, recante: *"Disposizioni ordinamentali in materia di pubblica amministrazione*" prevede che il Dipartimento della Pubblica Sicurezza, può stipulare convenzioni con soggetti, pubblici e privati, dirette a fornire servizi specialistici finalizzati ad incrementare la sicurezza pubblica;
- il Decreto Legge 27 luglio 2005 n. 144, recante "*Misure urgenti per il contrasto del terrorismo internazionale*" dispone che con decreto del Ministro dell'Interno sono individuate le infrastrutture critiche informatizzate di interesse nazionale, alla cui protezione informatica provvede l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;
- con il D. Lgs. 18 maggio 2018 n. 51, recante "*Attuazione della Direttiva UE 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016*" sono state ridefinite le regole riguardanti il trattamento dei dati personali effettuato per "finalità di polizia", ovvero direttamente collegate all'attività di prevenzione e repressione dei reati e di tutela dell'ordine e della sicurezza pubblica;
- con decreto del Capo della Polizia del 28 giugno 2022, è stata attuata la complessiva revisione dell'assetto ordinativo delle articolazioni periferiche dell'Amministrazione della Pubblica Sicurezza e, in

particolare, dei Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) quale nuova denominazione dei Compartimenti di Polizia Postale e delle Comunicazioni, al cui interno sono stati istituiti i Nuclei Operativi Sicurezza Cibernetica (N.O.S.C.);

- con il Decreto del 7 febbraio 2024 del Ministro dell'Interno è stata istituita la Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, tra le cui articolazioni è incardinato il Servizio Polizia Postale e per la Sicurezza Cibernetica;

- il Centro Operativo Sicurezza Cibernetica - Polizia Postale e per la Sicurezza Cibernetica per la Toscana provvede, come organo periferico del Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza, ad assicurare i Servizi della Polizia Postale e per la Sicurezza Cibernetica, con particolare riferimento alla prevenzione e repressione dei reati;

Considerato che i sistemi informatici e le reti telematiche di supporto alle funzioni istituzionali dell'Azienda Ospedaliero Universitaria Careggi sono da ritenere infrastrutture sensibili di interesse pubblico e che, pertanto, risulta necessario prevenire e contrastare ogni forma di accesso illecito, anche tentato, finalizzato:

a) all'interruzione dei servizi di pubblica utilità;
b) all'indebita sottrazione di informazioni;
c) a realizzare qualsiasi ulteriore attività illecita;

Vista l'allegata bozza di Protocollo di Intesa in materia di sicurezza informatica con la quale si intende instaurare una stretta cooperazione tra il Centro Operativo Sicurezza Cibernetica - Polizia Postale e per la Sicurezza Cibernetica per la Toscana e l'Azienda Ospedaliero Universitaria Careggi, volta alla prevenzione e alla repressione dei crimini informatici (allegato A).

Dato atto che a conclusione di specifici incontri tra i rappresentanti del Centro Operativo Sicurezza Cibernetica e dell'Azienda Ospedaliero Universitaria Careggi è stato concordato di elaborare, in parallelo alla conclusione del suddetto Protocollo di intesa, un documento con il modello operativo di collaborazione per la prevenzione ed il contrasto dei crimini informatici riguardanti i sistemi ed i servizi "critici" dell'Azienda (documento non soggetto a pubblicazione per motivi di sicurezza e riservatezza delle informazioni);

Dato altresì atto che:

- la gestione dei sistemi e servizi informatici e delle infrastrutture tecnologiche dell'Azienda Ospedaliero Universitaria Careggi prevede, per la fase più propriamente operativa, il prevalente coinvolgimento di ESTAR – Ente di Supporto Tecnico Amministrativo Regionale – che ha tra i propri compiti istituzionali in ambito ICT anche quelli di governare l'operatività quotidiana dei sistemi informativi, delle reti e dei data center delle Aziende del Servizio Sanitario Regionale;

- con la sottoscrizione del Protocollo di intesa, l'Azienda si impegna a garantire il necessario collegamento collaborativo con le competenti strutture di ESTAR.

Vista la Legge Regionale 24 febbraio 2005, n. 40 "*Disciplina del Servizio Sanitario Regionale*";

Preso atto del vigente Statuto dell'AOU Careggi adottato con provvedimento del Direttore Generale n° 690/2024

Preso atto che il responsabile del procedimento ai sensi della legge 7 agosto 1990 n. 241, art. 6, è la Dott.ssa Linda Luzzi afferente alla U.O. Affari Generali;

Attestata la legittimità e la regolarità formale e sostanziale della presente proposta;

PROPONE AL DIRETTORE GENERALE

per quanto espresso in premessa che qui si intende integralmente riportato:

1. di approvare l'allegato testo di Protocollo di intesa da sottoscrivere con il Centro Operativo per la Sicurezza Cibernetica – Polizia Postale e Sicurezza Cibernetica della Toscana - avente ad oggetto "*Protocollo di intesa per la prevenzione e il contrasto dei crimini informatici sui sistemi informativi critici dipendenti dall'AOU Careggi*" (allegato A).
2. di dare atto che dalla sottoscrizione del Protocollo di intesa non derivano costi per l'Azienda;
3. di dichiarare la presente delibera immediatamente esecutiva ai sensi dell'art. 42 comma 4 della legge regionale toscana n. 40 del 2005 per la necessità di attivare con urgenza le procedure operative concordate tra le parti ai fini di prevenzione e contrasto dei crimini informatici sui sistemi informativi critici dell'AOU Careggi;
4. di inviare il presente provvedimento al Collegio Sindacale di questa Azienda, ai sensi dell'art. 42, comma 2 della legge della Regione Toscana n. 40 del 2005;

Il Direttore UOC Affari Generali

dott. Enrico Masotti

firma acquisita digitalmente

IL DIRETTORE GENERALE

Visto il Decreto del Presidente della Giunta Regionale Toscana n. 61 del 7 aprile 2023 con cui è stata nominata la dr.ssa Daniela Matarrese Direttore Generale dell'Azienda Ospedaliera-Universitaria-Careggi;

Letta e Valutata la sopra esposta proposta di deliberazione presentata dal Direttore della U.O.C. Affari Generali avente ad oggetto "*Protocollo di intesa per la prevenzione e il contrasto dei crimini informatici sui sistemi informativi critici dipendenti dall'AOU Careggi*";

Preso Atto dell'attestazione della legittimità, nonché della regolarità formale e sostanziale, espressa dal Dirigente che propone il presente atto;

Visto il parere favorevole del Direttore Amministrativo e del Direttore Sanitario;

Il Direttore Amministrativo Dr. Dario Rosini

Il Direttore Sanitario Dr.ssa Elvira Bianco

firme acquisite digitalmente

DELIBERA

per quanto sopra premesso, da intendersi qui integralmente trascritto e riportato:

1. di approvare l'allegato testo di Protocollo di intesa da sottoscrivere con il Centro Operativo per la Sicurezza Cibernetica – Polizia Postale e Sicurezza Cibernetica della Toscana - avente ad oggetto "*Protocollo di intesa per la prevenzione e il contrasto dei crimini informatici sui sistemi informativi critici dipendenti dall'AOU Careggi*" (allegato A);

2. di dare atto che dalla sottoscrizione del Protocollo di intesa non derivano costi per l'Azienda;
3. di dichiarare la presente delibera immediatamente esecutiva ai sensi dell'art. 42 comma 4 della legge regionale toscana n. 40 del 2005 per la necessità di attivare con urgenza le procedure operative concordate tra le parti ai fini di prevenzione e contrasto dei crimini informatici sui sistemi informativi critici dell'AOU Careggi;
4. di incaricare la UOC Affari Generali:
    - di provvedere alla pubblicazione all'Albo on line, ai sensi della legge 18 giugno 2009 n. 69, art. 32 comma 1, consultabile sul sito web istituzionale;
    - di trasmettere il presente atto al Collegio Sindacale entro il termine di cui alla legge regionale 24 febbraio 2005, n. 40, art. 42, comma 2.

Il Direttore Generale
Dr.ssa Daniela Matarrese

firma acquisita digitalmente

PROTOCOLLO D'INTESA
PER LA PREVENZIONE E CONTRASTO DEI CRIMINI INFORMATICI SUI SISTEMI INFORMATIVI "CRITICI" DIPENDENTI DA AZIENDA OSPEDALIERO UNIVERSITARIA CAREGGI

Il Centro Operativo per la Sicurezza Cibernetica - Polizia postale e per la Sicurezza Cibernetica per Toscana, d'ora innanzi C.O.S.C. "Toscana", con sede a Firenze, in Via della Casella n. 19, rappresentato dal Dirigente Dr.ssa Lorena LA SPINA, in qualità di responsabile del coordinamento e del controllo delle attività e dei servizi della Polizia Postale per la Sicurezza Cibernetica, nel proprio ambito territoriale

e

L'Azienda Ospedaliero Universitaria Careggi, con sede in Firenze, Largo Brambilla n. 3 (C.F. 04612750481), rappresentata, ai fini della sottoscrizione del presente atto, dal Direttore Generale, dr.ssa Daniela MATARRESE

d'ora innanzi, congiuntamente, le "Parti".

PREMESSO

- che la legge 31 luglio 1997, n. 249, ha istituito l'Autorità per le garanzie nelle comunicazioni dettando norme sui sistemi delle telecomunicazioni e radiotelevisivo;
- che, in relazione all'art. 1, commi 13 e 15 della citata legge, con decreto del Ministro dell'Interno, adottato di concerto con il Ministro delle Comunicazioni e con il Ministro del Tesoro, del Bilancio e della Programmazione Economica, in data 19 gennaio 1999, è stato individuato il Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza quale organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni;
- che l'articolo 39 della legge 16 gennaio 2003, n. 3, recante: *"Disposizioni ordinamentali in materia di pubblica amministrazione*" prevede che il Dipartimento della Pubblica Sicurezza, nell'ambito delle direttive impartite dal Ministro dell'Interno per il potenziamento dell'attività di prevenzione, può stipulare convenzioni con soggetti, pubblici e privati, dirette a fornire, con la contribuzione degli stessi soggetti, servizi specialistici, finalizzati ad incrementare la sicurezza pubblica;
- che il decreto legge 27 luglio 2005 n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005 n. 155, recante "*Misure urgenti per il contrasto del terrorismo internazionale*" e in particolare, l'art. 7 bis, comma 1, dispone che con decreto del

Ministro dell'Interno sono individuate le infrastrutture critiche informatizzate di interesse nazionale, alla cui protezione informatica provvede l'organo del Ministero dell'Interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;

- che il D.P.C.M. del 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, definisce all'art.1 l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali;
- che il D.P.C.M. del 27 gennaio 2014 ha adottato il "Quadro Strategico Nazionale per la Sicurezza Nazionale dello Spazio Cibernetico" e con DPCM 31/03/2017 è stato ridefinito il "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica";
- che con il D.Lgs. 18 maggio 2018 n. 51, recante "*Attuazione della Direttiva UE 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016*" sono state ridefinite le regole riguardanti il trattamento dei dati personali effettuato per "finalità di polizia", ovvero direttamente collegate all'attività di prevenzione e repressione dei reati e di tutela dell'ordine e della sicurezza pubblica;
- che con il Decreto 19 settembre 2017, n. 215 del Ministero dell'Interno, di concerto con i Ministri dello Sviluppo Economico e dell'Economia e delle Finanze, è stato adottato il "*Regolamento recante individuazione delle denominazioni, degli stemmi, degli emblemi e degli altri segni distintivi in uso esclusivo alla Polizia di Stato e al Corpo nazionale dei vigili del fuoco, nonché le modalità attuative ai fini della loro concessione in uso temporaneo a terzi*";
- che la Direttiva del Ministro dell'Interno del 15 agosto 2017 "sui comparti delle Specialità e sulla razionalizzazione dei Presidi di Polizia" ha ribadito, al punto 1.4, la competenza della Polizia Postale e delle Comunicazioni in materia di protezione delle infrastrutture critiche, nonché di sicurezza e regolarità dei servizi di telecomunicazione;
- che nell'ambito della direttiva generale per l'attività amministrativa e per la gestione relativa all'anno 2024, il Ministro dell'Interno, in ordine agli obiettivi operativi, nel ribadire l'esigenza di ampliare la sfera di tutela del C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) per le infrastrutture critiche informatizzate e delle infrastrutture sensibili presenti sul territorio (piccole e medie imprese – pubbliche amministrazioni locali) da realizzarsi tramite l'incremento di accordi bilaterali tra l'amministrazione e gli enti gestori dei sistemi informatici strategici, ha altresì previsto il rafforzamento -

attraverso le risorse del PNRR – delle difese cibernetiche, aumentando il grado di resilienza informatica dell'amministrazione attraverso la creazione di 8 sezioni operative per la sicurezza cibernetica distrettuali, di laboratori operativi dotati delle infrastrutture per le attività forensi (CLABS) e il potenziamento della sala server, al fine di prevedere o rilevare tempestivamente attacchi e incidenti informatici;

- che, con decreto del Capo della Polizia del 28 giugno 2022, è stata attuata la complessiva revisione dell'assetto ordinativo delle articolazioni periferiche dell'Amministrazione della Pubblica Sicurezza e, in particolare, dei Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) quale nuova denominazione dei Compartimenti di Polizia Postale e delle Comunicazioni, al cui interno sono stati istituiti i Nuclei Operativi Sicurezza Cibernetica (N.O.S.C.);
- che con il D.Lgs. 18 maggio 2018 n. 65 è stata recepita la Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, recante "*misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*" (c.d. Direttiva NIS), che individua quale Autorità di contrasto il Servizio Polizia Postale e delle Comunicazioni in qualità di organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n.155, così come individuato dal Decreto Interministeriale del 10 gennaio 1999;
- che con il Decreto del 7 febbraio 2024 del Ministro dell'Interno, di concerto con il Ministro dell'Economia e delle Finanze, è stata istituita la Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, tra le cui articolazioni è incardinato il Servizio Polizia Postale e per la Sicurezza Cibernetica;
- che il Centro Operativo Sicurezza Cibernetica - Polizia Postale e per la Sicurezza Cibernetica per la "Toscana" provvede, come organo periferico del Servizio Polizia Postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza, ad assicurare i Servizi della Polizia Postale e per la Sicurezza Cibernetica, con particolare riferimento alla prevenzione e repressione dei reati commessi avvalendosi delle specifiche potenzialità tecniche dei servizi o mezzi di comunicazione, anche ad alta tecnologia, ovvero alterando il normale funzionamento degli stessi;
- che i sistemi informatici e le reti telematiche di supporto alle funzioni istituzionali dell'Azienda Ospedaliero Universitaria Careggi sono da considerare infrastrutture sensibili di interesse pubblico. Risulta, pertanto, necessario prevenire e contrastare ogni forma di accesso illecito, anche tentato, finalizzato:

a) all'interruzione dei servizi di pubblica utilità;

b) all'indebita sottrazione di informazioni;

c) a porre in essere qualsiasi ulteriore attività illecita;

- che a conclusione di specifici incontri tra i rappresentanti del Centro Operativo Sicurezza Cibernetica e dell'Azienda Ospedaliero Universitaria Careggi e le sue strutture tecniche (Area innovazione e controllo), sarà elaborato un modello operativo di collaborazione per la prevenzione ed il contrasto dei crimini informatici che hanno per oggetto, nella loro complessità, i sistemi ed i servizi informatici "critici" dell'Azienda;
- che la gestione dei sistemi e servizi informatici e delle infrastrutture tecnologiche dell'Azienda Ospedaliero Universitaria Careggi prevede, per la fase più propriamente operativa, il prevalente coinvolgimento di ESTAR – Ente di Supporto Tecnico Amministrativo Regionale – che ha tra i propri compiti istituzionali in ambito ICT anche quelli di governare l'operatività quotidiana dei sistemi informativi, delle reti e dei data center delle Aziende del Servizio Sanitario Regionale.
- che la cooperazione tra il Centro Operativo Sicurezza Cibernetica - Polizia Postale e per la Sicurezza Cibernetica per la "Toscana" e l'Azienda Ospedaliero Universitaria Careggi, volta alla prevenzione e alla repressione dei crimini informatici, ispirata al principio di sicurezza partecipata, nell'intento di assicurare in via sinergica ed efficiente le risorse del Sistema Paese a vantaggio dell'intera collettività, contribuisce al contenimento dei costi operativi derivanti da interruzioni dei servizi erogati attraverso sistemi informatici e di telecomunicazioni.

TUTTO CIO' PREMESSO
LE PARTI STIPULANO E CONVENGONO QUANTO SEGUE

Articolo 1

1. Le Parti si impegnano a sviluppare un piano di collaborazione volto:
   a) alla condivisione e all'analisi di informazioni idonee a prevenire e contrastare attacchi o danneggiamenti in pregiudizio delle infrastrutture informatiche dell'Azienda Ospedaliero Universitaria Careggi per le finalità meglio in premessa specificate;
   b) alla segnalazione di emergenze relative a vulnerabilità, minacce ed incidenti in danno della regolarità dei servizi di telecomunicazione;

c) all'identificazione dell'origine degli attacchi che abbiano come destinazione le infrastrutture tecnologiche dell'Azienda Ospedaliero Universitaria Careggi o che traggano origine dalle medesime;
d) alla realizzazione e alla gestione di attività di comunicazione fra le Parti per fronteggiare situazioni di emergenza.

2. Le attività necessarie al conseguimento degli obiettivi di cui al precedente comma 1 verranno assicurate dal Centro Operativo Sicurezza Cibernetica e dall'Azienda Ospedaliero Universitaria Careggi che, per la parte operativa e di intervento su sistemi ed infrastrutture tecnologiche aziendali, rappresenta il riferimento nei confronti di ESTAR.

Articolo 2

1. Le Parti potranno sviluppare attività formativa congiunta sui sistemi e sulle tecnologie informatiche utilizzate, nonché sulle procedure di intervento atte a prevenire e contrastare gli accessi illeciti o i tentativi di accesso illecito ai danni di tali sistemi e tecnologie nonché i fenomeni delittuosi di cui all'art. 1.

Articolo 3

1. Le Parti cooperano al fine di realizzare eventuali tecnologie necessarie per rendere operativo il presente Protocollo d'Intesa, il cui oggetto primario è rappresentato dalla collaborazione da parte della Polizia Postale e per la Sicurezza Cibernetica, anche attraverso l'interscambio di dati, finalizzata ad incrementare i livelli di prevenzione e contrasto dei crimini informatici ai danni dei sistemi dell'Azienda Ospedaliero Universitaria Careggi, precisando che gli eventuali oneri, comunque concordati preventivamente, relativi all'attuazione della stessa, sono a carico dell'Azienda Ospedaliero Universitaria Careggi, in coerenza con l'art. 39, comma 2, della L. 16 gennaio 2003, n. 3.
2. La cooperazione tra le parti dovrà tenere conto del ruolo rivestito da ESTAR all'interno del Servizio Sanitario Regionale della Toscana così come indicato in premessa
3. Nessun onere economico specifico deriva dal presente accordo per l'Amministrazione della Pubblica Sicurezza.

Articolo 4

1. Le Parti si impegnano a sviluppare iniziative congiunte, concordate preventivamente, volte a valorizzare il reciproco rapporto di collaborazione,

anche tramite l'utilizzo delle denominazioni, degli stemmi, degli emblemi e degli altri segni distintivi in uso esclusivo alla Polizia di Stato, nel rispetto del decreto del Ministro dell'Interno 19 settembre 2017, n. 215.

2. Le Parti hanno facoltà di promuovere i rispettivi brand, anche attraverso la realizzazione di spot dedicati da trasmettere su network televisivi e piattaforme social ovvero a mezzo stampa sui principali quotidiani. Le predette attività saranno realizzate con il coordinamento del competente Ufficio relazioni esterne, cerimoniale e studi storici della Segreteria del Dipartimento. A tal fine, l'Azienda Ospedaliero Universitaria Careggi avrà cura di comunicare preventivamente al C.O.S.C. "Toscana" ogni eventuale iniziativa attraverso la competente struttura aziendale.

Articolo 5

1. Le Parti si impegnano a trattare ed a custodire i dati e le informazioni personali acquisite nell'ambito delle attività previste dal presente Protocollo d'Intesa nel rispetto della normativa in materia di protezione dei dati personali.
2. Ciascuna *Parte* si impegna a mantenere riservati ed a non utilizzare i risultati delle attività svolte in comune senza il preventivo consenso scritto dell'altra *Parte*.
3. L'obbligo di riservatezza di cui al comma che precede, permane anche successivamente all'estinzione del presente Protocollo d'Intesa.

Articolo 6

1. Il presente Protocollo d'Intesa, che entra in vigore dalla data della sottoscrizione, ha durata di tre anni e può essere rinnovato con accordo scritto tra le parti.

Articolo 7

1. Ogni controversia relativa all'interpretazione ed all'esecuzione del presente Protocollo d'Intesa viene esaminata bonariamente dalle Parti.
2. Le Parti potranno recedere dal presente accordo senza onere alcuno previo preavviso scritto.
3. A tutti gli effetti di legge, l'Azienda ospedaliero Universitaria Careggi dichiara di eleggere domicilio presso la sede legale di Largo Brambilla 3, 50134 a Firenze

Azienda Ospedaliero Universitaria Careggi

Letto, approvato e sottoscritto.
Redatto in n. 3 copie originali.

Luogo, data

IL DIRIGENTE
DEL CENTRO OPERATIVO
SICUREZZA CIBERNETICA
POLIZIA POSTALE PER LA
SICUREZZA CIBERNETICA
"TOSCANA"

Dr.ssa Lorena La Spina

IL DIRETTORE GENERALE
DELL'AZIENDA OSPEDALIERO
UNIVERSITARIA CAREGGI

Dr.ssa Daniela Matarrese