DELIBERAZIONE DEL DIRETTORE GENERALE

Deliberazione n.ro	Data di Adozione
0001901	06/10/2022

OGGETTO: Presa d'atto del Protocollo d'Intesa in materia di Cybersecurity sottoscritto tra ASL Bari e Scudomed – Health Risk Manager e Legal Advisor.

PROPOSTA DI DELIBERAZIONE DEL DIRETTORE GENERALE N.RO 20220003124 DEL 04/10/2022
COMPOSTA COMPLESSIVAMENTE DA 11 (undici) PAGINE
DI 1 (uno) ALLEGATI SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 13 (tredici) PAGINE
DI 0 (zero) ALLEGATI NON SOGGETTI A PUBBLICAZIONE PER UN TOTALE DI 0 (zero) PAGINE
DI 0 (zero) DOCUMENTI ISTRUTTORI NON ALLEGATI PER UN TOTALE DI 0 (zero) PAGINE

Con la sottoscrizione in calce, i Direttori dichiarano di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, alla Parte II, par. 1, lett. c) del vigente PTPCT – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

Parere del Direttore Amministrativo	Parere del Direttore Sanitario
Firmato Digitalmente il 04/10/2022 15:18 Luigi FRUSCIO	*Firmato Digitalmente il 04/10/2022 18:03* Donato SIVO

Il Segretario	Il Direttore Generale
Firmato Digitalmente il 06/10/2022 09:08 Gianpaolo PARISI	*Firmato Digitalmente il 06/10/2022 08:29* Antonio SANGUEDOLCE

ATTESTAZIONE DI AVVENUTA PUBBLICAZIONE

Si attesta che il presente provvedimento viene pubblicato all'Albo pretorio *on-line* della ASL BA, ai sensi dell'art. 32, c. 1, l. 69/2009, per la durata di 30 giorni naturali, decorrenti dal **06/10/2022**

Unità Operativa Affari Generali
L'Addetto alla Pubblicazione
Firmato Digitalmente il 06/10/2022 09:09
Domenico ROVETO

Oggetto: Presa d'atto del Protocollo d'Intesa in materia di Cybersecurity sottoscritto tra ASL Bari e Scudomed – Health Risk Manager e Legal Advisor.

IL DIRETTORE GENERALE

Vista la Deliberazione n. 239/DG del 16.02.2022 con l'assistenza del Segretario, sulla base della istruttoria e della proposta formulata dal Direttore del Servizio di Informazione e Comunicazione Istituzionale che attesta la regolarità formale del procedimento ed il rispetto della legalità, considera e delibera quanto segue.

VISTO il Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico, emanato dalla Presidenza del Consiglio dei Ministri nel dicembre 2013, che demanda all'Agenzia per l'Italia Digitale la formulazione di "indirizzi, regole tecniche e linee guida in materia di sicurezza informatica" e la cura della "promozione e diffusione delle iniziative di alfabetizzazione informatica".

VISTA la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6.7.2016, recante Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

VISTA la Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, adottata con D.P.C.M. 17.2.2017, riferimento nazionale strategico e operativo entro cui operare in modo coordinato tra il settore pubblico e quello privato.

VISTO il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica, emanato dalla Presidenza del Consiglio dei Ministri nel marzo 2017.

VISTE le Misure minime di sicurezza ICT per le pubbliche amministrazioni, definite e adottate da AgID con la Circolare n. 2 del 18.4.2017, e le Linee guida di sicurezza nello sviluppo delle applicazioni (Linee guida per lo sviluppo del software sicuro), emesse da AgID in data 21.11.2017 e i relativi allegati.

VISTO il Libro Bianco concernente il futuro della cybersecurity in Italia, redatto e pubblicato nel gennaio 2018 dal Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l'Informatica, in cui si auspica che la politica nazionale sulla sicurezza informatica "si traduca al più presto in azioni concrete" e che sottolinea come "la realizzazione dei progetti, data la diversità degli obiettivi e delle competenze necessarie, richiederà una

particolare sinergia tra il mondo della ricerca, quello governativo e quello dell'industria, anche attraverso opportuni meccanismi di partnership pubblicoprivato".

VISTO il Piano nazionale di ripresa e resilienza, deliberato dal Consiglio dei ministri nella riunione del 29 aprile 2021, prevede apposite progettualità nell'ambito della cybersicurezza, quale fattore necessario per tutelare la sicurezza dello sviluppo e della crescita dell'economia e dell'industria nazionale, ponendo la cybersicurezza a fondamento della trasformazione digitale.

VISTA l'Agenzia per la cybersicurezza nazionale istituita per soddisfare la connessa esigenza di ridefinire l'architettura italiana di cybersicurezza al fine di adeguarla all'evoluzione tecnologica, al contesto di minaccia proveniente dallo spazio cibernetico, nonché al quadro normativo europeo.

VISTO che l'interesse manifestato a livello nazionale evoca l'importanza del tema della cybersicurezza.

CONSIDERATO che è necessario assicurare anche nelle Aziende Sanitarie uno sviluppo diffuso della cultura digitale con particolare riferimento alla sicurezza informatica, anche alla luce della normativa e delle direttive sia europee sia nazionali.

CONSIDERATO che il crimine informatico è in aumento costante ed esponenziale e che risulta improcrastinabile la promozione di una maggiore consapevolezza in merito alle misure di sicurezza necessarie a ridurre il rischio di attacchi informatici.

CONSIDERATO che il crimine informatico costituisce oggi una minaccia comune e trasversale nel Paese, in tutti gli ambiti, e specie in quello della sanità, coinvolgendo tanto il settore pubblico quanto quello privato.

CONSIDERATA, pertanto, l'opportunità di predisporre iniziative in materia di sicurezza informatica a favore della azienda Sanitaria locale di Bari.

CONSIDERATO che una collaborazione solida, strutturata e continuativa tra il settore pubblico e il panorama di soggetti, anche privati, con elevata specializzazione ed esperienza nella materia di che trattasi, è in grado di garantire uno sviluppo trasversale e sinergico delle competenze necessarie all'implementazione delle strategie di sicurezza informatica.

PREMESSO CHE

- secondo il rapporto CLUSIT 2022 dell'Associazione Italiana per la Sicurezza Informatica, a livello globale, i cyber attacchi sono cresciuti sia in quantità che in qualità: rispetto all'anno precedente, infatti, nel 2021 si è verificato un aumento di attacchi del 10%, con l'ulteriore dato che il 79% degli attacchi rilevati (contro il 50% del 2020) ha avuto un impatto "elevato"

e, di questi, il 32% è stato caratterizzato da una severity "critica" ed il 47% da una severity "alta";

- il medesimo rapporto ha, altresì, evidenziato come in Italia il settore sanitario sia tra quelli maggiormente colpiti: nell'anno 2021, infatti, il 13% degli attacchi informatici è stato realizzato in tale ambito, con un incremento del 24,8% rispetto all'anno precedente e con il coinvolgimento del 66% delle strutture sanitarie, rispetto al 34% del 2020;
- con specifico riferimento all'ambito sanitario, si tratta di un trend in costante crescita, aggravatosi con lo scoppio della guerra in Ucraina e, già prima di essa, in via di ampliamento a fronte del maggiore uso delle tecnologie ICT dovuto alla pandemia da Covid -19, tanto che, con riferimento agli ultimi mesi del 2021 ed ai primi otto mesi del 2022, l'Italia occupa il quarto posto tra le nazioni al mondo interessate dal maggior numero di aggressioni cyber alle strutture sanitarie ed ospedaliere;
- in questi mesi sono stati rivendicati più di 10 attacchi informatici rivolti a strutture sanitarie, tra cui quelli che hanno colpito l'Ospedale San Giovanni Addolorata di Roma, la ASL 3 di Roma, la ASL 2 di Savona, la ASP di Messina 2021, la ASST Lecco, la ASP Messina, la ATS Insubria e l'Ospedale Macedonio Melloni di Milano, cui si aggiungono l'attacco ransomware alla Regione Lazio che ha interessato, tra l'altro, il portale di prenotazione dei vaccini Covid 19, l'attacco ransomware ai sistemi informativi dell'Unità Socio Sanitaria Locale 6 Euganea di Padova che ha riguardato il Cup, i centri prelievo, le funzionalità di registrazione dei nuovi pazienti, il sistema dei laboratori e gli hub vaccinali, con conseguente diffusione di dati sensibili (9.346 file contenenti referti e diagnosi dei pazienti, protocolli di cura, cedolini paga del personale ospedaliero, informazioni sul budget dei reparti e molto altro ancora), l'attacco ransomware all'Usl Napoli 3 che ha bloccato il sistema di prenotazione vaccini, l'attacco ai Presidi Ospedalieri e Territoriali dell'Azienda Socio Sanitaria Territoriale Fatebenefratelli Sacco che ha compromesso la funzionalità dei sistemi informatici gestionali, imponendo così la gestione cartacea con conseguente impossibilità di accedere allo storico nonché il dirottamento delle emergenze verso gli ospedali non facenti parte dell'ASST Fatebenefratelli Sacco stante la compromessa capacità del Pronto Soccorso di ricevere i pazienti nonché, da ultimo, l'attacco del 19.08 u.s. messo in atto nei confronti della ASL Città di Torino che ha coinvolto gli Ospedali San Giovanni Bosco, Maria Vittoria, Martini e Oftalmico e ha reso necessario fermare tutti i sistemi informatici aziendali, per effettuare le verifiche ed i monitoraggi indispensabili per la messa in sicurezza dei dati ed il ripristino degli applicativi aziendali cautelativamente bloccati;

- tali eventi rendono fondate le conclusioni dello studio "Healthcare Cybersecurity" di Bitdefender, reso pubblico l'anno scorso, secondo il quale in Italia, il 93% delle aziende del settore sanitario ha subito attacchi informatici in passato, mentre il 64% ritiene probabile, o altamente probabile, un attacco nel prossimo futuro;
- la copiosità numerica degli attacchi informatici in ambito sanitario trova la propria giustificazione nell'elevata mole di dati sensibili gestiti dagli enti operanti nel settore che li rende un obiettivo appetibile per i cyber attacchi visto che i dati sanitari sono di grande valore e, perciò, trovano molti acquirenti nel dark web o comunque diventano oggetto di richiesta di riscatto elevato.

CONSIDERATO CHE

- gli attacchi informatici diretti alle strutture sanitarie si caratterizzano per il rilevante impatto che producono sui cittadini e sulla loro salute, oltreché sul sistema sanitario in sé, visto che comportano, ancorché temporaneamente, la paralisi o comunque una minore efficienza di servizi essenziali quali quelli ospedalieri, stante l'impossibilità da parte dei sanitari di accedere per un lasso di tempo più o meno lungo alle cartelle cliniche elettroniche e/o ad altri servizi basati su connessione di rete, con conseguente sensibile riduzione della capacità di offrire ai pazienti le cure di cui necessitano in modo tempestivo;
- recenti studi hanno messo in luce l'ulteriore grande criticità degli attacchi informatici in sanità, evidenziando la sussistenza di una diretta correlazione tra i medesimi e l'incremento della mortalità negli ospedali coinvolti, anche in considerazione del fatto che gli inconvenienti causati da cyber attacchi talvolta rendono indispensabile dirottare le ambulanze verso altri presidi e questo, in situazioni di emergenza, può determinare una significativa riduzione delle possibilità di sopravvivenza del paziente in condizioni critiche;
- uno studio pubblicato dall'agenzia americana CISA (Cybersecurity and Infrastructure Security Agency) ha segnalato che la perdita di dati causata dai cyber attacchi produce effetti deleteri per i sistemi sanitari anche a lungo termine, in considerazione dei ritardi nella prestazione di servizi diagnostici o di assistenza registrati anche settimane o mesi dopo gli attacchi;
- gli attacchi informatici producono altresì conseguenze reputazionali negative per gli enti del settore sanitario, con conseguente danno all'immagine delle stesse.

RITENUTO CHE

- la gravità delle conseguenze dei cyber attacchi in ambito sanitario, nonché la copiosità numerica degli stessi rende necessario, da un lato, sviluppare una maggiore consapevolezza del rischio tra i dipendenti e, dall'altro, potenziare i sistemi informatici degli enti sanitari, adottando misure attuative dei principi della sicurezza predittiva, preventiva e proattiva, al fine di proteggere adeguatamente non solo i dati sanitari, ma anche l'operatività dei servizi stessi, salvaguardando così la salute dei pazienti;
- ai fini della sicurezza predittiva, è indispensabile monitorare accuratamente quali siano le principali minacce presenti sul web, sul deepweb e sul darkweb, cercando – ove possibile - di fare attività di early warning;
- la sicurezza preventiva impone di predisporre delle simulazioni di attacco alle proprie infrastrutture, in modo da stabilire con anticipo quali siano le minacce alle quali si è esposti e poter adottare le opportune contromisure;
- la sicurezza proattiva si prefigge di comprendere come reagire in modo efficace ad un attacco hacker, cercando di limitare i danni diretti e indiretti ed abbreviare il più possibile il tempo di ripristino dell'infrastruttura.

PRESO ATTO CHE

- il Piano nazionale di ripresa e resilienza, deliberato dal Consiglio dei ministri nella riunione del 29 aprile 2021, prevede apposite progettualità nell'ambito della cybersicurezza, quale fattore necessario per tutelare la sicurezza dello sviluppo e della crescita dell'economia e dell'industria nazionale, ponendo la cybersicurezza a fondamento della trasformazione digitale;
- per soddisfare la connessa esigenza di ridefinire l'architettura italiana di cybersicurezza, è stata istituita un'apposita Agenzia per la cybersicurezza nazionale, per adeguarla all'evoluzione tecnologica, al contesto di minaccia proveniente dallo spazio cibernetico, nonché al quadro normativo europeo;
- l'interesse manifestato a livello nazionale evoca l'importanza del tema della cybersicurezza.

RILEVATA

- la necessità di potenziare la sicurezza dei sistemi informativi della l'ASL Bari, sia attraverso l'analisi della maturità digitale dell'Azienda - tra l'altro in tema di cybersecurity - sia

mediante l'individuazione di corrette procedure aziendali volte a ridurre il rischio di attacchi informatici e a gestire correttamente l'eventuale verificarsi degli stessi;

- la necessità, all'uopo, di affidarsi a soggetti specializzati dotati di esperienza e competenze tecniche specialistiche nel settore.

TENUTO CONTO CHE

- Scudomed – Health Risk Manager e Legal Advisor, associazione senza scopo di lucro specializzata nell'identificazione, valutazione e misurazione dei rischi in ambito sanitario, nonché nella gestione, mitigazione ed eliminazione dei rischi individuati e nel testing dell'adeguatezza e dell'efficacia dei processi aziendali di governo dei rischi connessi alla digital health, ha trasmesso, in data 15.06.2022 , una bozza di Protocollo d'intesa in materia di Cybersecurity da stipularsi con questa Azienda ;
- le finalità istituzionali dell'associazione includono la promozione e lo studio delle dinamiche organizzative e dei connessi rischi derivanti dalla presa in carico dei pazienti durante i processi di diagnosi e cura, anche a fini di ricerca scientifica;
- la Scudomed, in virtù dell'esperienza maturata nel settore e delle competenze tecniche di cui dispone, è stata riconosciuta presso il Ministero dello Sviluppo Economico come associazione professionale, ai sensi della L. 14 gennaio 2013, n. 4, autorizzata a rilasciare attestati di qualificazione professionale dei servizi prestati nell'ambito della gestione dei rischi.

VISTI

- il documento "Protocollo d'intesa" trasmesso in bozza dalla predetta associazione Scudomed;
- le successive modifiche ed integrazioni apportate al suddetto Protocollo da questa Azienda e condivise con Scudomed;
- in particolare, l'art. 3 "Oggetto" del Protocollo d'intesa che risulta pienamente conforme e rispondente alle esigenze e finalità perseguite dall'ASL Bari attraverso la stipula del suddetto Accordo.

RAVVISATA la necessità di istituire un Comitato, composto da Referenti del Protocollo d'Intesa nominati dalle Parti, per assicurare la gestione ed il coordinamento delle attività oggetto del presente atto demandando agli stessi il compito di coordinare le azioni intraprese

dal proprio Ente di appartenenza con quelle poste in essere dall'altra Parte, al fine di raggiungere una maggiore efficacia e una migliore efficienza degli sforzi profusi, come meglio specificato all'art. 5 dello stesso Protocollo.

DATO ATTO CHE il Comitato ha durata biennale, coincidente con la durata del protocollo di intesa di cui trattasi. La partecipazione al Comitato non comporta oneri né alcun tipo di spese, ivi compresi compensi o gettoni di presenza, salari, provvigioni, emolumenti, indennità o altri benefici, comunque denominati.
Le riunioni del Comitato tecnico scientifico possono essere effettuate anche in modalità telematica.

TENUTO CONTO, ALTRESÌ, CHE le attività di cui al presente Protocollo saranno rese da Scudomed a titolo gratuito senza ulteriori oneri a carico del bilancio dell'Azienda Sanitaria Locale di Bari.
L'ASL Bari riconoscerà alla Scudomed un rimborso delle spese vive, strettamente connesse allo svolgimento delle attività di cui al presente Protocollo, quantificato, in maniera forfettaria, in un importo omnicomprensivo pari ad € 10.000,00 annui, oltre IVA come per legge.

DATO ATTO CHE Scudomed ed ASL Bari hanno stipulato, con apposizione di firma digitale rispettivamente in data 3 e 4 ottobre u.s., il succitato "Protocollo d'Intesa in materia di Cybersecurity" che si allega al presente provvedimento per formarne parte integrante e sostanziale.

RITENUTO, PERTANTO, PER QUANTO ESPOSTO SOPRA:

- di dover recepire con atto deliberativo il Protocollo d'Intesa in oggetto stipulato tra le Parti, che si allega al presente provvedimento per formarne parte integrante.

Assunto il parere favorevole del Direttore Amministrativo e del Direttore Sanitario

DELIBERA

Per le motivazioni esposte in premessa, che qui si intendono completamente acquisite e che formano parte sostanziale del presente atto deliberativo:

1) di prendere atto del Protocollo d'Intesa in materia di Cybersecurity, stipulato tra Scudomed – Health Risk Manager e Legal Advisor e la ASL Bari, allegato al presente atto per costituirne parte integrante (all. n. 1);

2) di stabilire che il suddetto Protocollo d'Intesa abbia durata di 2 anni, come meglio dettagliato quanto a modalità e contenuto all'art. 7 del predetto Protocollo;

3) di dare atto che le attività di cui al presente Protocollo saranno rese da Scudomed a titolo gratuito senza ulteriori oneri a carico del bilancio dell'Azienda Sanitaria Locale di Bari.

4) di stabilire che la ASL Bari riconoscerà alla SCUDOMED esclusivamente il rimborso delle spese vive, strettamente connesse allo svolgimento delle attività di cui al presente Protocollo, quantificate, in maniera forfettaria, in un importo omnicomprensivo pari ad € 10.000,00 annui, oltre IVA come per legge, imputando detta spesa sul conto n.733.105.0050 "Altri oneri di gestione" del Bilancio 2022;

5) di istituire il Comitato dei Referenti del Protocollo d'Intesa in materia di Cybersecurity per assicurare la gestione ed il coordinamento delle attività oggetto del presente atto demandando agli stessi il compito di coordinare le azioni intraprese dal proprio Ente di appartenenza con quelle poste in essere dall'altra Parte, al fine di raggiungere una maggiore efficacia e una migliore efficienza degli sforzi profusi, come meglio specificato all'art. 5 dello stesso Protocollo;

6) di prevedere che la partecipazione al suddetto Comitato non comporta oneri, né alcun tipo di spese a carico del Bilancio Aziendale, ivi compresi compensi o gettoni di presenza, salari, provvigioni, emolumenti, indennità o altri benefici, comunque denominati;

7) di trasmettere il presente provvedimento all'Area Gestione Risorse Finanziarie per gli adempimenti di competenza ed al Collegio Sindacale;

8) di trasmettere il suddetto provvedimento, per conoscenza, a tutte le Macrostrutture Aziendali;

9) di demandare alla UOS Privacy la notificazione del presente provvedimento alla Scudomed – Health Risk Manager e Legal Advisor;

10) di prevedere la pubblicazione del presente provvedimento nella Sezione Amministrazione Trasparente/Provvedimenti ai sensi dell'art. 23 del D.Lgs. n. 33/2013;

11) di attestare di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, 1. 241/90, artt. 6 e 7, D.P.R. 62/2013, vigente codice di comportamento aziendale e art. 1, c. 9, lett. e), 1. 190/2012, tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, d. lgs.165/2001.

SCUDOMED ®
Health Risk Manager e Legal Advisor

ASL Bari
PugliaSalute

PROTOCOLLO D'INTESA

IN MATERIA DI CYBERSECURITY

Tra

SCUDOMED Health Risk Manager e Legal Advisor, c.f./p.iva 97742980580, con sede in Roma (RM) alla Via Cesare Fracassini, 25, 00196, in persona del suo legale rapp.te in carica p.t., Avv. Massimiliano D. Parla (di seguito **Scudomed**)

e

AZIENDA SANITARIA LOCALE della provincia di Bari, c.f. e p.iva 06534340721, con sede in Lungomare Starita 6, 70123 Bari (BA), in persona del suo legale rapp.te in carica p.t., Dr. Antonio Sanguedolce (di seguito **Azienda**),

VISTO il Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico, emanato dalla Presidenza del Consiglio dei Ministri nel dicembre 2013, che demanda all'Agenzia per l'Italia Digitale la formulazione di "indirizzi, regole tecniche e linee guida in materia di sicurezza informatica" e la cura della "promozione e diffusione delle iniziative di alfabetizzazione informatica";
VISTA la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6.7.2016, recante Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;
VISTA la Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, adottata con D.P.C.M. 17.2.2017, riferimento nazionale strategico e operativo entro cui operare in modo coordinato tra il settore pubblico e quello privato;
VISTO il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica, emanato dalla Presidenza del Consiglio dei Ministri nel marzo 2017;
VISTE le Misure minime di sicurezza ICT per le pubbliche amministrazioni, definite e adottate da AgID con la Circolare n. 2 del 18.4.2017, e le Linee guida di sicurezza nello sviluppo delle applicazioni (Linee guida per lo sviluppo del software sicuro), emesse da AgID in data 21.11.2017 e i relativi allegati;
VISTO il Libro Bianco concernente il futuro della cybersecurity in Italia, redatto e pubblicato nel gennaio 2018 dal Laboratorio Nazionale di Cybersecurity del Consorzio Interuniversitario Nazionale per l'Informatica, in cui si auspica che la politica nazionale sulla sicurezza informatica "si traduca al

più presto in azioni concrete" e che sottolinea come "la realizzazione dei progetti, data la diversità degli obiettivi e delle competenze necessarie, richiederà una particolare sinergia tra il mondo della ricerca, quello governativo e quello dell'industria, anche attraverso opportuni meccanismi di partnership pubblico-privato";

VISTO il Piano nazionale di ripresa e resilienza, deliberato dal Consiglio dei ministri nella riunione del 29 aprile 2021, che prevede apposite progettualità nell'ambito della cybersicurezza, quale fattore necessario per tutelare la sicurezza dello sviluppo e della crescita dell'economia e dell'industria nazionale, ponendo la cybersicurezza a fondamento della trasformazione digitale;

VISTA l'Agenzia per la cybersicurezza nazionale istituita per soddisfare la connessa esigenza di ridefinire l'architettura italiana di cybersicurezza al fine di adeguarla all'evoluzione tecnologica, al contesto di minaccia proveniente dallo spazio cibernetico, nonché al quadro normativo europeo;

VISTO che l'interesse manifestato a livello nazionale evoca l'importanza del tema della cybersicurezza;

CONSIDERATO che è necessario assicurare anche nelle Aziende Sanitarie uno sviluppo diffuso della cultura digitale con particolare riferimento alla sicurezza informatica, anche alla luce della normativa e delle direttive sia europee sia nazionali;

CONSIDERATO che il crimine informatico è in aumento costante ed esponenziale e che risulta improcrastinabile la promozione di una maggiore consapevolezza in merito alle misure di sicurezza necessarie a ridurre il rischio di attacchi informatici;

CONSIDERATO che il crimine informatico costituisce oggi una minaccia comune e trasversale nel Paese, in tutti gli ambiti, e specie in quello della sanità, coinvolgendo tanto il settore pubblico quanto quello privato;

CONSIDERATA, pertanto, l'opportunità di predisporre iniziative in materia di sicurezza informatica a favore della Azienda Sanitaria Locale di Bari;

CONSIDERATO che una collaborazione solida, strutturata e continuativa tra il settore pubblico e il panorama di soggetti anche privati con elevata specializzazione ed esperienza nella materia di che trattasi, è in grado di garantire uno sviluppo trasversale e sinergico delle competenze necessarie all'implementazione delle strategie di sicurezza informatica;

PREMESSO CHE

- secondo il rapporto CLUSIT 2022 dell'Associazione Italiana per la Sicurezza Informatica, a livello globale, i cyber attacchi sono cresciuti sia in quantità che in qualità: rispetto all'anno

precedente, infatti, nel 2021 si è verificato un aumento di attacchi del 10%, con l'ulteriore dato che il 79% degli attacchi rilevati (contro il 50% del 2020) ha avuto un impatto "elevato" e, di questi, il 32% è stato caratterizzato da una severity "critica" ed il 47% da una severity "alta";

- il medesimo rapporto ha, altresì, evidenziato come in Italia il settore sanitario sia tra quelli maggiormente colpiti: nell'anno 2021, infatti, il 13% degli attacchi informatici è stato realizzato in tale ambito, con un incremento del 24,8% rispetto all'anno precedente e con il coinvolgimento del 66% delle strutture sanitarie, rispetto al 34% del 2020;
- con specifico riferimento all'ambito sanitario, si tratta di un trend in costante crescita, aggravatosi con lo scoppio della guerra in Ucraina e, già prima di essa, in via di ampliamento a fronte del maggiore uso delle tecnologie ICT dovuto alla pandemia da Covid -19, tanto che, con riferimento agli ultimi mesi del 2021 ed ai primi otto mesi del 2022, l'Italia occupa il quarto posto tra le nazioni al mondo interessate dal maggior numero di aggressioni cyber alle strutture sanitarie ed ospedaliere;
- in questi mesi sono stati rivendicati più di 10 attacchi informatici rivolti a strutture sanitarie, tra cui quelli che hanno colpito l'Ospedale San Giovanni Addolorata di Roma, la ASL 3 di Roma, la ASL 2 di Savona, la ASP di Messina 2021, la ASST Lecco, la ASP Messina, la ATS Insubria e l'Ospedale Macedonio Melloni di Milano, cui si aggiungono l'attacco ransomware alla Regione Lazio che ha interessato, tra l'altro, il portale di prenotazione dei vaccini Covid 19, l'attacco ransomware ai sistemi informativi dell'Unità Socio Sanitaria Locale 6 Euganea di Padova che ha riguardato il Cup, i centri prelievo, le funzionalità di registrazione dei nuovi pazienti, il sistema dei laboratori e gli hub vaccinali, con conseguente diffusione di dati sensibili (9.346 file contenenti referti e diagnosi dei pazienti, protocolli di cura, cedolini paga del personale ospedaliero, informazioni sul budget dei reparti e molto altro ancora), l'attacco ransomware all'Usl Napoli 3 che ha bloccato il sistema di prenotazione vaccini, l'attacco ai Presidi Ospedalieri e Territoriali dell'Azienda Socio Sanitaria Territoriale Fatebenefratelli Sacco che ha compromesso la funzionalità dei sistemi informatici gestionali, imponendo così la gestione cartacea con conseguente impossibilità di accedere allo storico nonché il dirottamento delle emergenze verso gli ospedali non facenti parte dell'ASST Fatebenefratelli Sacco stante la compromessa capacità del Pronto Soccorso di ricevere i pazienti nonché, da ultimo, l'attacco del 19.08 u.s. messo in atto nei confronti della ASL Città di Torino che ha coinvolto gli Ospedali San Giovanni Bosco, Maria Vittoria, Martini e Oftalmico e ha reso necessario fermare tutti i sistemi informatici aziendali, per effettuare le verifiche ed i

monitoraggi indispensabili per la messa in sicurezza dei dati ed il ripristino degli applicativi aziendali cautelativamente bloccati;

- tali eventi rendono fondate le conclusioni dello studio "Healthcare Cybersecurity" di Bitdefender, reso pubblico l'anno scorso, secondo il quale in Italia, il 93% delle aziende del settore sanitario ha subito attacchi informatici in passato, mentre il 64% ritiene probabile, o altamente probabile, un attacco nel prossimo futuro;
- la copiosità numerica degli attacchi informatici in ambito sanitario trova la propria giustificazione nell'elevata mole di dati sensibili gestiti dagli enti operanti nel settore che li rende un obiettivo appetibile per i cyber attacchi visto che i dati sanitari sono di grande valore e, perciò, trovano molti acquirenti nel dark web o comunque diventano oggetto di richiesta di riscatto elevato;

CONSIDERATO CHE

- gli attacchi informatici diretti alle strutture sanitarie si caratterizzano per il rilevante impatto che producono sui cittadini e sulla loro salute, oltreché sul sistema sanitario in sé, visto che comportano, ancorché temporaneamente, la paralisi o comunque una minore efficienza di servizi essenziali quali quelli ospedalieri, stante l'impossibilità da parte dei sanitari di accedere per un lasso di tempo più o meno lungo alle cartelle cliniche elettroniche e/o ad altri servizi basati su connessione di rete, con conseguente sensibile riduzione della capacità di offrire ai pazienti le cure di cui necessitano in modo tempestivo;
- recenti studi hanno messo in luce l'ulteriore grande criticità degli attacchi informatici in sanità, evidenziando la sussistenza di una diretta correlazione tra i medesimi e l'incremento della mortalità negli ospedali coinvolti, anche in considerazione del fatto che gli inconvenienti causati da cyber attacchi talvolta rendono indispensabile dirottare le ambulanze verso altri presidi e questo, in situazioni di emergenza, può determinare una significativa riduzione delle possibilità di sopravvivenza del paziente in condizioni critiche;
- uno studio pubblicato dall'agenzia americana CISA (Cybersecurity and Infrastructure Security Agency) ha segnalato che la perdita di dati causata dai cyber attacchi produce effetti deleteri per i sistemi sanitari anche a lungo termine, in considerazione dei ritardi nella prestazione di servizi diagnostici o di assistenza registrati anche settimane o mesi dopo gli attacchi;
- gli attacchi informatici producono, altresì, conseguenze reputazionali negative per gli enti del settore sanitario, con conseguente danno all'immagine delle stesse;

RITENUTO CHE

- la gravità delle conseguenze dei cyber attacchi in ambito sanitario, nonché la copiosità numerica degli stessi rende necessario, da un lato, sviluppare una maggiore consapevolezza del rischio tra i dipendenti e, dall'altro, potenziare i sistemi informatici degli enti sanitari, adottando misure attuative dei principi della sicurezza predittiva, preventiva e proattiva, al fine di proteggere adeguatamente non solo i dati sanitari, ma anche l'operatività dei servizi stessi, salvaguardando così la salute dei pazienti;
- ai fini della sicurezza predittiva, è indispensabile monitorare accuratamente quali siano le principali minacce presenti sul web, sul deepweb e sul darkweb, cercando – ove possibile - di fare attività di early warning;
- la sicurezza preventiva impone di predisporre delle simulazioni di attacco alle proprie infrastrutture, in modo da stabilire con anticipo quali siano le minacce alle quali si è esposti e poter adottare le opportune contromisure;
- la sicurezza proattiva si prefigge di comprendere come reagire in modo efficace ad un attacco hacker, cercando di limitare i danni diretti e indiretti ed abbreviare il più possibile il tempo di ripristino dell'infrastruttura;
- risulta necessario potenziare la sicurezza dei sistemi informativi della l'ASL Bari, sia attraverso l'analisi della maturità digitale dell'Azienda - tra l'altro in tema di cybersecurity - sia mediante l'individuazione di corrette procedure aziendali volte a ridurre il rischio di attacchi informatici e a gestire correttamente l'eventuale verificarsi degli stessi;
- la ASL di Bari intende affidarsi a soggetti specializzati dotati di esperienza e competenze tecniche specialistiche nel settore;

DATO ATTO CHE

- **SCUDOMED** no profit nasce nel 2013 e, in breve tempo, diviene il punto di riferimento nazionale per le maggiori Società Scientifiche, enti pubblici e privati sanitari e sociosanitari, affiancandoli nella analisi e trattamento dei rischi in ambito sanitario con la predisposizione di linee guida, *best practies*, procedure e protocolli di pianificazione, nonché *policy* aziendali.

Le finalità istituzionali dell'Associazione includono la promozione e lo studio delle dinamiche organizzative e ai connessi rischi derivanti dalla presa in carico dei pazienti durante i processi di diagnosi e cura, anche a fini di ricerca scientifica.

L'Associazione si prefigge, altresì, il compito di fornire agli associati e ai propri *partner* tutti i migliori ed innovativi strumenti tecnici e formativi, anche in vista delle decisive sfide e innovazioni che stanno interessando in maniera rivoluzionaria il comparto sanitario nazionale, con particolare riferimento alla *digital health* al fine di perseguire la massima qualità, efficienza ed efficacia dell'assistenza fornita dalle strutture sanitarie e socio-sanitarie sia pubbliche che private, anche al fine di prevenire, ridurre ed eliminare i rischi operativi e finanziari in ambito sanitario.

L'esperienza nonché le specifiche competenze tecniche e manageriali nella gestione operativa dei rischi in ambito sanitario, ed in particolare nell'ambito della sicurezza delle informazioni e *privacy* hanno reso Scudomed un leader nel settore, tanto da essere riconosciuta presso il Ministero dello Sviluppo Economico come associazione professionale ai sensi della Legge n. 4 del 2013, autorizzata a rilasciare attestati di qualificazione professionale dei servizi prestati nell'ambito della gestione dei rischi (artt. 4, 7 e 8 della Legge n. 4/2013), https://www.mise.gov.it/index.php/it/mercato-e-consumatori/professioni-non-organizzate/associazioni-che-rilasciano-attestato-di-qualita;

- l'Azienda Sanitaria Locale della provincia di Bari, principale polo sanitario della Regione Puglia, ha interesse affinché Scudomed la supporti nell'individuazione delle corrette procedure aziendali inerenti alle attività di cui l'Associazione è *leader*, anche, e soprattutto, alla luce degli obiettivi perseguiti dal Piano Nazionale di Ripresa e Resilienza. Tale piano ha evidenziato l'importanza, per le strutture sanitarie, di poter contare su un adeguato sfruttamento delle tecnologie più avanzate, su elevate competenze digitali, professionali e manageriali, su nuovi processi per l'erogazione delle prestazioni e delle cure e su un più efficace collegamento fra la ricerca, l'analisi dei dati, i processi trattamentali sanitari e la loro programmazione a livello di sistema;
- una corretta gestione del rischio sanitario, la conoscenza dei principi in tema di *data protection*, l'analisi della maturità digitale dell'organizzazione aziendale e la consapevolezza delle responsabilità derivanti da eventuali violazioni di sicurezza si rendono necessarie anche alla luce degli obiettivi perseguiti dalla riforma che interesserà il Servizio Sanitario Nazionale, la quale mira a rafforzare le prestazioni erogate sul territorio grazie al potenziamento e alla

creazione di strutture e presidi territoriali (come le Case della Comunità e gli Ospedali di Comunità, tra gli altri), al rafforzamento dell'assistenza domiciliare, allo sviluppo della telemedicina e ad una più efficace integrazione con tutti i servizi socio-sanitari attraverso la realizzazione dei Centri Operativi Territoriali (COT). A ciò si aggiungano il completamento e la diffusione del Fascicolo Sanitario Elettronico (FSE), una migliore capacità di erogazione e monitoraggio dei Livelli Essenziali di Assistenza (LEA) attraverso più efficaci e aggiornati sistemi informativi;

- tali tipologie di attività impattano inevitabilmente sui rischi connessi all'attività sanitaria rendendo, conseguentemente, necessaria la relativa loro identificazione e valutazione e la successiva gestione, mitigazione ed eliminazione;
- tale rivoluzione digitale sta portando e porterà, altresì, ad un mutamento nella gestione della sicurezza delle informazioni. Si è passati, infatti, da un atteggiamento conservativo, volto a proteggere informazioni in un contesto "chiuso", come la documentazione cartacea archiviata nei locali dell'Azienda o di terzi conservatori, ad un approccio dinamico, volto a gestire in modo "aperto" i flussi informativi, con la necessità che l'Azienda attui una continua vigilanza ed un aggiornamento costante e proattivo nell'affrontare le problematiche di sicurezza;
- pertanto, non si può prescindere dall'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), volto alla predisposizione ed effettiva adozione di un reticolato di procedure estrapolate anche da norme volontarie internazionali che possano garantire la riservatezza, l'integrità e la disponibilità delle informazioni dell'Azienda;
- alla luce di quanto precede, l'ASL Bari intende avvalersi delle competenze, dell'esperienza e della professionalità di Scudomed al fine di comprendere meglio il suo contesto interno ed esterno prima di avviare i processi di necessario adeguamento in vista del raggiungimento degli obiettivi di efficienza e innovazione digitale nel campo sanitario, così come anche inseriti dal Piano Nazionale di Ripresa e Resilienza.

Tutto ciò premesso, le Parti stipulano e convengono le seguenti condizioni:

Art. 1 – Premesse

Le premesse costituiscono parte integrante del presente contratto.

Art. 2 – Finalità

Le Parti stipulano il presente Protocollo al fine condiviso di incentivare la diffusione della cultura digitale mediante la promozione di una maggiore attenzione ai temi della sicurezza informatica.
Le Parti, in particolare, intendono cooperare al fine di creare una maggiore consapevolezza nell'uso delle tecnologie e nel ricorso alla sicurezza informatica, attraverso la pianificazione e la realizzazione di iniziative mirate a contrastare minacce informatiche, fornendo adeguato supporto e assistenza in caso di attacchi informatici.

Le Parti opereranno nel rispetto di quanto previsto in materia dalle Istituzioni nazionali preposte alla sicurezza informatica e, laddove ne ravvisino l'opportunità, potranno estendere la partecipazione alle attività oggetto del presente Protocollo ad altri soggetti che ne siano interessati, al fine di ottenere la massima valorizzazione dei risultati pianificati.

Art. 3 – Oggetto del contratto

ASL Bari e Scudomed svolgeranno congiuntamente e nell'esclusivo interesse di Asl Bari un'attività di analisi dei principali *asset* tecnico-organizzativi aziendali finalizzata all'innalzamento dei livelli di sicurezza fisica e digitale di uso corrente, in ossequio alle buone pratiche/procedure/policy disponibili.

Lo scopo condiviso è quello in base al quale l'azienda potrà migliorare il fronte tecnico-organizzativo sotto il profilo della prevenzione degli attacchi *cyber* e accompagnare l'Azienda nella definizione di un *framework* in materia di sicurezza delle informazioni, in armonia con la normazione di riferimento.

Più specificamente, le Parti svolgeranno congiuntamente attività di analisi dell'"*as is*" tecnico-organizzativo che prenderà in considerazione la componente *HR*, le politiche e le procedure aziendali in atto, nonché gli *asset* utilizzati, nei processi di diagnosi e cura, per la finalizzazione della più corretta integrazione tra quanto esistente e i processi innovativi di *digital health* per la presa in carico di pazienti e/o utenti nell'ambito territoriale di competenza dell'Azienda.

Detta analisi sarà conclusa attraverso un documento proiettivo del "*to be*" da concepirsi secondo una logica *by design* e *risk based*, dovendo prestare particolare attenzione ai profili della sicurezza delle informazioni e alla *cyber* sicurezza, senza trascurare i principi e le finalità esistenti in ambito privacy,

condizioni necessarie per una piena messa in *compliance* abilitativa ai processi di innesto con le nuove tecnologie.

Scudomed, all'esito delle attività di *assessment* in parola, indicherà alla ASL Bari le modalità di strutturazione dei migliori ed opportuni modelli di *compliance*, anche in applicazione del *framework* in materia di *cyber security* e protezione cibernetica, per la finalizzazione della più corretta implementazione di *policy* e procedure aziendali, oltre che di messa a terra di misure di sicurezza tecniche ed organizzative adeguate nell'ambito della prevenzione del rischio nel particolare contesto trattamentale.

Le suddette operazioni porteranno all'individuazione di corrette procedure aziendali volte a ridurre il rischio di attacchi hacker e a gestire correttamente l'eventuale verificarsi degli stessi e confluiranno in un apposito documento: "Procedura aziendale per la Cybersecurity" che andrà ad integrare, per quanto attiene alla specifica fattispecie, quanto già previsto nella "Procedura Aziendale per la Gestione delle Violazioni di Dati Personali (Data Breach)".

Scudomed, anche attraverso l'opera di suoi *partners* tecnologici, eseguirà preliminarmente un Vulnerability Assessment, avente l'obiettivo di far emergere potenziali vulnerabilità dell'infrastruttura, della rete IT e degli applicativi web e non.
Il Vulnerability Assessment si concluderà con la redazione, da parte di Scudomed, del Remediation Plan, ossia un report contenente un elenco dettagliato e completo delle vulnerabilità rilevate e della gravità delle medesime con riferimento alle esigenze e specificità aziendali. L'obiettivo di tale report è ridurre e, ove possibile, eliminare i rischi che potrebbero scaturire da un eventuale sfruttamento dei punti deboli presenti.
A seguito dell'attuazione del Remediation Plan da parte della ASL Bari, Scudomed procederà ad un nuovo Vulnerability Assessment per accertare che siano state adottate tutte le contromisure necessarie a correggere le vulnerabilità precedentemente rilevate; in caso si rilevino ancora mancanze, si procederà per miglioramenti successivi.
Dopo aver messo in atto tutte le misure di sicurezza per rimuovere i punti deboli, Scudomed, anche attraverso l'opera dei suoi *partners* tecnologici, eseguirà un Penetration Test, inteso come una vera e propria simulazione di attacco informatico, al fine di misurare il grado di efficacia ed efficienza di quanto implementato, a seguito delle attività scaturite dal o dai Vulnerability Assessment.

Il Penetration Test, a differenza del Vulnerability Assessment, avrà l'obiettivo di mostrare concretamente come un attacco cyber potrebbe eludere la sicurezza attraverso le falle del sistema. Scudomed, a seguito del Penetration Test, sottoporrà all'attenzione dell'ASL di Bari un documento analitico di quanto riscontrato. Quest'ultimo, in ottica di sicurezza proattiva, dovrà proporre anche delle best practice per reagire in modo efficace agli attacchi hacker, al fine di contenere i danni diretti e indiretti e minimizzare il più possibile il tempo di ripristino dell'infrastruttura.

Scudomed indicherà all'ASL di Bari come dotarsi di efficaci strumenti di sicurezza predittiva, in modo da poter ricevere early warning relativi alle principali minacce presenti sul web, sul deepweb e sul darkweb.

Scudomed ed ASL Bari redigeranno un apposito documento: "Procedura aziendale per la Cybersecurity" che andrà ad integrare, per quanto attiene alla specifica fattispecie, quanto già previsto nella "Procedura Aziendale per la Gestione delle Violazioni di Dati Personali (Data Breach)". Detto documento descriverà le modalità operative adottate dall'ASL Bari per fronteggiare in modo efficace ed efficiente gli attacchi hacker, al fine di contenere i danni diretti e indiretti e minimizzare il più possibile il tempo di ripristino dell'infrastruttura e dei sistemi aziendali.

Art. 4 – Modalità di svolgimento dell'incarico

Tali attività verranno svolte prevalentemente attraverso un sistema di *audit* da remoto finalizzati alla comprensione del contesto interno ed esterno all'ente oppure *on site* ad insindacabile parere di Scudomed. Le attività verranno pianificate e schedulate attraverso un SPOC (single point of contact – ovvero un referente di progetto che sarà messo a disposizione dell'azienda) e svolte da remoto od *on site* (ad insindacabile giudizio di Scudomed) secondo un calendario bimestrale che verrà condiviso tra le parti.

All'esito di ogni *audit*, Scudomed sarà tenuta ad informare l'azienda attraverso opportuna reportistica.

Scudomed presterà la sua opera in piena autonomia giuridica e organizzativa, anche avvalendosi di professionisti esperti nella particolare materia riferita all'oggetto del presente Protocollo ed alle azioni in esso previste.

Art. 5 – Referenti del Protocollo d'Intesa – Comitato dei Referenti

Le parti, per la gestione ed il coordinamento delle attività oggetto del presente Protocollo, designano i seguenti referenti:

Rappresentanti della ASL di Bari:

Avv. Luigi Fruscio – Direttore Amministrativo ASL Bari

Avv. Elisabetta Fortunato – DPO ASL Bari

Dott.ssa Marialessandra Nacucchi – Staff Direzione Strategica ASL Bari

Prof. Giuseppe Pirlo – Professore Ordinario di Sistemi di Elaborazione delle Informazioni presso l'Università degli Studi di Bari "Aldo Moro" - in qualità di esperto della materia

Rappresentanti della SCUDOMED – Health Risk Manager e Legal Advisor

Avv. Massimiliano Parla - Presidente Nazionale di Scudomed – Health Risk Manager e Legal Advisor

Ai referenti è demandato il compito di coordinare le azioni intraprese dal proprio Ente di appartenenza con quelle poste in essere dall'altra Parte, al fine di raggiungere una maggiore efficacia e una migliore efficienza degli sforzi profusi.

I suddetti referenti dovranno, a tal fine, individuare e promuovere, con cadenza periodica, le fasi e le modalità di attuazione del presente Protocollo d'intesa, nonché monitorarne i risultati e approvare, in relazione agli obiettivi specifici, il piano annuale delle attività.

Alle riunioni del Comitato dei referenti, le Parti potranno invitare, di volta in volta, esperti anche esterni, sulla base degli argomenti presenti all'ordine del giorno.

Il Comitato ha durata biennale, in coincidenza con la durata del protocollo di intesa di cui trattasi. La partecipazione al Comitato non comporta oneri né alcun tipo di spese, ivi compresi compensi o gettoni di presenza, salari, provvigioni, emolumenti, indennità o altri benefici, comunque denominati.

Le riunioni del Comitato tecnico scientifico possono essere effettuate anche in modalità telematica.

Art. 6 – Obblighi delle parti

Scudomed si impegna a svolgere l'incarico secondo i principi di onestà, trasparenza, correttezza e diligenza che la natura delle attività richiedono.

L'Asl Bari si impegna a rendere possibili le attività che saranno condotte da Scudomed mettendo a disposizione le risorse umane e i mezzi necessari al buon andamento e svolgimento dell'incarico affidatogli.

Art. 7 – Durata e Recesso

Il presente Protocollo d'intesa ha la durata di due anni a decorrere dal momento della sottoscrizione delle Parti, e potrà essere rinnovato, con apposito atto scritto, per una ulteriore annualità.

Ciascuna delle Parti ha facoltà di recedere dal presente Protocollo in qualsiasi momento, previa comunicazione scritta da inviare, mezzo PEC, all'altra Parte, con un preavviso di trenta giorni e senza alcuna penale o onere di qualsivoglia natura, ferme restando le spese eventualmente sostenute da Scudomed per le attività svolte in favore dell'Azienda sino al momento del recesso.

Art. 8 – Rimborso spese

Le attività di cui al presente Protocollo saranno rese da SCUDOMED a titolo gratuito senza ulteriori oneri a carico del bilancio aziendale.

L'ASL Bari riconoscerà alla SCUDOMED un rimborso delle spese vive, strettamente connesse allo svolgimento di cui al presente Protocollo, quantificato, in maniera forfettaria, in un importo omnicomprensivo pari ad € 10.000,00 annui, oltre IVA come per legge.

Art. 9 – Riservatezza

Le parti si impegnano ad adottare tutte le misure adeguate allo stato dell'arte per mantenere la segretezza e assicurare di non rilevare a terzi il contenuto di tutte le informazioni o dati forniti e/o di cui le stesse entrano a conoscenza nell'ambito delle attività di cui al presente contratto, ivi inclusi – a titolo esemplificativo e non limitativo – idee, materiali vari, documenti in qualsiasi formato anche elettronico, prodotti di qualsiasi genere, nonché qualsiasi informazione relativa a processi, procedure interne e/o quelle adottate.

Art. 10 – Controversie e foro competente

Le Parti si impegnano a risolvere amichevolmente tutte le controversie che dovessero eventualmente insorgere tra loro in dipendenza del presente Protocollo. In mancanza di composizione amichevole, tutte le controversie comunque derivanti dal presente Protocollo saranno deferite, in via esclusiva, alla competenza del Foro di Bari. Non è ammessa la competenza arbitrale. Il presente Protocollo è regolato dal diritto italiano. Per quanto non espressamente previsto dal presente Protocollo si fa riferimento alle norme del codice civile e ad ogni altra disposizione normativa in materia.

Art. 11 – Trattamento dei dati personali

Le parti prendono atto che, nel corso dell'esecuzione del presente contratto, anche in sede precontrattuale, potrebbero entrare in possesso di informazioni personali riguardanti dipendenti, amministratori, funzionari, altri rappresentanti dell'altra Parte ("Dati dei Contatti Business") e gli interessati in generale.

Ai sensi del Regolamento UE 2016/679 (GDPR) e del D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018 (Codice Privacy), le Parti tratteranno i dati suddetti esclusivamente per finalità connesse al presente contratto, tra cui l'esecuzione e la tenuta del rapporto contrattuale, finalità amministrativo-contabili e l'esecuzione di obblighi di legge.

Scudomed, nell'ambito delle attività del presente contratto, si impegna altresì a sottoscrivere apposita nomina a Responsabile del trattamento ex art. 28 GDPR.

****

Le Parti si danno reciprocamente atto che quanto sopra convenuto è frutto di libera negoziazione tra le medesime intervenuta, non essendosi fatto ricorso a moduli, formulari e/o condizioni generali di contratto, con la conseguenza che risultano inapplicabili gli artt. 1341 e 1342 del Codice Civile.

Le parti sottoscrivono il presente accordo in duplice copia originale e composta da nr. 13 pagine.

Letto, confermato e sottoscritto a Roma-Bari il 3 ottobre 2022

Scudomed Health Risk Manager e Legal Advisor
Il Presidente Nazionale

Azienda Sanitaria Locale della provincia di Bari
Il Direttore Generale

PROFILI CONTABILI

☒ RILEVANTE, a valere su: ☐ NON rilevante

Conto Economico/Patrimoniale	Anno	Importo
7331050050 -	2022	10.000,00
7331050050 -	2023	10.000,00

☐ CONTIENE liquidazione ☒ NON Contiene Liquidazione

ONERI DI PUBBLICAZIONE OBBLIGATORIA EX D. LGS. 33/2013:

☒ SOGGETTA a pubblicazione ☐ NON soggetta a pubblicazione

Sottosezione di Primo LIvello	Sottosezione di Secondo LIvello	Riferimento Normativo
Provvedimenti	Provvedimenti organi indirizzo politico	Art. 23, c. 1, d.lgs. n. 33/2013 /Art. 1, co. 16 della l. n. 190/2012

ONERI DI RISERVATEZZA:

☐ CONTIENE dati personali da NON pubblicare ☒ NON contiene dati personali

DESTINATARI NOTIFICA/TRASMISSIONE

Area Gestione Risorse Finanziarie	

PROPOSTA N.RO 20220003124 APPROVATA CON DELIBERAZIONE N.RO 20220001901 DEL 06/10/2022

Con la sottoscrizione in calce al presente provvedimento, i firmatari di cui sopra, ciascuno in relazione al proprio ruolo come indicato e per quanto di rispettiva competenza, attestano che il procedimento istruttorio è stato espletato nel rispetto della normativa regionale e nazionale applicabile e che il provvedimento predisposto è conforme alle risultanze istruttorie agli atti d'ufficio.

I medesimi soggetti dichiarano, inoltre, di non versare in alcuna situazione di conflitto di interesse, anche potenziale, ex art. 6-bis, l. 241/90, artt. 6, 7 e 13, c. 3, D.P.R. 62/2013, vigente codice di comportamento aziendale (DDG n. 132/2019) e art. 1, c. 9, lett. e), l. 190/2012 – quest'ultimo come recepito, a livello aziendale, alla Parte II, par. 1, lett. c) del vigente PTPCT – tale da pregiudicare l'esercizio imparziale di funzioni e compiti attribuiti, in relazione al procedimento indicato in oggetto, così come di non trovarsi in alcuna delle condizioni di incompatibilità di cui all'art. 35-bis, D.L.gs. 165/2001.

RUOLO	NOME E COGNOME	FIRMA
Responsabile UOS/UOSD	Fortunato Elisabetta	*Firmato digitalmente il 04/10/2022 11:31*
Direttore/Responsabile di Struttura	Fruscio Luigi	*Firmato digitalmente il 04/10/2022 12:01*