

ACCORDO DI CONTITOLARITÀ RIS-CIS-PACS

AZIENDA REGIONALE DELLA SALUTE SARDEGNA (ARES Sardegna) in persona del legale rappresentante pro tempore il Direttore Generale Dott. Giuseppe Pintor, con sede in Selargius (CA) - Via Piero della Francesca n. 1

AZIENDA SOCIO-SANITARIA LOCALE n.1 SASSARI in persona del legale rappresentante pro tempore il Direttore Generale Dott. Antonio Lorenzo Spano con sede in Sassari – Via Enrico Costa n.57

AZIENDA SOCIO-SANITARIA LOCALE n.2 GALLURA in persona del legale rappresentante pro tempore il Direttore Generale Dott. Antonio Irione con sede in Olbia - Via Bazzoni - Sircana n. 2 / 2a

AZIENDA SOCIO-SANITARIA LOCALE n. 3 NUORO in persona del legale rappresentante pro tempore il Direttore Generale Dott. Francesco Trotta, con sede in Nuoro - Via A. Demurtas n. 1

AZIENDA SOCIO-SANITARIA LOCALE n.4 OGLIASTRA in persona del legale rappresentante pro tempore il Direttore Generale Dott. Andrea Fabbo, con sede in Lanusei - Via Piscinas n. 5

AZIENDA SOCIO-SANITARIA LOCALE n.5 ORISTANO in persona del legale rappresentante pro tempore il Direttore Generale Dott.ssa Grazia Cattina, con sede in Oristano - Via Carducci n. 35

AZIENDA SOCIO-SANITARIA LOCALE n.6 MEDIO CAMPIDANO in persona del legale rappresentante pro tempore il Direttore Generale Dott. Joseph Polimeni, con sede in Sanluri - Via Ungaretti n. 9

AZIENDA SOCIO-SANITARIA LOCALE n.7 SULCIS IGLESIENTE in persona del legale rappresentante pro tempore il Direttore Generale Dott. Paolo Cannas, con sede in Carbonia - Via Dalmazia n. 83

AZIENDA SOCIO-SANITARIA LOCALE n.8 CAGLIARI in persona del legale rappresentante pro tempore il Direttore Generale Dott. Aldo Atzori con sede in Cagliari - Via Lungomare Poetto n. 12

AZIENDA OSPEDALIERO UNIVERSITARIA SASSARI in persona del legale rappresentante pro tempore il Direttore Generale Dott. Serafinangelo Ponti, con sede in Sassari - Viale San Pietro n. 10

AZIENDA OSPEDALIERO UNIVERSITARIA CAGLIARI in persona del legale rappresentante pro tempore il Direttore Generale Dott. Vincenzo Serra, con sede in Cagliari - Via Ospedale n. 54

AZIENDA DI RILIEVO NAZIONALE ED ALTA SPECIALIZZAZIONE “G. BROTTU” in persona del legale rappresentante pro tempore il Direttore Generale Dott. Maurizio Marcias, con sede in Selargius - Piazzale Alessandro Ricchi n.1,
qui di seguito nel presente atto denominate “Parti”

Premesso

- che il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali ed il D.lgs 101/2018 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati personali) dispone la nuova disciplina europea in materia di trattamento dei dati personali delle persone fisiche;
- il Regolamento (UE) 2016/679 stabilisce che, *“qualora due o più titolari determinino congiuntamente finalità e mezzi del trattamento”*, essi operano in qualità di contitolari e disciplinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità, con particolare riguardo ai rapporti con gli interessati, alle informative e all’esercizio dei diritti;
- il D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, integra il quadro nazionale in materia di protezione dei dati personali applicabile anche ai trattamenti di dati relativi alla salute effettuati da soggetti pubblici del Servizio sanitario;
- che la Regione Autonoma della Sardegna con la L.R. n.24/2020 “Riforma del sistema sanitario regionale e riorganizzazione sistematica delle norme in materia. Abrogazione della legge regionale n.10 del 2006, della legge regionale n.23 del 2014 e della legge regionale n.17 del 2016 e di ulteriori norme di settore” riorganizza il Sistema sanitario regionale, affidando alle Aziende Socio-sanitarie Locali (ASL) la responsabilità dei servizi assistenziali nei rispettivi territori di competenza, e all’Azienda Regionale per la Salute (ARES) funzioni e compiti centralizzati di carattere tecnico-amministrativo in favore delle ASL, come meglio declinati all’art. 3 della legge medesima. In particolare, è compito di ARES promuovere le attività di sanità digitale finalizzate a garantire una maggiore appropriatezza delle prestazioni sanitarie, È attribuita ad ARES la funzione di raccolta dei fabbisogni relativi ai fattori produttivi e di supporto tecnico--organizzativo alla loro programmazione, secondo un modello di gestione e pianificazione centralizzata, al fine di assicurare l’efficienza e l’efficacia nell’erogazione dei Livelli Essenziali di Assistenza (LEA). In particolare, nell’ambito di tale funzione, rientrano le seguenti attività: i servizi tecnici per la valutazione delle tecnologie sanitarie (Health Technology Assessment – HTA) e di ingegneria clinica; la gestione delle infrastrutture informatiche, della connettività, dei sistemi informativi e della telemedicina (art. 8), promossa in un’ottica di omogeneizzazione, integrazione e sviluppo del sistema ICT regionale; esercita, altresì, tutte le competenze e funzioni ulteriori previste dalle norme regionali vigenti e dal presente accordo;
- che la Regione Autonoma della Sardegna con la L.R. n.8/2025 “Disposizioni urgenti di adeguamento dell’assetto organizzativo ed istituzionale del sistema sanitario regionale. Modifiche alla legge regionale 11 settembre 2020, n.24”, è ulteriormente intervenuta sulle competenze e funzioni degli Enti operanti nel SSR;
- che le ASL e le ulteriori Aziende, svolgono le proprie funzioni ed attività assicurando la garanzia dei LEA, attraverso servizi direttamente gestiti: l'assistenza sanitaria collettiva in ambiente di vita e di lavoro, l'assistenza distrettuale e l'assistenza ospedaliera, fatte salve le funzioni riservate dalla normativa regionale alla competenza di ARES Sardegna;
- che l’art.5 del Regolamento UE 2016/679 in materia di protezione di dati personali prevede espressamente che il Titolare del trattamento sia competente ad assicurare il rispetto dei principi di

liceità, correttezza, trasparenza, limitazione delle finalità, adeguatezza, minimizzazione, esattezza, limitazione della conservazione, sicurezza e protezione dei dati personali trattati e ciò anche tramite persone fisiche espressamente designate che operano sotto la sua autorità e direzione;

- che, l'art.5 del Regolamento UE 2016/679 prevede, inoltre, che il Titolare del trattamento sia soggetto al principio di "accountability" ovvero che non solo debba adottare un processo complessivo di misure giuridiche, organizzative e tecniche per la protezione dei dati personali ma debba anche essere in grado di dimostrare e provare il rispetto dei principi del trattamento attraverso il modello organizzativo adottato;
- che a decorrere dal 1° gennaio 2022, gli Enti del Sistema Sanitario Regionale (SSR), come individuati dalla Legge regionale n. 24 del 2020 e dalla Legge regionale n. 8 del 2025, assumono la qualifica di Titolari del trattamento dei dati in relazione alle specifiche funzioni e competenze loro attribuite dalla legge;
- che il diritto alla libera scelta del luogo di cura dei pazienti è principio cardine dell'ordinamento giuridico e che, pertanto, ARES, le ASL e le Aziende Ospedaliere determinano congiuntamente le finalità e i mezzi del trattamento dei dati per garantire che la mobilità del paziente non comprometta la sicurezza e la riservatezza delle sue informazioni sanitarie;
- che, l'art. 26 par.1 del Reg. UE 2016/679 recita che *"Allorché due o più titolari del trattamento determinano congiuntamente le finalità e modalità del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione e dello Stato membro cui i Titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati"*;
- che, pertanto, quello di contitolarità è concetto che prescinde da un'esplicita previsione normativa ma si basa sull'analisi specifica della situazione di fatto che potrebbe dare origine alla contitolarità del trattamento medesima, privilegiando l'applicazione del principio di effettività e la valutazione degli elementi fattuali sussistenti *"case by case"* rispetto ad una previsione normativa aprioristica anche alla luce della oggettiva difficoltà di prevedere in un testo normativo specifico le innumerevoli ipotesi fattuali che potrebbero dare origine a contitolarità;
- che quanto sopra viene richiamato nelle Linee Guida 7/2020 versione 2.0 adottate il 7 luglio 2021, a tutt'oggi ancora in vigore, dell'European Data Protection Board le quali richiedono come la valutazione della contitolarità si fondi su *"un'analisi fattuale piuttosto che formale dell'influenza effettivamente esercitata sulle finalità e sui mezzi del trattamento Qualsiasi configurazione esistente o prevista dovrebbe essere verificata alla luce delle circostanze concretamente relative al rapporto tra le parti"*;
- che le medesime dianzi citate Linee Guida sostengono come la partecipazione congiunta possa derivare da decisioni convergenti di due o più soggetti per quanto concerne le finalità e i mezzi essenziali e che il criterio per individuare tali decisioni convergenti sia rappresentato dal verificare se il trattamento non sarebbe possibile senza la partecipazione delle parti alle finalità ed ai mezzi ovvero che i trattamenti di ciascuna parte sono tra loro indissociabili ovvero indissolubilmente legati;

- che, altresì, l'esercizio dell'influenza sui mezzi del trattamento non significa che, per esservi contitolarietà, ciascun soggetto coinvolto debba in ogni caso determinare tutti i mezzi in quanto i contitolari possono determinare i mezzi del trattamento in misura diversa a seconda di chi sia effettivamente in grado di effettuare tale determinazione potendo, infatti, accadere che uno dei soggetti coinvolti fornisca i mezzi del trattamento e li metta a disposizione per le attività di trattamento dei dati personali da parte di altri soggetti consentendo che anche questi ultimi, decidendo di avvalersi di tali mezzi affinché i dati personali possano essere trattati per una determinata finalità, partecipino alla determinazione dei mezzi di trattamento;
- che il nuovo Sistema Sanitario Regionale (SSR) è strutturato in modo che tutti gli Enti operanti al suo interno contribuiscano, ciascuno secondo le proprie competenze e funzioni attribuite, all'erogazione dei servizi sanitari e socio-sanitari. Tale organizzazione, per quanto sopra esposto, implica una contitolarietà funzionale "*ex lege*" per decisioni convergenti tra gli Enti del S.S.R. tale che il trattamento non sarebbe possibile senza la partecipazione di tutte le parti alle finalità ed ai mezzi, essendo i trattamenti di ciascuna parte indissociabili ovvero indissolubilmente legati per garantire l'efficace trattamento dei dati personali, nel rispetto delle normative vigenti. In particolare, gli Enti condividono la responsabilità dei trattamenti dei dati personali eseguiti salvo che operino come Titolari autonomi nell'ambito delle proprie specifiche competenze e attribuzioni derivanti dalla Legge Regionale n. 24/2020 e dalla Legge Regionale n. 8/2025, o abbiano configurazioni specifiche nel trattamento dei dati personali in relazione alle funzioni e ai ruoli loro attribuiti e svolti;
- che nell'ambito delle attività di radiologia, cardiologia diagnostica e dei correlati percorsi clinico-assistenziali, le ASL e le altre Aziende utilizzano sistemi RIS (Sistema Informativo Radiologico), CIS (Sistema Informativo Cardiologico) e PACS (Sistema di Archiviazione e Trasmissione di Immagini) per gestire le attività amministrative e diagnostiche, quali l'accettazione del paziente, gli esami, la refertazione e l'archiviazione digitale del referto e delle immagini con l'obiettivo di rendere più efficiente e rapida la diagnosi e cura del paziente all'interno delle proprie strutture sanitarie;
- che il modello applicativo RIS/CIS/PACS, quando consente la visione controllata di referti, immagini e dati diagnostici da parte di professionisti sanitari appartenenti a Aziende diverse, richiede una disciplina espressa dei ruoli privacy, dei limiti di accesso, delle regole di tracciamento e delle responsabilità;
- che secondo l'Autorità Garante per la Protezione dei Dati Personali, il dossier sanitario è lo strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento, al cui interno operano più professionisti, e raccoglie informazioni relative a eventi clinici occorsi esclusivamente presso un'unica struttura sanitaria;
- che la medesima Autorità ha evidenziato come il Fascicolo Sanitario Elettronico, diversamente dal dossier, è caratterizzato dalla presenza di documenti e informazioni generate da più strutture sanitarie in qualità di autonomi titolari tra le quali non vi sono, tuttavia, le immagini diagnostiche
- che, alla luce di tale distinzione, l'accesso, per finalità di cura, da parte di professionisti sanitari di una Azienda ai dati RIS/CIS/PACS originati presso altra Azienda deve essere ricondotto a un modello di interoperabilità regolata tra soggetti pubblici del SSR che, per la specifica finalità disciplinata nel presente atto, determinano congiuntamente finalità e mezzi essenziali del trattamento;
- che, pertanto, il sistema RIS/CIS/PACS costituisce, nei limiti di cui al presente Accordo, uno strumento essenziale di supporto alla presa in carico e alla continuità delle cure; il Garante ha inoltre riconosciuto, in relazione al dossier sanitario, la necessità di assicurare specifiche garanzie di

sicurezza, obblighi di tracciamento degli accessi, diritto dell'interessato all'oscuramento e alla conoscibilità degli accessi;

- che, in coerenza con quanto precedentemente esposto, gli Enti operanti nel SSR devono poter erogare le prestazioni e a svolgere le funzioni di supporto di propria competenza avvalendosi della piena interoperabilità, visibilità e utilizzabilità dei dati trattati da ciascuno di essi. Ciò consente ai diversi Enti di condividere in tempo reale le informazioni sanitarie, nel rispetto dei principi di liceità, necessità, minimizzazione e pertinenza, con gli altri Enti coinvolti, facilitando la continuità assistenziale e migliorando l'efficacia delle prestazioni erogate, nel pieno rispetto dei principi di protezione dei dati personali stabiliti dal Reg. UE 2016/679;
- che le Parti intendono pertanto disciplinare, con il presente Accordo, la contitolarità limitatamente ai trattamenti di dati personali effettuati attraverso l'ecosistema RIS/CIS/PACS per finalità di cura, continuità assistenziale, consultazione diagnostica e correlata gestione tecnica e organizzativa del servizio interoperabile, fermo restando che ciascuna Parte opera quale titolare autonomo per i trattamenti estranei al perimetro qui definito.

Tutto ciò premesso, le Parti convengono e stipulano quanto segue.

Art. 1 – Definizioni

1. Ai fini del presente Accordo si applicano le definizioni di cui al Regolamento (UE) 2016/679 e al D.Lgs. 196/2003, nonché le nozioni di dossier sanitario e di consenso al dossier richiamate nelle Linee guida del Garante del 4 giugno 2015.
2. Per ecosistema RIS/CIS/PACS si intende l'insieme coordinato di applicativi, infrastrutture, repository, servizi di interoperabilità, componenti di visualizzazione e funzioni di consultazione che consentono la gestione e la fruizione di immagini diagnostiche, tracciati, referti e dati tecnico-clinici correlati nell'ambito delle attività di radiologia e cardiologia diagnostica svolte dalle Parti.

Art. 2 – Oggetto dell'Accordo

1. Il presente Accordo disciplina, ai sensi e per gli effetti dell'art. 26 GDPR, i trattamenti di dati personali effettuati in contitolarità tra ARES e le altre Aziende del SSR della Sardegna per la finalità di interoperabilità e consultazione controllata dei sistemi RIS/CIS/PACS.
2. La contitolarità riguarda esclusivamente i trattamenti nei quali le Parti determinano congiuntamente le finalità e i mezzi essenziali connessi a:
 - interoperabilità interaziendale dei sistemi RIS/CIS/PACS;
 - consultazione selettiva di immagini, referti e dati diagnostici del paziente da parte di professionisti sanitari coinvolti nel percorso di cura;
 - messa a disposizione controllata dei precedenti diagnostici necessari alla continuità assistenziale;
 - gestione delle regole condivise di autenticazione, autorizzazione, profilazione, tracciamento, audit e sicurezza del servizio interoperabile;

- supporto tecnico-organizzativo all'evoluzione e al funzionamento del sistema regionale RIS/CIS/PACS.
3. Restano esclusi dal presente Accordo:
- i trattamenti effettuati da ciascuna Parte quale titolare autonomo per finalità non riconducibili alla interoperabilità del RIS/CIS/PACS;
 - i trattamenti svolti per ulteriori sistemi informativi non espressamente ricompresi nel presente perimetro;

Art. 3 – Finalità del trattamento in contitolarità

1. Le Parti trattano i dati personali nell'ambito del sistema RIS/CIS/PACS condiviso esclusivamente per le seguenti finalità:
 - assicurare la prevenzione, diagnosi, assistenza, cura e continuità assistenziale del paziente nell'ambito del SSR;
 - consentire la consultazione dei precedenti diagnostici e la disponibilità tempestiva di immagini e referti nei casi in cui il paziente sia preso in carico da professionisti sanitari di Aziende diverse nello specifico e con espresso riferimento all'accesso ai dati sanitari contenuti nella Cartella Clinica Elettronica Regionale al fine di consentire l'immediata attivazione dell'interoperabilità interaziendale dei sistemi RIS-PACS nelle more della definizione delle modalità tecniche di dialogo tra i predetti sistemi;
 - evitare duplicazioni inappropriate di esami, ridurre i tempi di attesa e migliorare l'appropriatezza clinica e organizzativa del percorso di cura;
 - garantire il funzionamento tecnico del servizio condiviso, la sicurezza, la resilienza, la tracciabilità degli accessi e l'integrità dei dati trattati.
2. L'accesso ai dati condivisi è consentito esclusivamente al personale sanitario e tecnico-amministrativo specificamente autorizzato e debitamente formato dalle singole aziende sanitarie, nei limiti delle mansioni effettivamente svolte e per il tempo necessario al perseguimento delle finalità sopra indicate.
3. È esclusa qualsiasi forma di accesso indiscriminato ai database clinici delle Parti; la visibilità dei dati deve essere circoscritta al singolo assistito,

Art. 4 – Base giuridica del trattamento e disciplina del consenso

1. Le Parti danno atto che i trattamenti di dati personali, specificamente i dati sanitari, effettuati nell'ambito del presente Accordo per finalità di prevenzione, diagnosi, assistenza, terapia, continuità assistenziale e gestione organizzativa e tecnica del servizio RIS/CIS/PACS interoperabile del SSR, sono fondati, in via ordinaria, sull'adempimento di compiti di interesse pubblico (**art. 6 par. 1 lett. a), d) ed e) - art. 9 par. 2 lett. a), g) ed h)** Reg. UE 679/2016 e **art. 2-sexies** D.Lgs. n.196/2003 così come modificato ed integrato dal D. Lgs. n.101/2018)) e sull'esercizio delle funzioni istituzionali attribuite alle Parti dalla normativa europea, statale e regionale di settore, nonché sulle condizioni di liceità previste per i trattamenti necessari alla finalità di cura e alla gestione dei sistemi e servizi sanitari.

2. In coerenza con il provvedimento del Garante in materia di dossier sanitario, le Parti riconoscono come la condivisione strutturata di informazioni sanitarie richieda una tutela rafforzata rappresentata dalla somministrazione di specifiche informazioni all'interessato, della tassativa delimitazione degli accessi e della piena tracciabilità degli stessi, soprattutto laddove la consultazione sia resa possibile a professionisti appartenenti a strutture diverse da quella di originaria formazione del dato.
3. Le Parti precisano che l'accesso ai dati sanitari dell'assistito del sistema RIS-CIS- PACS da parte di professionisti appartenenti a una diversa ASL del SSR è consentito, senza necessità di consenso, esclusivamente nei casi in cui esso risulti strettamente necessario per finalità di prevenzione, diagnosi, cura o riabilitazione dell'interessato, sulla base di uno specifico presupposto normativo e nel rispetto dei principi di liceità, necessità, minimizzazione e pertinenza. In assenza di una situazione di emergenza o urgenza, ovvero di un concreto e attuale percorso di cura o presa in carico dell'assistito, tale accesso non può ritenersi giustificato né dall'interesse vitale dell'interessato né da un generico richiamo all'interesse pubblico, e deve, pertanto, considerarsi non conforme alla disciplina in materia di protezione dei dati personali, in quanto eccedente rispetto alle finalità legittime del trattamento e suscettibile di integrare un trattamento non autorizzato. L'esecuzione invece del trattamento dei dati personali del paziente riguardanti invece il complesso degli eventi clinici presenti e passati presenti nell'ecosistema RIS/CIS/PACS sarà subordinata alla previa acquisizione del consenso libero, specifico, informato, inequivocabile e documentato dell'interessato, con evidenza del perimetro di visibilità autorizzato.
4. Laddove il consenso sia richiesto:
 - esso è raccolto dalla Azienda che prende in carico l'interessato o da quella individuata nell'informativa applicativa;
 - può essere espresso in forma scritta o con altra modalità idonea a garantirne la documentabilità;
 - è registrato nei sistemi informativi o negli archivi documentali individuati dalle Parti;
 - è revocabile in ogni momento, fermo restando il trattamento già effettuato sulla base del consenso precedentemente prestato.
6. Nei casi di urgenza sanitaria o di impossibilità dell'interessato a esprimere la propria volontà, restano ferme le ulteriori condizioni di liceità previste dalla normativa vigente, ivi inclusa, ove ne ricorrano i presupposti, la salvaguardia dell'interesse vitale dell'interessato o di altra persona fisica (**art. 9 par. 2 lett. c)** Reg. UE 2016/679).

Art. 5 – Categorie di dati e interessati

1. Il trattamento in contitolarità può riguardare le seguenti categorie di dati personali degli assistiti del SSR della Sardegna:
 - dati identificativi e anagrafici del paziente;
 - dati relativi alla salute, comprese immagini diagnostiche, referti radiologici, referti cardiologici, tracciati, esiti, informazioni cliniche di corredo, dati di prenotazione, accettazione ed esecuzione dell'esame;
 - dati identificativi e professionali del personale sanitario coinvolto nella prescrizione, esecuzione, refertazione o consultazione;

- log di accesso, dati tecnici e metadati necessari alla sicurezza, al monitoraggio e all'audit del sistema.

Art. 6 – Riparto delle funzioni e dei compiti tra le Parti

1. ARES Sardegna, nell'ambito delle attribuzioni riconosciute dalla L.R. 24/2020 e dalla L.R. 8/2025 e con riferimento al perimetro del presente Accordo:
 - progetta, coordina, governa e presidia l'architettura tecnologica condivisa del sistema RIS/CIS/PACS regionale di competenza;
 - assicura la gestione delle infrastrutture, della connettività, delle componenti di integrazione e dei servizi tecnologici comuni di propria spettanza;
 - definisce, con il coinvolgimento delle Aziende, gli standard tecnico-organizzativi comuni relativi a interoperabilità, profilazione, autenticazione, logging, sicurezza, audit e continuità operativa;
 - supporta l'uniformazione di policy, format di informativa, modulistica, procedure e standard di configurazione privacy e sicurezza;
 - procede alla stipula e all'aggiornamento, anche per conto degli altri contitolari, degli accordi sulla protezione dei dati personali con i fornitori dell'ecosistema RIS/CIS/PACS, conformemente all'art. 28 Reg. UE 679/2016, e coerentemente al suo ruolo di progettazione, coordinamento, governo e presidio dell'architettura tecnologica;
 - coopera nella gestione delle richieste degli interessati, dei reclami, delle verifiche ispettive, delle violazioni dei dati personali e delle valutazioni di impatto quando relative al sistema condiviso.
1. Ciascuna Azienda:
 - tratta i dati dei propri assistiti nell'ambito dell'erogazione delle prestazioni e della presa in carico clinica;
 - alimenta i sistemi RIS/CIS/PACS con dati corretti, pertinenti e aggiornati per la parte di propria competenza;
 - individua e autorizza il personale che può accedere alle funzionalità condivise, secondo profili coerenti con mansioni e ruoli;
 - rende l'informativa agli interessati e, nei casi previsti dal presente Accordo, provvede alla raccolta del consenso;
 - gestisce in via primaria le richieste di esercizio dei diritti degli interessati relative agli episodi di cura o ai dati di propria competenza, coordinandosi con ARES e con le altre ASL coinvolte ove necessario.
2. Le Parti, per i trattamenti oggetto del presente Accordo, determinano congiuntamente:
 - le finalità del sistema interoperabile RIS/CIS/PACS così come dianzi rappresentato all'art.3 del presente Accordo;
 - i mezzi essenziali del trattamento, inclusi criteri di accesso, logica di visibilità, tracciabilità, tempi di disponibilità applicativa e misure di sicurezza comuni;
 - il contenuto essenziale dell'informativa e le procedure di gestione coordinata degli eventi di sicurezza e dei diritti degli interessati.

Art. 7 – Informativa agli interessati e contenuto essenziale dell'Accordo

1. Le Parti rendono agli interessati una informativa ai sensi degli artt. 13 e 14 GDPR, chiara, completa e specifica rispetto al trattamento effettuato mediante il sistema RIS/CIS/PACS interoperabile.
2. L'informativa deve indicare almeno:
 - i contitolari del trattamento;
 - le finalità del trattamento;
 - la base giuridica applicabile;
 - le categorie di dati trattati;
 - i soggetti o le categorie di soggetti legittimati alla consultazione;
 - le ipotesi in cui sia richiesto il consenso;
 - le modalità di esercizio dei diritti, incluso il diritto all'oscuramento;
 - il punto di contatto per gli interessati;
 - il diritto dell'interessato di conoscere gli accessi eseguiti sui dati condivisi, nei termini e secondo le modalità previste dalla normativa applicabile e dal presente Accordo.
1. Il contenuto essenziale del presente Accordo è messo a disposizione degli interessati mediante pubblicazione sui siti istituzionali delle Parti e con ulteriori modalità idonee a garantirne la conoscibilità.

Art. 8 – Esercizio dei diritti degli interessati

1. L'interessato può esercitare i diritti di cui agli artt. 15-22 GDPR nei confronti di ciascuna Parte, ai sensi dell'art. 26, par. 3, GDPR.
2. La Parte che riceve la richiesta ne cura il riscontro nei termini di legge per quanto di competenza e, ove necessario, acquisisce tempestivamente da ARES o dalle altre ASL interessate le informazioni indispensabili a fornire un riscontro completo.
3. In coerenza con il provvedimento del Garante sul dossier sanitario, l'interessato ha diritto di ottenere informazioni sugli accessi effettuati ai dati consultabili tramite il sistema RIS/CIS/PACS interoperabile, con indicazione almeno della struttura che ha effettuato l'accesso e della data e ora dello stesso, nei limiti di quanto tecnicamente registrato e giuridicamente dovuto.

Art. 9 – Sicurezza, tracciamento e audit

1. Le Parti, nel rispetto del principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. f) del Reg. UE 2016/679, nei limiti delle proprie funzioni e delle rispettive prerogative e tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, adottano le misure tecniche e organizzative adeguate ai sensi degli artt. 25 - 32 del Reg. UE 2016/679 e delle vigenti norme in materia di trattamento dei dati personali. Tali misure sono finalizzate a garantire un livello di sicurezza adeguato al rischio associato alle operazioni di trattamento dei dati personali trattati tramite il sistema RIS/CIS/PACS.
2. In particolare, le Parti si impegnano a garantire:

- autenticazione forte o comunque adeguata degli utenti;
- profilazione per ruolo, struttura, funzione e relazione di cura;
- accessi selettivi e non massivi;
- registrazione, conservazione e verifica periodica dei log di accesso e delle operazioni rilevanti;
- audit periodici sugli accessi e sulle anomalie;
- segregazione degli ambienti e protezione delle reti e dei repository;
- procedure di disaster recovery coerenti con la criticità del servizio;
- individuare, nominare formalmente, autorizzare e adeguatamente formare e informare il personale incaricato dell'esecuzione dei trattamenti, ai sensi dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies, comma 2, del Codice della Privacy.

Art. 10 – Data breach e incidenti di sicurezza

1. In caso di violazione dei dati personali o incidente di sicurezza che coinvolga il sistema RIS/CIS/PACS interoperabile, la Parte che rileva l'evento ne dà immediata comunicazione alle altre Parti interessate e ad ARES, condividendo senza ritardo tutte le informazioni necessarie alla valutazione del rischio e alla gestione coordinata dell'evento.
2. Le Parti cooperano nella valutazione della violazione, nella documentazione dell'evento, nelle eventuali notifiche all'Autorità di controllo e, ricorrendone i presupposti, nelle comunicazioni agli interessati, secondo il riparto operativo definito nelle procedure attuative.
3. Le Parti tengono conto, nella gestione degli incidenti relativi al sistema RIS/CIS/PACS, dell'attenzione rafforzata posta dal Garante ai trattamenti effettuati mediante strumenti di condivisione strutturata di informazioni sanitarie e alla necessità di presidiare i rischi di accesso non autorizzato.

Art. 11 – Registro dei trattamenti, DPIA e verifiche periodiche

1. Ciascuna Parte aggiorna il proprio registro delle attività di trattamento ai sensi dell'art. 30 GDPR, indicando il trattamento svolto in contitolarità ai sensi del presente Accordo.
2. Le Parti effettuano, ove necessario, una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 GDPR, anche in forma coordinata, in considerazione della natura dei dati trattati, del livello di interoperabilità e dei rischi per i diritti e le libertà degli interessati.
3. Le Parti si impegnano a verificare periodicamente l'adeguatezza delle regole di accesso, dei profili autorizzativi, delle misure di sicurezza e delle informative, anche alla luce dell'evoluzione del FSE e dell'eventuale maggiore alimentazione del medesimo.

Art. 12 – Conservazione dei dati

1. La conservazione dei dati trattati tramite il sistema RIS/CIS/PACS resta disciplinata dalla normativa vigente, dai massimari e prontuari di scarto applicabili, nonché dalle regole organizzative delle singole Aziende per i dati di rispettiva competenza, fermo restando il rispetto dei tempi di conservazione previsti per la documentazione sanitaria e per i log di accesso.

2. I tempi di conservazione dei log, delle informazioni di audit e delle evidenze relative al consenso, ove richiesto, sono definiti in modo uniforme dalle Parti in apposita disciplina attuativa, nel rispetto dei principi di necessità, proporzionalità e accountability.

Art. 13 – Responsabilità e regresso interno

1. Le Parti rispondono nei confronti dell'interessato secondo quanto previsto dal GDPR (art. 82) per i trattamenti effettuati in contitolarità, ferma la possibilità di regresso interno in base all'effettiva imputabilità della violazione o dell'evento dannoso e alla sfera di competenza concretamente coinvolta.
2. Resta ferma la responsabilità esclusiva della singola Parte per i trattamenti svolti quale titolare autonomo al di fuori del perimetro del presente Accordo.

Art. 14 – Punto di contatto e cooperazione tra DPO

1. Le Parti determinano congiuntamente di creare un sistema coordinato di punti di contatto aziendali il cui nominativo e recapiti saranno espressamente indicato nelle rispettive informative.
2. I Responsabili della Protezione dei Dati delle Parti cooperano stabilmente ai fini dell'attuazione del presente Accordo, dell'aggiornamento delle misure di garanzia e della gestione coordinata delle questioni interpretative e applicative.

Art. 15 – Durata, aggiornamento e disposizioni finali

1. Il presente Accordo ha efficacia dalla data della sua sottoscrizione e resta valido fino a revoca o sostituzione concordata tra le Parti, fatti salvi gli obblighi che per loro natura sono destinati a permanere anche successivamente.
2. L'Accordo è soggetto a revisione periodica e comunque ogniqualvolta intervengano modifiche normative, regolamentari, organizzative o tecnologiche rilevanti, ivi incluse quelle connesse all'evoluzione del Fascicolo Sanitario Elettronico, dell'ecosistema regionale di sanità digitale o del modello applicativo RIS/CIS/PACS.
3. Per quanto non espressamente disciplinato nel presente Accordo restano ferme le disposizioni del Regolamento (UE) 2016/679, del D.Lgs. 196/2003 e della normativa nazionale e regionale vigente in materia di trattamento dei dati personali e organizzazione del Servizio sanitario regionale.

Spazi per sottoscrizione

Letto, confermato e sottoscritto digitalmente.

AZIENDA	FIRMA
ARES Sardegna – Il Direttore Generale	
ASL n. 1 di Sassari – Il Direttore Generale	
ASL n. 2 della Gallura – Il Direttore Generale	
ASL n. 3 di Nuoro – Il Direttore Generale	
ASL n. 4 dell'Ogliastra – Il Direttore Generale	
ASL n. 5 di Oristano – Il Direttore Generale	
ASL n. 6 del Medio Campidano – Il Direttore Generale	
ASL n. 7 del Sulcis – Il Direttore Generale	
ASL n. 8 di Cagliari – Il Direttore Generale	
AOU di Cagliari - il direttore Generale	
AOU di Sassari - il Direttore Generale	
ARNAS Brotzu - il Direttore Generale	