

DELIBERAZIONE DEL DIRETTORE GENERALE

N. DEL

Il Direttore Generale dell'Azienda U.L.S.S. n. 9 SCALIGERA, dott. Pietro Girardi, nominato con D.P.G.R.V. n. 23 del 28/02/2026, coadiuvato dai Direttori:

- dott. Flavia Dal Bosco	Direttore Amministrativo
- dott. Viviana Coffele	Direttore Sanitario
- dott. Felice Alfonso Nava	Direttore dei Servizi Socio-Sanitari

ha adottato in data odierna la presente deliberazione:

OGGETTO

PROGRAMMA DI SCREENING DEL TUMORE DEL COLON-RETTO. RINNOVO ACCORDO TRA L'AZIENDA ULSS 9 SCALIGERA E L'IRCCS OSPEDALE SACRO CUORE DON CALABRIA DI NEGRAR DI VALPOLICELLA PER L'EFFETTUAZIONE DI PRESTAZIONI DI COLONSCOPIA DI SECONDO LIVELLO.

Note per la trasparenza: Con il presente provvedimento si intende rinnovare l'accordo di collaborazione tra l'Azienda Ulss 9 Scaligera e l'IRCCS Ospedale Sacro Cuore Don Calabria di Negrar di Valpolicella per l'effettuazione, all'interno del Programma di screening del tumore del colon-retto dell'Azienda ULSS 9 Scaligera, di prestazioni di colonscopia di secondo livello, nel periodo 01.07.2026 – 30.06.2027.

Il Direttore di Dipartimento di Prevenzione

riferisce quanto segue:

Premesso che:

-con D.G.R. n. 528 del 15.06.2001 la Regione Veneto ha previsto che "al Dipartimento di Prevenzione delle Aziende Sanitarie afferisca tutto il complesso delle attività di prevenzione collettiva", sia per motivi di opportunità, ma soprattutto per affrontare unitariamente le problematiche connesse ai rischi della salute e conseguentemente fornire risposte uniformi ai bisogni della popolazione;

- con D.G.R. n. 2605 del 07.08.2007 la Regione Veneto ha ritenuto necessario che tutte le Aziende ULSS provvedano all'unificazione della funzione di organizzazione e di valutazione dei tre programmi di screening, cervice uterina, mammella e colon retto, affidandone la regia ai Dipartimenti di Prevenzione di ciascuna Azienda, al fine di ottenere migliori risultati in termini di efficienza e di economie di scala;

- con D.P.C.M. 12.01.2017 "Definizione e aggiornamento dei livelli essenziali di assistenza, di cui all'articolo 1, comma 7, del decreto legislativo 30.12.1992, n. 502" gli screening oncologici effettuati nell'ambito di programmi organizzati di diagnosi precoce e prevenzione collettiva sono stati classificati L.E.A.;

Preso atto che:

- con D.G.R. n. 760 del 14.05.2015, avente oggetto "Prevenzione e diagnosi precoce dei tumori: prime indicazioni di riordino dei programmi di screening oncologici regionali ai sensi del D.Lgs. 29.4.1998, n. 124 e delle prestazioni specialistiche e di diagnostica strumentale e di laboratorio erogate ai sensi dell'art. 85, comma 4, della legge 23.12.2000, n. 388", la Regione Veneto provvede all'assorbimento dello screening spontaneo nei programmi di screening del carcinoma della cervice uterina, della mammella e del colon retto effettuati presso le Aziende ULSS e al superamento del doppio regime di erogazione delle prestazioni al fine di incrementare la copertura, la qualità e l'efficienza dell'offerta di prestazioni per la prevenzione secondaria e la diagnosi precoce dei tumori;

Precisato che:

- l'allegato A della D.G.R.V. n. 760/2015, punto 6, prevede, tra l'altro, che eventuali erogatori di prestazioni connessi ai programmi di screening oncologici saranno oggetto di specifici accordi e dovranno inoltre essere integrati con il programma di

Il Proponente: Il Direttore Dipartimento di Prevenzione dott. Alessandra De Salvia

screening aziendale sia dal punto di vista organizzativo che informatico e pertanto tenuti a fornire al programma di screening copia della documentazione sanitaria richiesta. In questo caso la prestazione non sarà oggetto di prescrizione su ricetta del SSR ma sarà remunerata a fatturazione diretta tra l'Azienda richiedente e l'erogatore;

- le prestazioni sopra citate non saranno oggetto di recupero crediti in caso di mancata disdetta entro i tempi previsti o di mancata presentazione dell'utente, essendo gli accertamenti diagnostici previsti dal programma di screening del tumore del colon-retto esenti dalla compartecipazione alla spesa sanitaria per la popolazione.

Vista la Deliberazione n. 487 del 01.07.2021, con cui si approvava l'accordo di collaborazione tra l'Azienda ULSS 9 Scaligera e l'IRCCS Ospedale Sacro Cuore Don Calabria di Negrar di Valpolicella, per l'esecuzione di prestazioni legate al programma di screening del tumore del colon-retto, rinnovato da ultimo con Deliberazione n. 845 del 04.07.2025 con validità dall'01.07.2025 al 30.06.2026.

Preso atto che con nota prot. n. 0187271 del 13.05.2026 si acquisisce la disponibilità dell'IRCCS Ospedale Sacro Cuore Don Calabria di Negrar di Valpolicella a continuare ad effettuare le prestazioni oggetto del presente atto, di seguito dettagliate, con una riduzione del 15% rispetto alle tariffe previste dal vigente Nomenclatore Tariffario Regionale.

Considerato opportuno mantenere un ulteriore canale di erogazione di prestazioni di secondo livello dello screening colon-rettale, al fine di facilitare l'accesso a tali prestazioni, in particolare all'utenza della zona della Valpolicella e della Lessinia.

Stimato il numero medio di prestazioni annue che i presidi sanitari pubblici dell'Azienda ULSS 9 Scaligera non sono attualmente in grado di soddisfare, nonché il relativo costo, come di seguito indicato:

Prestazione	Codice	Tariffa	Tariffa scontata (15%)	Numero (stima)	Totale
Sedazione cosciente	99.29.A	19,00 €	16,15 €	400	6.460,00 €
Colonscopia con endoscopio flessibile	45.23	120,00 €	102,00 €	400	40.800,00 €
Biopsia sede multipla intestino crasso	45.25.1	90,95 €	77,31 €	40	3.092,30 €
Polipectomia endoscopica intestino Crasso	45.42	117,05 €	99,49 €	240	23.878,20 €
Ist. app. digerente: Bio endoscopica	91.41.8	42,30 €	35,96 €	40	1.438,20 €
Ist. app. digerente: Polipect.endoscopica	91.41.9	42,30 €	35,96 €	240	8.629,20 €
Rettosigmoidoscopia	45.24	47,40 €	40,29 €	10	402,90 €
Biopsia sede unica in corso di rettosigmoidoscopia	45.25.2	64,95 €	55,21 €	1	55,21€
Totale complessivo					84.756,01 €

Specificato che il numero massimo di prestazioni annue potrà essere oggetto di rimodulazione in funzione della dinamica della capacità produttiva dei presidi sanitari pubblici.

Considerato che, del costo complessivo massimo presunto pari ad € 84.756,01 derivante dal presente provvedimento, sarà tenuto conto in sede di predisposizione del Bilancio economico preventivo e budget generale generale anno 2026 (Euro 42.405,61) e anno 2027 (Euro 42.350,40) con disponibilità ad ordinare e da registrare al conto BA1530D1 (B.2.A.16.4.4) Altri servizi sanitari da privato – ALTRO.

Ritenuto opportuno:

- rinnovare l'accordo di collaborazione tra l'Azienda ULSS 9 Scaligera e l'IRCCS Ospedale Sacro Cuore Don Calabria di Negrar di Valpolicella, con decorrenza dal 01.07.2026 fino al 30.06.2027, parte integrante e sostanziale del presente provvedimento, per l'effettuazione all'interno del Programma di screening del tumore del colon-retto dell'Azienda ULSS 9 Scaligera, di prestazioni di colonscopia di secondo livello;

- delegare il Direttore del Dipartimento di Prevenzione alla stipula della dell'accordo oggetto del presente provvedimento;
- proporre il Direttore del Dipartimento di Prevenzione quale responsabile dell'esecuzione del presente provvedimento per quanto di competenza;

Visto il D.lgs. 30.12.1992, n. 502 e successive modifiche ed integrazioni;

Viste le LL.RR. 14.09.1994 nn. 55 e 56 e successive modifiche ed integrazioni;

Vista la L.R. n. 19 del 25.10.2016.

IL DIRETTORE GENERALE

Vista l'attestazione del Direttore del Dipartimento di Prevenzione dell'avvenuta regolare istruttoria del provvedimento anche in ordine alla compatibilità con la vigente legislazione regionale e nazionale, sia alla sua conformità alle direttive e regolamentazioni aziendali;

Acquisito agli atti il parere favorevole del Direttore Amministrativo, del Direttore Sanitario nonché del Direttore dei Servizi Socio-Sanitari, per quanto di competenza;

DELIBERA

- 1) di rinnovare l'accordo di collaborazione, con decorrenza dal 01.07.2026 fino al 30.06.2027, allegato al presente provvedimento quale parte integrante e sostanziale, tra l'Azienda ULSS9 Scaligera e l'IRCCS Ospedale Sacro Cuore Don Calabria di Negrar di Valpolicella per l'effettuazione, all'interno del programma di screening del tumore del colon-retto dell'Azienda ULSS 9, di un massimo di prestazioni annue, proporzionate ai mesi di operatività dell'accordo, come di seguito indicato ed erogate senza oneri a carico dell'assistito:

Prestazione	Codice	Tariffa	Tariffa scontata (15%)	Numero (stima)	Totale
Sedazione cosciente	99.29.A	19,00 €	16,15 €	400	6.460,00 €
Colonscopia con endoscopio flessibile	45.23	120,00 €	102,00 €	400	40.800,00 €
Biopsia sede multipla intestino crasso	45.25.1	90,95 €	77,31 €	40	3.092,30 €
Polipectomia endoscopica intestino Crasso	45.42	117,05 €	99,49 €	240	23.878,20 €
Ist. app. digerente: Bio endoscopica	91.41.8	42,30 €	35,96 €	40	1.438,20 €
Ist. app. digerente: Polipect.endoscopica	91.41.9	42,30 €	35,96 €	240	8.629,20 €
Rettosigmoidoscopia	45.24	47,40 €	40,29 €	10	402,90 €
Biopsia sede unica in corso di rettoidoscopia	45.25.2	64,95 €	55,21 €	1	55,21 €
Totale complessivo					84.756, 01 €

- 2) di specificare che il massimo di prestazioni annue di cui al punto 1 potrà essere oggetto di rimodulazione in funzione della dinamica della capacità produttiva dei presidi sanitari pubblici;
- 3) di specificare che eventuali ulteriori esigenze relative a prestazioni non ricomprese al punto 1) saranno oggetto di successiva valutazione ed eventuale integrazione dell'accordo oggetto del presente provvedimento;
- 4) di delegare il Direttore del Dipartimento di Prevenzione alla stipula dell'accordo di collaborazione, oggetto del presente provvedimento e di tutti gli atti inerenti e conseguenti, come da deliberazione n. 288 del 03/03/2026;
- 5) di designare il Direttore del Dipartimento di Prevenzione quale responsabile dell'esecuzione del presente

Il Proponente: Il Direttore Dipartimento di Prevenzione dott. Alessandra De Salvia

provvedimento per quanto di competenza;

6) di prendere atto che del costo complessivo massimo presunto pari ad € 84.756,01 derivante dal presente provvedimento sarà tenuto conto in sede di predisposizione del Bilancio economico preventivo e budget generale generale anno 2026 (Euro 42.405,61) e anno 2027 (Euro 42.350,40) con disponibilità ad ordinare e da registrare al conto BA1530D1 (B.2.A.16.4.4) Altri servizi sanitari da privato – ALTRO.

Il Direttore Sanitario
dott. Viviana Coffele

Il Direttore Amministrativo
dott. Flavia Dal Bosco

Il Direttore dei Servizi Socio-Sanitari
dott. Felice Alfonso Nava

IL DIRETTORE GENERALE
dott. Pietro Girardi

ACCORDO DI COLLABORAZIONE PER L'EFFETTUAZIONE DI PRESTAZIONI DI COLONSCOPIA DI
SECONDO LIVELLO NEL PROGRAMMA DI SCREENING DEL TUMORE DEL COLON-RETTO

TRA

AZIENDA U.L.S.S. 9 Scaligera, con sede in Verona, Via Valverde 42, C.F. e P.IVA n. 02573090236, d'ora innanzi denominata AULSS 9, in persona del Direttore del Dipartimento di Prevenzione, Dott.ssa Alessandra De Salvia, giusta deliberazione di incarico n. 174 del 14.02.2025, a ciò delegata dal Direttore Generale con deliberazione n. 288 del 03/03/2026;

E

IRCCS Ospedale Sacro Cuore Don Calabria, con sede in Negrar di Valpolicella (VR) Via Don A. Sempredoni n. 5, C.F. e P.IVA n. 00280090234, nella persona dell'Amministratore Delegato, Dott. Claudio Cracco, il quale dichiara, consapevole delle responsabilità previste dall'art.76 del D.P.R. 455/2000, di non essere stato condannato con provvedimento definitivo (inclusi sentenza pronunciata a seguito di applicazione della pena su richiesta delle parti, decreto penale di condanna) per reati che comportano l'incapacità di contrarre con la Pubblica Amministrazione;

PREMESSO CHE:

- con D.G.R. n. 528 del 15.06.2001 la Regione Veneto ha previsto che *“al Dipartimento di Prevenzione delle Aziende Sanitarie afferisca tutto il complesso delle attività di prevenzione collettive”*, motivando tale scelta organizzativa sia per motivi di opportunità, ma soprattutto per affrontare unitariamente le problematiche connesse ai rischi della salute e conseguentemente fornire risposte uniformi ai bisogni della popolazione;
- con D.G.R. n. 2605 del 07.08.2007 la Regione Veneto ha ritenuto necessario che tutte le Aziende ULSS provvedano all'unificazione della funzione di organizzazione e di valutazione dei tre programmi di screening, affidandone la regia ai Dipartimenti di Prevenzione di ciascuna Azienda, al fine di ottenere migliori risultati in termini di efficienza e di economie di scala;
- con D.G.R. n. 760 del 14.05.2015, avente oggetto *“Prevenzione e diagnosi precoce dei tumori: prime indicazioni di riordino dei programmi di screening oncologici regionali ai sensi del D.Lgs. n. 29.4.1998, n. 124 e delle prestazioni specialistiche e di diagnosi strumentale e di laboratorio erogate ai sensi dell'art. 85, comma 4, della legge 23.12.2000, n. 388”*, la Regione Veneto provvede all'assorbimento dello screening spontaneo nei programmi di screening del carcinoma della cervice uterina, della mammella e del colon effettuati presso le Aziende ULSS e al superamento del doppio regime di erogazione delle prestazioni al fine di incrementare la copertura, la qualità e l'efficienza dell'offerta di prestazioni per la prevenzione secondaria e la diagnosi precoce dei tumori;
- all'allegato A della medesima D.G.R. , punto 6, è previsto, tra l'altro, che eventuali erogatori di prestazioni connessi ai programmi di screening oncologici, saranno oggetto di specifici accordi e dovranno, inoltre, essere integrati con il programma di screening aziendale, sia dal punto di vista organizzativo che informatico e, pertanto, tenuti a fornire al programma di screening copia della documentazione sanitaria richiesta. In questo caso la prestazione non sarà oggetto di prescrizione su ricetta del SSR ma sarà remunerata a fatturazione diretta tra

l'Azienda richiedente e l'erogatore;

- con D.P.C.M. 12.01.2017 "Definizione e aggiornamento dei livelli essenziali di assistenza, di cui all'articolo 1, comma 7, del decreto legislativo 30.12.1992, n. 502" gli screening oncologici effettuati nell'ambito di programmi organizzati di diagnosi precoce e prevenzione collettiva sono classificati L.E.A.

Tutto ciò premesso e ritenuto parte integrante del presente accordo

SI CONVIENE E SI STIPULA QUANTO SEGUE:

ART. 1 – Oggetto

L'IRCCS Ospedale Sacro Cuore Don Calabria assicura, compatibilmente con la propria attività istituzionale, l'effettuazione, all'interno del programma di screening del tumore del colon-retto di AULSS 9, un massimo di prestazioni annue, proporzionate ai mesi di operatività dell'accordo, come di seguito indicato ed eroga senza oneri a carico dell'assistito:

Prestazione	Codice	Tariffa	Tariffa scontata (15%)	Numero (stima)	Totale
Sedazione cosciente	99.29.A	19,00 €	16,15 €	400	6.460,00 €
Colonscopia con endoscopio flessibile	45.23	120,00 €	102,00 €	400	40.800,00 €
Biopsia sede multipla intestino crasso	45.25.1	90,95 €	77,31 €	40	3.092,30 €
Polipectomia endoscopica intestino Crasso	45.42	117,05 €	99,49 €	240	23.878,20 €
Ist. app. digerente: Bio endoscopica	91.41.8	42,30 €	35,96 €	40	1.438,20 €
Ist. app. digerente: Polipect.endoscopica	91.41.9	42,30 €	35,96 €	240	8.629,20 €
Rettosigmoidoscopia	45.24	47,40 €	40,29 €	10	402,90 €
Biopsia sede unica in corso di rettosigmoidoscopia	45.25.2	64,95 €	55,21 €	1	55,21€
Totale complessivo					84.756, 01 €

Tale tetto massimo potrà essere oggetto di rimodulazione in funzione della dinamica della capacità produttiva dei presidi sanitari pubblici.

ART. 2 – Accordi economici

AULSS 9, come corrispettivo per l'esecuzione delle prestazioni di cui all'art. 1 del presente accordo, si impegna a corrispondere ad IRCCS Ospedale Sacro Cuore Don Calabria, i compensi previsti dal vigente Nomenclatore Tariffario Regionale scontati del 15%.

In caso di aggiornamento del Nomenclatore Tariffario Regionale le tariffe specificate nell'art. 1 saranno automaticamente allineate alle nuove tariffe previste, alle quali sarà sempre applicato lo sconto del 15%.

L'IRCCS Ospedale Sacro Cuore Don Calabria provvede all'emissione di fattura mensile a consuntivo per l'attività oggetto del presente accordo.

ART. 3 – Trasmissione documentazione

L'IRCCS Ospedale Sacro Cuore Don Calabria si impegna a coordinarsi per l'attività oggetto del presente accordo con il programma di screening aziendale di AULSS 9 sia dal punto di vista organizzativo che informatico; L'IRCCS Ospedale Sacro Cuore Don Calabria è pertanto tenuto a fornire all'U.O.S.D. Servizio di Epidemiologia, Prevenzione MCNT, Screening e Promozione della Salute – Area Funzionale Screening Oncologici – di AULSS 9, con congruo anticipo, agende dedicate almeno trimestrali, oltre a copia della documentazione sanitaria prodotta (copia dei referti delle prestazioni erogate, modulistica conclusioni secondo livello ed eventuale modulo chirurgia di terzo livello predisposta dal programma di screening) per le prestazioni di cui all'art. 1, nonché la reportistica necessaria ai fini della rendicontazione dell'attività ai competenti enti regionali, secondo le tempistiche concordate con all'U.O.S.D. Servizio di Epidemiologia, Prevenzione MCNT, Screening e Promozione della Salute di AULSS 9.

Inoltre, le prestazioni di cui all'art. 1 del presente accordo saranno inserite direttamente dall'IRCCS Ospedale Sacro Cuore Don Calabria nel flusso SPS con codice 12 per la tipologia di erogazione, al fine di identificare dette prestazioni come erogate in regime di screening.

Come previsto dalla DGRV n. 760/2015, citata in premessa, la prestazione non sarà oggetto di prescrizione su ricetta del SSR e sarà remunerata a fatturazione diretta, senza oneri a carico dell'assistito.

Le prestazioni di cui all'art. 1, inoltre, non saranno oggetto di recupero crediti in caso di mancata disdetta entro i tempi previsti o di mancata presentazione dell'utente, essendo gli accertamenti diagnostici previsti dal programma di screening del tumore del colon-retto esenti dalla compartecipazione alla spesa sanitaria per la popolazione.

L'IRCCS Ospedale Sacro Cuore Don Calabria trasmetterà al Responsabile dell'U.O.S.D. Servizio di Epidemiologia, Prevenzione MCNT, Screening e Promozione della Salute di AULSS 9 copia della documentazione sanitaria prodotta in formato protetto e il riepilogo mensile delle prestazioni effettuate entro sessanta giorni dalla conclusione del mese di riferimento.

ART. 4 – Privacy

Le parti si danno reciprocamente atto che nell'espletamento dell'attività di cui all'art. 1, dovrà essere garantita la massima riservatezza dei dati personali, con particolare riferimento a quelli idonei a rivelare lo stato di salute, fermo restando che gli operatori coinvolti sono tenuti ad osservare tutte le regole di condotta prescritte dal Regolamento UE 2016/679 e dal D.lgs. 196/2003 così come modificato dal Dlgs. 101/2018, nonché i regolamenti, i protocolli e le procedure adottate dalle rispettive aziende in tema di privacy.

AULSS 9 è titolare del trattamento dei dati di cui al presente accordo di collaborazione, ai sensi dell'art. 4 del Regolamento (UE) 2016/679.

Per le attività oggetto del presente accordo, il trattamento dei dati avverrà inoltre in conformità all' "CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 PARAGRAFO 3) DEL REGOLAMENTO UE N. 2016/679" allegato al presente accordo.

ART. 5 – Durata

Il presente accordo di collaborazione ha validità dall'01.07.2026 al 30.06.2027.

ART. 6 – Inadempimento e recesso

In caso di mancato rispetto di quanto previsto nel presente accordo, la collaborazione potrà essere risolta previa disdetta anche da una sola delle Parti, in qualsiasi momento, a mezzo PEC, con effetto a 30 giorni dal ricevimento.

E' ammesso il recesso dal presente accordo di collaborazione, previa disdetta anche di una sola delle parti, tramite PEC, con effetto a 30 giorni dal ricevimento.

ART. 7 – Norme applicabili

Per tutto quanto non espressamente convenuto nel presente accordo di collaborazione, si fa rinvio alle norme del codice civile.

ART. 8 – Foro competente

Per ogni controversia è competente in via esclusiva il Foro di Verona.

ART. 9 – Disposizioni finali

Agli effetti fiscali le parti dichiarano che trattasi di atto soggetto a registrazione solo in caso d'uso, ai sensi dell'art. 5 della Parte II della Tariffa allegata al D.P.R. 26 aprile 1986, n. 131 e successive modificazioni, a causa ed a spese della parte richiedente.

Le spese di bollo sono assolte da AULSS 9.

L'accordo di collaborazione è sottoscritto dalle parti con firma digitale ai sensi dell'art. 15, comma 2 bis della legge 241/1990 introdotto dall'art. 6 del D.L. 179/2012, convertito in Legge 221/2012.

Il presente accordo si compone di 9 articoli.

Letto, approvato e sottoscritto.

Verona,

IRCCS OSPEDALE
SACRO CUORE DON CALABRIA
L'AMMINISTRATORE DELEGATO
(Dott. Claudio Cracco)

AZIENDA U.L.S.S. 9 SCALIGERA
IL DIRETTORE DIPARTIMENTO
DI PREVENZIONE
(Dott.ssa Alessandra DE SALVIA)

**CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28
PARAGRAFO 3) DEL REGOLAMENTO UE N. 2016/679**

Tra

AZIENDA ULSS 9 SCALIGERA, (P. IVA: 02573090236), con sede legale in Verona, via Valverde, 42, in persona del Responsabile della UOSD Direzione Amministrativa Dipartimento di Prevenzione, Dott.ssa Gessica Martello, delegato dal rappresentante legale dell'Azienda, giusta delega nota prot. n. 93947 del 22/05/2026 confermata con deliberazione n. 299 del 11/03/2026, in qualità di Titolare del trattamento ex artt. 4 n. 7) e 24 del Regolamento UE n. 2016/679 (GDPR) (infra "SCALIGERA" e/o "Titolare del trattamento");

e

IRCCS OSPEDALE SACRO CUORE DON CALABRIA (C.F. e P.IVA n 00280090234), con sede in Negrar di Valpolicella (VR) Via Don A. Sempreboni n. 5, in persona dell'Amministratore Delegato, Dott. Claudio Cracco, in qualità di Responsabile del trattamento ex artt. 4 n. 8) e 28 del GDPR (infra "Responsabile del trattamento" e/o "Fornitore").

Il Titolare ed il Responsabile potranno essere denominati, di seguito, congiuntamente anche come le "Parti".

1. Premesse.

1.1. Le Parti hanno concordemente convenuto, ai sensi dell'art. 28 paragrafo 3) del GDPR, le seguenti clausole contrattuali (infra "Clausole"/"Contratto di nomina" e/o "Contratto") volte a disciplinare la nomina del Fornitore quale Responsabile del trattamento, ad opera di SCALIGERA, nella sua veste di Titolare del trattamento, a fronte dello svolgimento, da parte di quest'ultima, di un processo preventivo di risk assessment¹ volto a valutare e documentare, in un'ottica di accountability ex art. 5 paragrafo 2) del GDPR (e di culpa in eligendo), il grado di affidabilità e di capacità, in capo al Responsabile del trattamento qui nominato, di fornire le garanzie necessarie, idonee ed adeguate a rendere, mediante l'adozione di misure di sicurezza tecniche ed organizzative ex art. 32 del GDPR, conforme il trattamento di specie alla normativa comunitaria e nazionale sulla protezione dei dati personali, ivi incluse le pronunzie e gli atti di cd. soft law emessi sul tema: a tal riguardo, giova precisare che l'onere previsto dall'art. 28 paragrafo 1) e Considerando n. 81) del GDPR è di natura continua, e, dunque, non termina nel momento in cui il Titolare ed il Responsabile del trattamento concludono un contratto o atto giuridico, dato che il primo è tenuto a verificare, ad intervalli appropriati, che il nominato Responsabile del trattamento possieda, in modo costante, le garanzie richieste, anche grazie all'esecuzione di appositi audit o ispezioni, ove appropriato e necessario.

1.2. Nel contesto del contratto/convenzione/accordo ad oggetto: "ACCORDO DI COLLABORAZIONE PER L'EFFETTUAZIONE DI PRESTAZIONI DI COLONSCOPIA DI SECONDO LIVELLO NEL PROGRAMMA DI SCREENING DEL TUMORE DEL COLON-RETTO" sottoscritto tra le Parti in data di cui alla delibera/determina/.. n. del] il Responsabile del trattamento provvede a svolgere, per conto del Titolare, le operazioni di trattamento meglio descritte nell'allegato 1) del presente Contratto di nomina (il quale, assieme ai restanti allegati, costituisce parte integrante del Contratto di nomina medesima), in conformità al Contratto di nomina ed alla normativa

¹ Tale attività di risk assessment viene svolta, in via generale, mediante l'analisi e scambio di una serie di documenti (es. informative ex artt. 13 e 14 del GDPR; termini di servizio; registro delle attività del trattamento ex art. 30 del GDPR; valutazione d'impatto sulla protezione dei dati ex art. 35 del GDPR; policy circa la sicurezza tecnica delle informazioni; certificazioni ottenute; rapporti di soggetti terzi; audit di terze parti). La valutazione, da parte del Titolare del trattamento, circa la sufficienza delle garanzie del Responsabile del trattamento è definibile, in sostanza, come una forma di valutazione del rischio, dipesa, in larga misura, dalla tipologia di trattamento affidato al Responsabile, da valutarsi caso per caso, tenendo conto della natura, portata, contesto e finalità del trattamento, così come i rischi per i diritti e le libertà delle persone fisiche. I seguenti elementi devono essere, in teoria, presi in considerazione dal Titolare del trattamento, al fine di valutare la sufficienza delle garanzie offerte dal Responsabile del trattamento: competenza settoriale e/o tecnica; affidabilità; risorse; reputazione sul mercato; certificazione; codici di condotta, anche di natura settoriale.

comunitaria e nazionale sulla protezione dei dati personali, ivi inclusa la relativa giurisprudenza, dottrina dominante ovvero normativa di secondo livello (soft law).

2. Obblighi del Responsabile del trattamento.

2.1. Fatti salvi gli altri obblighi previsti dalle disposizioni di legge applicabili, ivi inclusi gli atti di soft law ovvero i Provvedimenti ad opera delle competenti Autorità di controllo ovvero di natura giurisdizionale, il Responsabile del trattamento è obbligato a svolgere i seguenti compiti:

- a. Trattare i dati personali sulla base del presente Contratto di nomina, sulla base del rapporto descritto al precedente punto 1.2.) ovvero in ragione di ogni altra istruzione impartita formalmente dal Titolare del trattamento, anche in caso di trasferimento dei relativi dati personali verso un paese terzo (ossia, situato al di fuori del Spazio Economico Europeo (SEE)) o un'organizzazione internazionale, salvo che lo richieda il diritto dell'UE o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento è tenuto ad informare il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- b. Garantire che le proprie persone autorizzate al trattamento ex artt. 4 n. 10), 29 e 32 n. 4) del GDPR – previamente designate per iscritto, e adeguatamente istruite circa l'ambito di attività di trattamento oggetto di tale autorizzazione – si siano impegnate alla riservatezza ovvero abbiano un adeguato obbligo legale di riservatezza²;
- c. Adottare le misure di sicurezza tecniche ed organizzative richieste dall'art. 32 del GDPR (meglio illustrate, seppur in via generale, al relativo allegato 3)), tenuto conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, così come anche il rischio di (varia) probabilità e gravità per i diritti e le libertà delle persone fisiche, onde così assicurare un livello di sicurezza adeguato al rischio associato alle attività di trattamento demandate;
- d. Rispettare le condizioni di cui all'art. 28 paragrafo 2) del GDPR, al fine di ricorrere ad un altro (sub) Responsabile del trattamento, così declinate nel caso di specie: il Responsabile del trattamento ha l'autorizzazione generale del Titolare del trattamento per l'assunzione di (sub) Responsabili del trattamento³; l'elenco dei (sub) Responsabili del trattamento già autorizzati dal Titolare del trattamento, al momento della sottoscrizione del presente atto, è contenuto nell'allegato 2).
- e. Rispettare le condizioni di cui all'art. 28 paragrafo 4) del GDPR, laddove il Responsabile del trattamento si avvale di un (sub) Responsabile del trattamento per lo svolgimento di specifiche attività di trattamento: a tal riguardo, il Titolare del trattamento ha la facoltà di domandare al Responsabile del trattamento di fornirgli copia del contratto (o atto giuridico) sottoscritto tra quest'ultimo e il relativo (sub) Responsabile del trattamento nominato;
- f. Tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, per quanto possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti del soggetto interessato di cui al capo III) del GDPR;
- g. Assistere il Titolare del trattamento nel garantire il rispetto degli adempimenti in materia di misure di sicurezza tecniche ed organizzative di cui all'art. 32 del GDPR, così come individuate, di volta in volta, dal Titolare del trattamento, ivi incluse le seguenti: i) pseudonimizzazione e/o cifratura dei dati personali; ii) capacità di assicurare la riservatezza, l'integrità e la disponibilità dei dati e la resilienza dei sistemi e dei servizi di trattamento; iii) capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; iv) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- h. Assistere il Titolare del trattamento nell'esecuzione dell'onere di notifica e/o di comunicazione, ai sensi degli artt. 33 e 34 del GDPR, di una violazione di dati personali (data breach) ex art. 4 n. 12) del GDPR riferita ad un attività di trattamento svolta dal Responsabile del trattamento ovvero dal

² L'elenco delle persone a cui è stato concesso l'accesso ai dati personali deve essere, altresì, sottoposto ad una revisione periodica, onde così verificare l'opportunità di revocare eventuali privilegi di accesso, invero, non più necessari. Inoltre, il Responsabile del trattamento è tenuto, su richiesta del Titolare, a dimostrare che le persone autorizzate al trattamento siano realmente soggette ai descritti obblighi di riservatezza.

³ In tal caso, il Titolare del trattamento precisa che il Responsabile del trattamento deve scegliere un (sub) Responsabile del trattamento che rispetti i parametri di assessment di cui alla nota n. 3) del contratto, gli oneri di cui all'art. 2 del contratto nonché, infine, le istruzioni di cui al relativo allegato 3).

nominato (sub) Responsabile del trattamento: a tal fine, il Responsabile del trattamento è tenuto ad informare il Titolare del trattamento di tale evento immediatamente o, comunque, entro il termine (inderogabile) di n. 24 (ventiquattro) ore dal momento in cui ne è venuto a conoscenza, inviando una comunicazione al seguente indirizzo (rpd@aulss9.veneto.it; o in alternativa, a: protocollo.generale@aulss9.veneto.it), cooperando, peraltro, al riguardo con il Titolare del trattamento al fine di adottare in modo immediato o, comunque, senza alcun indebito (ed ingiustificato) ritardo tutte le misure necessarie al fine di minimizzare i rischi derivanti dalla violazione per i soggetti interessati, porre rimedio al data breach e mitigarne qualsiasi ulteriore effetto negativo;

- i. Assistere il Titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati (DPIA) ex art. 35 del GDPR e, in via eventuale, cooperare con il Titolare del trattamento nell'ambito dell'esecuzione degli oneri previsti dall'art. 36 del GDPR;
- j. Al termine del rapporto descritto al precedente punto 1.2.), il Responsabile del trattamento è tenuto a restituire tutti i dati personali al Titolare del trattamento e cancellare le copie esistenti, a meno che il diritto dell'UE o dei relativi Stati membri imponga la conservazione dei dati personali in questione, da ottemperare tuttavia nel rispetto del principio di minimizzazione ex art. 5 paragrafo 1) lettera c) del GDPR⁴;
- k. Mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al GDPR ed alla connessa normativa nazionale applicabile in materia, e consentire a quest'ultimo di svolgere, ove ritenuto opportuno o necessario, un'attività di revisione nei confronti del Responsabile del trattamento, ivi incluse le ispezioni, da realizzarsi ad opera del Titolare del trattamento ovvero da parte di un altro soggetto da questi appositamente incaricato;
- l. Informare, in modo immediato o comunque senza indebito ritardo, il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR ovvero altre disposizioni normative, anche nazionali, applicabili in materia;
- m. Curare, ove richiesto, assieme al Titolare del trattamento l'eventuale rapporto con la competente Autorità di Controllo ovvero l'organo giurisdizionale, anche in caso di eventuali procedimenti amministrativi, civili e/o penali;
- n. Comunicare al Titolare del trattamento – immediatamente, senza ingiustificato ritardo, e comunque entro e non oltre il termine di n. 12 ore dall'effettiva conoscenza – un incidente ex art. 25 comma 4) del D. Lgs. n. 138/2024.

3. Durata e corrispettivo.

3.1. Il presente Contratto è da considerarsi valido ed efficace a decorrere dalla data di validità e di efficacia del rapporto descritto al precedente punto 1.2.); esso, tuttavia, perderà di efficacia e di validità in caso di cessazione, per qualsivoglia motivo, del rapporto descritto al precedente punto 1.2.).

3.2. L'attività di trattamento, resa dal Responsabile del trattamento in favore del Titolare del trattamento, disciplinata dal presente Contratto di nomina, da ulteriori eventuali istruzioni, per iscritto, da parte del Titolare del trattamento nonché dalle ulteriori disposizioni normative nazionali/comunitarie applicabili è da intendersi a titolo gratuito, in deroga all'art. 1709 c.c.

4. Esonero di responsabilità.

4.1. Il Responsabile del trattamento si impegna, infine, a tenere indenne il Titolare del trattamento da qualsivoglia pregiudizio o responsabilità, anche in via indiretta ovvero parziale, derivante dalla violazione, ad opera del primo, degli oneri illustrati al precedente art. 2, delle ulteriori istruzioni eventualmente comunicate ovvero di qualsivoglia normativa applicabile alle operazioni di trattamento indicate nel Contratto ovvero connesse, anche in via indiretta, al contratto di cui al precedente punto 1.2.).

5. Disposizioni finali.

5.1. L'eventuale invalidità, inapplicabilità o inefficacia di alcune delle clausole che compongono il presente Contratto non determina, di conseguenza, l'invalidità, inapplicabilità o l'inefficacia integrale del Contratto medesimo.

⁴ Nel caso in cui una specifica disposizione normativa nazionale o comunitaria imponga al Responsabile del trattamento la conservazione dei dati personali trattati in nome e per conto del Titolare del trattamento, il primo si impegna a svolgere tale operazione di trattamento esclusivamente per la finalità e per la durata prevista dal relativo atto normativo.

5.2. Le Parti concordano che eventuali controversie circa l'interpretazione della validità, applicabilità od efficacia del presente Contratto sono devolute, in via esclusiva, alla competenza giurisdizionale del Foro di Verona.

**Sub n.1 Allegato 1) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del
Regolamento UE n. 2016/679.**

INFORMAZIONI SULLE ATTIVITÀ DI TRATTAMENTO

1.1. Natura/finalità dell'attività di trattamento.

Le operazioni di trattamento che il Responsabile del trattamento può eseguire sulle tipologie di dati personali sono connesse, anche in via indiretta, a dare esecuzione al rapporto tra le Parti descritto al punto 1.2.) del Contratto di nomina in questione.

1.2. Categoria dei soggetti interessati

Indicare quale categoria di soggetti interessati sono coinvolti nell'operazione di trattamento in questione (barrare la/e casella/e)

- ☐ Lavoratore dipendente o simile (ivi incluso, il collaboratore).
☒ Paziente
☐ Altro soggetto: indicare

1.3. Categoria di dati personali.

Indicare quale categoria di dati personali sono coinvolti nell'operazione di trattamento in questione (barrare la/e casella/e)

- ☒ Dati personali ex art. 4 n. 1) del GDPR.
☒ Dati personali cd. particolari ex art. 9 del GDPR.
☐ Dati personali cd. giudiziari ex art. 10 del GDPR.

Sub n.2 Allegato 1) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del Regolamento UE n. 2016/679.

(SUB) RESPONSABILI DEL TRATTAMENTO AUTORIZZATI

Ai sensi dell'art. 2.1. lettera b) del Contratto di nomina, il Titolare del trattamento autorizza il Responsabile del trattamento ad utilizzare i seguenti (sub) Responsabili del trattamento (elencare eventuali soggetti terzi):

Denominazione	Sede	Sistemi/applicativi utilizzati	Attività di trattamento delegata

A tal riguardo, si ricorda che il Titolare del trattamento autorizza, sin dalla data di efficacia e validità del presente Contratto, il Responsabile del trattamento ad utilizzare i sopra descritti (sub) Responsabili del trattamento, i quali non possono, tuttavia, effettuare (direttamente ovvero per il tramite di un altro (sub) Responsabile del trattamento) un'attività di trattamento differente da quella sopra concordata ed autorizzata, in assenza di una specifica ed esplicita autorizzazione da parte del Titolare.

**Sub n.3 Allegato 1) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del
Regolamento UE n. 2016/679.**

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Il Titolare **raccomanda, laddove coerente con la tipologia di servizio/attività oggetto del rapporto di cui all'art. 1.2. delle Premesse del Contratto di nomina in questione,** al Responsabile del trattamento di implementare le seguenti misure di sicurezza⁵, in conformità con i più importanti standard (dottrina, giurisprudenza ed atti di soft law) del settore (nel caso, il Responsabile del trattamento è tenuto a far sì che le descritte misure di sicurezza vengano rispettate anche dagli eventuali (sub) Responsabili del trattamento indicati nell'allegato Sub n.2 ovvero successivamente nominati in base all'art. 2.1. lettera d) di sopra):

- a. Tutto il personale – ivi inclusi, ove opportuno, i collaboratori – deve ricevere un'adeguata sensibilizzazione, istruzione, formazione, addestramento e aggiornamento periodico sulle politiche di sicurezza delle informazioni anche personali implementate, sulle procedure (e prassi) organizzative nonché sulla normativa comunitaria e nazionale sulla protezione dei dati personali (“addestramento, awareness e formazione del cd. fattore umano”)⁶. Inoltre, ove ritenuto opportuno, dovrebbe essere istituito un processo disciplinare, formale e comunicato, volto ad intraprendere provvedimenti nei confronti del personale che ha commesso, con dolo o colpa grave, una violazione della sicurezza delle informazioni anche personali (data breach e/o incidente di sicurezza), della normativa comunitaria e nazionale sulla protezione dei dati personali ovvero di qualsivoglia altra normativa applicabile.
- b. È stata predisposta una politica che mira a disciplinare, in modo compiuto, l'ipotesi di cessazione ovvero di variazione di responsabilità, durante il rapporto di lavoro o di collaborazione, di un soggetto autorizzato al trattamento⁷.
- c. I dati personali, oggetto di trattamento, devono essere archiviati mediante l'utilizzo di misure idonee a proteggerli da accessi non autorizzati, alterazioni, danni o distruzioni. Inoltre, il Responsabile del trattamento è tenuto a far sì che tutto il personale (e i collaboratori, ove opportuno) restituisca gli asset utilizzati ed in loro possesso, al termine del periodo di impiego o del contratto stipulato, fatti salvi differenti e specifici accordi.
- d. Viene implementato un sistema di autorizzazione dei profili di accesso⁸, in base a ruoli e responsabilità (RBAC: Role Based Access Control): i) i profili di autorizzazione devono essere definiti e configurati dall'inizio del trattamento in modo da consentire l'accesso ai dati strettamente necessari (principio del “need to know”/“least privilege”)⁹; ii) i profili di autorizzazione devono essere revisionati con cadenza periodica grazie ad un'apposita politica di accessi e di autorizzazione, da aggiornare sulla base dei requisiti di business ovvero di sicurezza delle informazioni (es. processo formale di registrazione e di de-registrazione per abilitare l'assegnazione dei diritti di accesso;

⁵ Tali misure possono, tuttavia, essere soggette ad una revisione (o meglio, una integrazione), tenuto conto della natura, della portata, del contesto e delle finalità delle attività di trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche interessate.

⁶ È necessario sensibilizzare e rendere consapevoli dei rischi tutti gli operatori che possono accedere ai dati o ad altre risorse attraverso l'uso dei vari dispositivi; in modo particolare, alcuni utenti come gli amministratori di sistema oppure i dirigenti, cioè utenti con privilegi più elevati, devono comprendere l'importanza, i rischi e le responsabilità che derivano dal loro ruolo. È di fondamentale importanza sviluppare una corretta cultura della sicurezza in tutto il personale, indipendentemente dalle sue responsabilità, per poi considerare, con particolare attenzione, i ruoli critici; tutti devono avere una consapevolezza dei rischi e della propria capacità di prevenire incidenti di sicurezza (e/o data breach) e/o di gestirli e delle insidie che sia la quotidianità sia gli eventi fuori dall'ordinario possono generare. La formazione deve essere appropriatamente progettata in base ai ruoli e alle competenze pregresse del personale, su argomenti diversificati e identificati al bisogno.

⁷ Le responsabilità e i doveri di sicurezza delle informazioni che rimangono validi dopo la cessazione o il cambio di impiego devono essere definiti, comunicati al relativo personale dipendente o al contraente, e fatti rispettare. I cambiamenti di responsabilità o di impiego dovrebbero essere gestiti come la cessazione delle responsabilità o dell'impiego attuale combinata con l'inizio di una nuova responsabilità o dell'impiego.

⁸ I controlli d'accesso sono sia logici che fisici, e questi dovrebbero essere considerati insieme. Tale politica dovrebbe tener conto, inter alia, dei seguenti elementi: requisiti di sicurezza delle applicazioni aziendali; politiche per la diffusione e l'autorizzazione delle informazioni, per esempio il principio della necessità di sapere e i livelli di sicurezza delle informazioni e la loro classificazione; segregazione dei ruoli di controllo dell'accesso; requisiti per l'autorizzazione formale delle richieste di accesso, per la revisione periodica e la rimozione dei diritti di accesso; ruoli con accesso privilegiato.

⁹ Le credenziali di accesso devono essere individuali per gli “user” e devono rispettare il principio di segregazione delle funzioni.

processo formale per l'assegnazione o la revoca dei diritti di accesso per le utenze e i sistemi e/o servizi; limitazione e controllo dell'assegnazione e uso dei diritti di accesso privilegiato; rimozione dei diritti di accesso al momento della cessazione del rapporto di lavoro/di collaborazione ovvero adozione, modifica, integrazione o revisione ad ogni variazione¹⁰); iii) i compiti e le aree di responsabilità in conflitto tra loro devono essere oggetto di separazione, al fine di ridurre la possibilità di uso improprio, modifica non autorizzata o non intenzionale dei dati personali¹¹.

- e. L'accesso ai sistemi e alle applicazioni viene controllato da procedure di log-in sicure.
- f. I sistemi di gestione delle password devono essere interattivi, devono assicurare che le stesse siano di qualità (dunque siano adeguatamente complesse), e che siano opportunamente conservate e protette da accessi o utilizzi ad opera di soggetti non autorizzati.

A tal fine, il Responsabile del trattamento deve assicurare la sussistenza dei seguenti requisiti:

- ✓ richiesta, in via automatica, di aggiornamento periodico della password (non oltre 90 giorni) nei confronti di tutti i soggetti autorizzati al trattamento;
- ✓ segretezza della password, la quale deve possedere, a tal fine, le seguenti caratteristiche minime:
 - i. deve contenere almeno 15/12 caratteri ovvero, nel caso in cui lo strumento elettronico non lo permetta, un numero di caratteri pari al massimo consentito¹²;
 - ii. deve contenere lettere minuscole e maiuscole, combinate con cifre o caratteri speciali;
 - iii. non deve contenere l'ID dell'utente, o comunque elemento agevolmente riconducibile a quest'ultimo;
 - iv. deve essere modificata autonomamente ed obbligatoriamente dal soggetto autorizzato al primo collegamento, dopo l'eventuale re-impostazione, nel rispetto della cadenza temporale sopra descritta, nonché nel rispetto del criterio "password history" (ossia, impossibilità di riutilizzare, a breve distanza di tempo, le credenziali già precedentemente utilizzate);
 - v. ove possibile, deve essere costituita dalla cd. "passphrase" (ossia, una raccolta di parole comuni casuali combinate in una frase che fornisca un'ottima combinazione di memorizzazione e sicurezza) ovvero a multi-fattore o strong authentication (MFA) (es. token; dato biometrico; informazione personale e riservata; OTP)¹³.
- ✓ la password deve essere conservata in modo sicuro, evitando la proliferazione di documenti non protetti contenenti liste di credenziali o appunti facilmente accessibili da chiunque;
- ✓ le credenziali di autenticazione, collegate alla relativa password, devono essere disattivate se non utilizzate, in modo totale, da almeno 6 mesi o 1 anno, a seconda delle specifiche circostanze (e ad eccezione di quelle esplicitamente autorizzate)¹⁴;
- ✓ la password deve essere tutelata mediante impostazioni idonee a contrastare efficacemente attacchi informatici di tipo "brute force" sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione (rate limiting)¹⁵.

¹⁰ Le identità digitali e le credenziali di accesso agli "user", i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza.

¹¹ L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate.

¹² Cfr. punto n. 5) dell'abrogato Allegato B) del previgente Codice Privacy: "La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito..."

¹³ Cfr., in via analogica, art. 1 comma 1) lettera q-bis) del Decreto Legislativo n. 11 del 17.1.2010: "autenticazione forte del cliente": "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (cfr. sul punto anche: Considerando n. 6) del Regolamento UE n. 389/2018 del 27.11.2017).

¹⁴ Cfr., sul punto, l'abrogato Allegato B) (denominato "Disciplinare tecnico in materia di misure minime di sicurezza") del previgente D.Lgs. n. 196/2003 (Codice Privacy).

¹⁵ Il "rate limiting" è una misura di sicurezza tecnica che comporta una limitazione al numero di tentativi infruttuosi di autenticazione costituendo un'efficace protezione dagli attacchi di "denial of service" (DDOS), dai tentativi di violazione delle password con metodi "brute force" e da altri comportamenti illegali: di conseguenza, tale misura provvede a limitare o rallentare la disponibilità di una procedura di login, qualora si verifica una quantità anomala di tentativi di accesso non andati a buon fine in un intervallo di

- g. Viene attuata la protezione delle credenziali di autenticazione con efficaci misure di sicurezza crittografiche¹⁶.
- h. Viene assicurata la sicurezza fisica agli uffici, locali ed impianti che racchiudono dati personali, ivi inclusa la protezione da incidenti ovvero attacchi malevoli (“controllo di accesso fisico”)¹⁷.
- i. Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce (ivi incluso, il malfunzionamento alla rete elettrica di alimentazione) e/o da accesso non autorizzato (interno o esterno), e le stesse devono essere, altresì, correttamente mantenute.
- j. I supporti fisici, al cui interno sono archiviati dati personali, devono essere protetti da idonee misure di sicurezza contro accessi non autorizzati, utilizzi impropri ovvero manomissioni¹⁸; inoltre, il personale dipendente e, ove opportuno, i collaboratori devono assicurare che le apparecchiature lasciate incustodite siano, comunque, adeguatamente protette.
- k. Viene adottata una politica di “scrivania pulita” (clear desk) per i documenti e i supporti di memorizzazione rimovibili (es. pendrive USB), e una politica di “schermo pulito” (clear screen) per i servizi di elaborazione delle informazioni¹⁹.
- l. Vengono controllati i cambiamenti all’interno dell’organizzazione, dei processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che influenzano la sicurezza delle informazioni (“gestione del cambiamento”)²⁰.
- m. E’ stata predisposta una politica volta alla protezione dei dati e dei sistemi da qualsivoglia software dannoso (virus/malware/ransomware²¹), da accessi remoti da rete pubblica da parte di sistemi non autorizzati, nonché è stato predisposto un sistema di protezione delle postazioni terminali (end point protection systems – EPS): i) i programmi di protezione anti virus e anti malware devono essere continuamente aggiornati; ii) gli aggiornamenti delle patch di sicurezza e le correzioni per le vulnerabilità di sistema note devono essere prontamente implementate; iii) i sistemi perimetrali,

tempo relativamente ristretto, procedendo, quindi, a bloccare temporaneamente i login per l’account sotto attacco; tale misura potrebbe, altresì, prevedere un incremento delle tempistiche di blocco, qualora si riscontrassero nuovi tentativi di accesso falliti dopo lo sblocco dell’account, preferibilmente per non più di un paio d’ore, al fine di non impedire l’accesso al servizio.

¹⁶ In merito, è opportuno che una politica sull’uso, la protezione e la durata delle chiavi crittografiche dovrebbe essere sviluppata e implementata attraverso il loro intero ciclo di vita.

¹⁷ L’accesso fisico alle risorse deve essere protetto ed amministrato. Nello specifico, le relative linee guida dovrebbero prevedere, inter alia, le seguenti prescrizioni: i perimetri di sicurezza dovrebbero essere definiti, e l’ubicazione e la forza di ogni perimetro dovrebbe dipendere dai requisiti di sicurezza degli asset all’interno del perimetro e dai risultati di una valutazione dei rischi; i perimetri di un edificio o di un sito contenente strutture per l’elaborazione delle informazioni dovrebbero essere fisicamente solidi e custoditi; un’area di accoglienza presidiata o altri mezzi per controllare l’accesso fisico al sito o all’edificio dovrebbe essere in atto, e limitato solo al personale autorizzato; adeguati sistemi di rilevamento delle intrusioni dovrebbero essere installati.

¹⁸ La documentazione deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l’accesso alle sole persone autorizzate, ovvero in armadi di sicurezza con procedure di tracciamento delle chiavi in uso.

¹⁹ La politica di clear desk/clear screen dovrebbe, inter alia, considerare i seguenti aspetti: le informazioni aziendali sensibili o critiche dovrebbero essere chiuse a chiave quando non sono necessarie, specialmente quando l’ufficio è lasciato libero; i computer e i terminali dovrebbero essere lasciati scollegati o protetti con un meccanismo di blocco dello schermo e della tastiera controllato da una password, un token o un meccanismo simile di autenticazione dell’utente quando non sono sorvegliati, e dovrebbero essere protetti da password o altri controlli quando non sono in uso. Una politica di clear desk/clear screen riduce i rischi di accesso non autorizzato, perdita e danno alle informazioni durante e al di fuori del normale orario di lavoro; invece, casseforti o altre forme di archiviazione sicura potrebbero anche proteggere le informazioni ivi conservate da disastri come un incendio, un terremoto, un’inondazione o un’esplosione.

²⁰ I cambiamenti nell’organizzazione, nei processi di business, nelle strutture di elaborazione delle informazioni e nei sistemi che influiscono sulla sicurezza delle informazioni devono essere controllati. In particolare, devono essere considerati i seguenti elementi: identificazione e registrazione dei cambiamenti significativi; valutazione degli impatti potenziali, compresi gli impatti sulla sicurezza delle informazioni anche personali, di tali cambiamenti; verifica che i requisiti di sicurezza delle informazioni siano stati soddisfatti; comunicazione dei dettagli del cambiamento a tutte le persone interessate; procedure di fall back.

²¹ Si definisce “malware” qualsiasi software che, una volta eseguito su un sistema informatico, possa apportare modifiche indesiderate o danni al sistema stesso e ai suoi utenti; i malware possono effettuare le azioni più diverse sul sistema “vittima”, quali ad esempio: possono sottrarre le informazioni memorizzate, danneggiarle o modificarle in maniera ponderata; catturare schermate del dispositivo “vittima” violando la privacy dei suoi utenti; rubare le credenziali degli utenti che usano il sistema. Invece, i “ransomware” rappresentano una tipologia specifica di malware il cui obiettivo è quello di impedire alla vittima l’accesso e l’uso di documenti e dispositivi cifrando i supporti di memoria. La politica contro il malware dovrebbe essere basata sul software di rilevamento e riparazione del malware, sulla consapevolezza della sicurezza delle informazioni e su controlli appropriati dell’accesso al sistema e della gestione dei cambiamenti. La relativa guida dovrebbe almeno: stabilire una politica formale che proibisca l’uso di software non autorizzato; implementazione di controlli che impediscano o rilevino l’uso di un software non autorizzato; implementare controlli che impediscano o rilevino l’uso di siti web maligni noti o sospetti; condurre revisioni regolari del contenuto del software e dei dati dei sistemi che supportano i processi aziendali critici: la presenza di qualsiasi file non approvato o modifiche non autorizzate dovrebbe essere formalmente indagata.

quali firewall²², devono essere presenti, aggiornati, mantenuti, ben configurati e rivisti periodicamente.

- n. E' stata predisposta una procedura di backup²³ (crittografato, ove possibile) volta a garantire il recupero dei dati e il ripristino dei sistemi in caso di incidenti di sicurezza, data breach, anomalie o altri eventi dannosi: i) la copia dei dati e delle configurazioni dei sistemi deve essere eseguita almeno su base giornaliera ove possibile; ii) la retention di tali copie deve essere pari ad almeno una settimana, salvo richieste differenti che potranno essere concordate nella fase contrattuale o nel corso dell'esecuzione del servizio di cui al punto 1.2.) del Contratto; iii) le copie dei dati devono essere protette da accessi non autorizzati e conservate in un luogo sicuro, preferibilmente offline; iv) deve essere garantita l'integrità delle copie dei dati e il funzionamento delle procedure di restore da testare con regolarità.
- o. Le attività degli Amministratori di Sistema (AdS)²⁴ vengono sottoposte ad audit log²⁵, conservati, protetti e riesaminati in modo periodico, nel rispetto del Provvedimento del 27.11.2008 del Garante Privacy, così come modificato in base al successivo Provvedimento del 25.6.2009.
- p. Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata, e appropriate misure devono essere intraprese per affrontare i rischi relativi (cd. gestione delle vulnerabilità tecniche).
- q. Le reti devono essere gestite e controllate al fine di proteggere le informazioni nei sistemi informativi e nelle applicazioni software.
- r. Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato (es. antispam; mail filter²⁶).
- s. È stata stabilita la responsabilità e la procedura di gestione volta ad assicurare una risposta rapida, efficace ed ordinata agli incidenti di sicurezza e/o agli incidenti relativi alla sicurezza delle informazioni personali: tali eventi devono essere segnalati il più velocemente possibile, tramite appropriati canali gestionali. A tal fine, il personale dipendente e, ove opportuno, i collaboratori che utilizzano i sistemi informativi e i servizi dell'organizzazione devono essere tenuti a registrare e a segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.
- t. I piani di ripristino (recovery plan)²⁷, la conoscenza acquisita dall'analisi e dalla soluzione degli incidenti costituenti la violazione di dati personali (data breach) o della sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto di incidenti futuri ("lesson learned").
- u. E' stata predisposta una procedura di risposta (Incident Response e Business Continuity, nel rispetto della ISO/IEC 22301:2014) e di recupero (Incident Recovery e Disaster Recovery²⁸), al fine di

²² Il "firewall" è un componente che si interpone tra due reti, e permette di imporre regole sul transito di informazioni tra queste.

²³ Quando si progetta un piano di back up, almeno i seguenti elementi dovrebbero essere presi in considerazione: devono essere prodotte registrazioni accurate e complete delle copie di back up e delle procedure di ripristino documentate; i back up dovrebbero essere conservati in un luogo remoto, ad una distanza sufficiente per sfuggire a qualsiasi danno di un disastro nel sito principale; le informazioni di back up dovrebbero ricevere un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati al sito principale; i supporti di back up dovrebbero essere testati regolarmente, al fine di garantire che si possa fare affidamento su di essi quando necessario; nelle situazioni in cui la riservatezza è importante, i back up dovrebbero essere protetti con mezzi di crittografia.

²⁴ Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate a: gestione e manutenzione di un impianto di elaborazione o di sue componenti (es. salvataggio dei dati; organizzazione dei flussi di rete; gestione dei supporti di memorizzazione; manutenzione degli hardware) (cd. AdS di una infrastruttura informatica); gestione e manutenzione di un sistema operativo; gestione e manutenzione di uno o più applicativi (es. database; application server) (cd. AdS degli applicativi). Inoltre, si ricorda che, nel rispetto del citato Provvedimento del Garante Privacy italiano, gli estremi identificativi delle persone fisiche qualificate come "amministratori di sistema" devono essere riportati in un documento interno da mantenere aggiornato.

²⁵ Audit log: consiste nel log sulle attività svolte all'interno di uno specifico sistema/apparato informativo; esso si differenzia dall'"access log", il quale riguarda, invece, i log di entrata e di uscita da un determinato sistema informativo.

²⁶ È un componente che esamina ogni mail in transito verso l'azienda, al fine di identificare e bloccare tempestivamente possibili minacce.

²⁷ I processi e le procedure di ripristino devono essere eseguiti e mantenuti al fine di assicurare un recupero dei sistemi o asset coinvolti da un incidente di sicurezza e/o da una violazione dei dati personali (data breach).

²⁸ Cfr., in via analogica, il Provvedimento n. 333 del 4.7.2013 a firma del Garante Privacy italiano: "...con il termine "disaster" si intende, ai fini del provvedimento in esame, "l'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'organizzazione", laddove la nozione di DR configura invece "l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro di elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare

fronteggiare un incidente, un evento imprevisto o di forza maggiore ovvero un disastro²⁹; le descritte procedure devono essere, altresì, verificate ad intervalli di tempo regolari, al fine così di assicurare che siano sempre valide ed efficaci durante il verificarsi di una situazione avversa, di crisi o comunque imprevista.

- v. I dati personali, oggetto dell'attività di trattamento demandata dal Titolare al Responsabile, vengono distrutti, cancellati, sovrascritti o comunque resi inutilizzabili (o in alcun modo ricostruibili) in modo irreversibile, in caso di sostituzione di un hardware/software o in caso di riutilizzo, per differenti finalità di trattamento, dell'hardware/software medesimo.
- w. È stato predisposto un sistema di prevenzione delle intrusioni (intrusion prevention systems³⁰ – IPS), da tenere aggiornato, mantenuto, ben configurato e rivisto periodicamente.
- x. Viene svolto, con cadenza periodica, il monitoraggio della rete informatica al fine di rilevare potenziali eventi di cybersecurity³¹.
- y. Viene attuata la protezione delle comunicazioni di dati in transito (data in transit) con tecniche crittografiche allo stato dell'arte.
- z. Vengono effettuate delle sessioni di vulnerability assessment e penetration test (VAPT) sui sistemi/applicativi coinvolti nell'esecuzione delle attività di trattamento di cui al Contratto, da eseguirsi con cadenza regolare e periodica, anche ad opera, ove necessario, di terze parti indipendenti.

Verona, lì

Totale pagine: 10 (dieci), di cui 3 (tre) allegati (Allegato 1 Sub n.1, n. 2 e n. 3)

IRCCS OSPEDALE SACRO CUORE DON CALABRIA

(in persona dell'Amministratore Delegato)

Dott. Claudio Cracco

AZIENDA ULSS N. 9 SCALIGERA

(in persona del delegato del legale rappresentante pro tempore)

Dott.ssa Gessica Martello

indisponibilità prolungate". Il DR comprende quindi le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture hardware, software e di servizi di comunicazione".

²⁹ A tal fine, deve sussistere un documento aggiornato di dettaglio contenente i piani di continuità operativa/disaster recovery, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: le politiche e i processi impiegati per identificare le priorità degli eventi; le fasi di attuazione dei piani; i ruoli e le responsabilità del personale; i flussi di comunicazione e reportistica.

³⁰ È un componente che controlla in modo continuo il traffico e le attività in essere nella rete aziendale per identificare e, laddove possibile, prevenire possibili intrusioni non autorizzate.

³¹ Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity.

DELIBERAZIONE DEL DIRETTORE GENERALE N. _____ DEL _____

ATTESTAZIONE DI PUBBLICAZIONE E DI ESECUTIVITÀ

La presente deliberazione è divenuta esecutiva dalla data di adozione.

In data odierna copia della presente deliberazione viene:

- Pubblicata per 15 giorni consecutivi nell'Albo on line, ai sensi e per gli effetti dell'art. 32 – comma 1 – della L. 18.06.2009, n. 69 e s.m.i..
- Trasmessa al Collegio Sindacale, ai sensi dell'art. 10 – comma 5 – della L.R. 14.09.1994, n. 56.

Verona, lì _____

Il Direttore
UOC Affari Generali

TRASMESSA PER L'ESECUZIONE A:

Dipartimento di Prevenzione

TRASMESSA PER CONOSCENZA A:

UOC Contabilità e bilancio