FASCICOLO PRIVACY

DEMO - STUDIO MEDICO AURORA S.R.L.

Registro delle attività di trattamento e fascicolo operativo ai sensi del Regolamento (UE) 2016/679

VERSIONE DIMOSTRATIVA
Tutti i dati, nomi, recapiti e soggetti presenti in questo fascicolo sono inventati e utilizzati esclusivamente per mostrare la qualità e la struttura del prodotto ImpresaAI.

Contenuti principali

- Registro completo dei trattamenti con schede analitiche
- Inventario asset e matrice degli accessi
- Valutazione di impatto (DPIA) con rischi iniziali e residui
- Procedura e Registro Data Breach
- Governance di consulenti, fornitori, cloud e provider AI
- Autorizzazioni nominative del personale
- Informative operative pronte da stampare e firmare
- AI Policy e registro degli strumenti AI
- Piano di riesame e aggiornamento

Esempio completo - il fascicolo reale viene personalizzato sulla specifica attività del cliente.

1. Identificazione del Titolare e perimetro

Titolare del trattamento	STUDIO MEDICO AURORA S.R.L. - DATI FITTIZI
Rappresentante	Dott.ssa Giulia Rossi - nome fittizio
P.IVA / C.F.	DEMO-00000000000
Codice ATECO	86.21.00 - Servizi degli studi medici di medicina generale
Attività effettiva	Poliambulatorio medico privato con visite specialistiche, ecografia, prenotazioni, refertazione e gestione amministrativa.
Sede	Via Esempio 10 - 73100 Lecce (LE) - indirizzo fittizio
PEC	studioaurora@pec.demo
Contatto Privacy	privacy@studioaurora.demo
DPO/RPD	Non nominato - presupposti da riesaminare in caso di variazioni rilevanti
Persone autorizzate censite	5
Soggetti/servizi esterni censiti	7

Perimetro. Il fascicolo comprende trattamenti sanitari e amministrativi, personale, fornitori, strumenti digitali, cloud, AI, prenotazioni e gestione dei diritti. Va aggiornato quando cambiano sistemi, sedi, professionisti, fornitori o modalità di trattamento.

2. Quadro normativo e principi applicati

- Regolamento (UE) 2016/679 (GDPR): artt. 5, 6, 9, 12-22, 24-32, 35-36 e 44-49.
- D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.
- Minimizzazione, limitazione della finalità, esattezza, conservazione, integrità, riservatezza e accountability.
- Protezione dei dati fin dalla progettazione e per impostazione predefinita.
- Per i dati sanitari: accessi selettivi, segreto professionale, tracciabilità e specifiche condizioni dell’art. 9 GDPR.

3. Mappa sintetica dei trattamenti

Cod.	Trattamento	Interessati	Dati	Base giuridica	Conservazione
CL-01	Gestione pazienti e richieste	Pazienti / utenti	Identificativi, contatti, amministrativi	Art. 6.1.b/c	Rapporto + termini applicabili
SA-01	Prestazioni sanitarie e referti	Pazienti	Dati salute, anamnesi, referti, immagini	Art. 6 + art. 9.2.h	Secondo normativa sanitaria
PR-01	Prenotazioni e agenda	Pazienti	Contatti, appuntamenti, specialista	Art. 6.1.b	Necessario al servizio
AM-01	Fatturazione e contabilità	Pazienti / fornitori	Fiscali, pagamenti	Art. 6.1.c/b	Di regola 10 anni
HR-01	Dipendenti e collaboratori	Personale	Contrattuali, paghe, salute lavoro	Art. 6.1.b/c + 9.2.b	Rapporto + termini legali
CV-01	Candidature	Candidati	CV, contatti, titoli	Art. 6.1.b	Selezione + termine proporzionato
AI-01	Supporto AI amministrativo	Persone i cui dati possono essere inseriti	Solo dati necessari e minimizzati	Base della finalità originaria	Minimo necessario
WB-01	Sito e richieste online	Utenti sito	Dati modulo e tecnici	Art. 6.1.b/f	Necessario alla richiesta

4. Registro delle attività di trattamento - schede analitiche

CL-01 - Gestione pazienti e richieste

Finalità	Gestione richieste, preventivi, accettazione, assistenza e rapporto con il paziente.
Interessati	Pazienti, utenti, familiari/delegati quando legittimati.
Dati	Identificativi, contatti, amministrativi, informazioni strettamente necessarie alla richiesta.
Base giuridica	Art. 6.1.b GDPR; art. 6.1.c per obblighi di legge.
Origine	Direttamente dall'interessato o da soggetto legittimato.
Destinatari	Personale autorizzato e fornitori necessari.
Asset	Gestionale, email, telefono, archivio cartaceo.
Conservazione	Durata del rapporto + termini amministrativi e tutela dei diritti.
Trasferimenti	Verifica provider cloud e messaggistica.
Misure	Credenziali individuali, MFA, separazione ruoli, backup, istruzioni al personale.

SA-01 - Prestazioni sanitarie e referti

Finalità	Diagnosi, assistenza, cura, refertazione e continuità della prestazione sanitaria.
Interessati	Pazienti.
Dati	Anamnesi, patologie, farmaci, immagini diagnostiche, referti e altri dati sanitari pertinenti.
Base giuridica	Art. 6 GDPR per i profili comuni e art. 9.2.h GDPR, quando applicabile alla prestazione sanitaria.
Origine	Paziente, professionisti sanitari, documentazione clinica legittimamente acquisita.
Destinatari	Professionisti sanitari autorizzati; eventuali laboratori/fornitori necessari.
Asset	Gestionale sanitario, ecografo, PACS/archivio immagini, referti PDF, cartella clinica.
Conservazione	Secondo normativa sanitaria e criteri documentati.
Trasferimenti	Da evitare per dati sanitari salvo provider e garanzie adeguate.
Misure	Accessi per ruolo, cifratura ove disponibile, backup testato, audit log, dismissione sicura dispositivi.

PR-01 - Prenotazioni e agenda

Finalità	Gestione appuntamenti, promemoria e organizzazione agenda.
Interessati	Pazienti.
Dati	Nome, contatti, data/ora, professionista, informazioni minime necessarie.
Base giuridica	Art. 6.1.b GDPR.
Origine	Interessato, reception, portale prenotazione.
Destinatari	Reception e professionisti coinvolti.
Asset	Agenda gestionale, telefono, email, WhatsApp Business se usato.
Conservazione	Tempo necessario alla gestione e documentazione degli appuntamenti.
Misure	Minimizzazione contenuto messaggi, verifica destinatari, accessi nominativi.

AM-01 - Fatturazione e contabilità

Finalità	Fatturazione, pagamenti, contabilità e obblighi fiscali.
Interessati	Pazienti, fornitori.
Dati	Anagrafici, fiscali, bancari e pagamento.
Base giuridica	Art. 6.1.c e 6.1.b GDPR.
Destinatari	Commercialista, banche, sistemi di pagamento, enti pubblici.
Asset	Gestionale fatture, email, home banking.
Conservazione	Di regola 10 anni salvo diversi obblighi.
Misure	Accessi limitati, MFA home banking, protezione documenti fiscali.

HR-01 - Dipendenti e collaboratori

Finalità	Gestione rapporto, paghe, presenze, formazione, sicurezza e obblighi.
Interessati	Dipendenti e collaboratori.
Dati	Anagrafici, contrattuali, retributivi, previdenziali; dati salute solo quando necessari.
Base giuridica	Art. 6.1.b/c GDPR; art. 9.2.b per dati particolari connessi al lavoro.
Destinatari	Consulente lavoro, enti, medico competente nei limiti del ruolo.
Asset	Fascicolo personale, software paghe, email.
Conservazione	Rapporto + termini legali/previdenziali.
Misure	Accessi HR limitati, documenti separati, autorizzazioni nominative.

CV-01 - Candidature

Finalità	Valutazione candidatura e selezione.
Interessati	Candidati.
Dati	CV, contatti, titoli, esperienze.
Base giuridica	Art. 6.1.b GDPR per misure precontrattuali.
Destinatari	Personale autorizzato e supporto selezione.
Asset	Email HR, cartella candidature.
Conservazione	Periodo selezione + termine proporzionato e documentato.
Misure	Accessi limitati, eliminazione candidature scadute.

AI-01 - Uso di sistemi AI

Finalità	Supporto alla redazione di comunicazioni e attività amministrative non decisionali.
Interessati	Persone i cui dati possono comparire nei prompt.
Dati	Solo dati necessari, preferibilmente anonimizzati/pseudonimizzati; vietato inserire dati sanitari salvo procedura autorizzata.
Base giuridica	Segue la finalità originaria; verifica ruolo/DPA del provider.
Asset	ChatGPT Business - esempio fittizio.
Conservazione	Minimo necessario; evitare archivi paralleli.
Misure	Account aziendali, policy AI, formazione, controllo umano, minimizzazione, no decisioni automatizzate significative.

WB-01 - Sito e richieste online

Finalità	Gestione form contatti, sicurezza tecnica, prenotazioni online.
Interessati	Visitatori sito e utenti.
Dati	Dati inseriti nei moduli e dati tecnici.
Base giuridica	Art. 6.1.b/f; consenso per tecnologie che lo richiedono.
Destinatari	Hosting, manutentore sito, personale autorizzato.
Asset	Sito web, hosting, modulo contatti.
Conservazione	Tempo necessario alla richiesta e log tecnici secondo politica documentata.
Misure	HTTPS, aggiornamenti, antispam, accessi amministrativi protetti.

5. Inventario degli asset e degli archivi

Asset	Dati	Rischio principale	Controlli
Gestionale sanitario	Dati pazienti e referti	Accesso improprio / indisponibilità	Account nominativi, ruoli, MFA, backup, log
Ecografo e archivio immagini	Immagini diagnostiche e dati salute	Copia non autorizzata / dismissione	Accessi, supporti removibili limitati, cancellazione sicura
Google Workspace Business	Email e documenti	Account compromesso / trasferimenti	MFA, DPA, gestione account, minimizzazione
WhatsApp Business	Contatti e messaggi di servizio	Invio errato / metadati	Messaggi minimi, niente referti salvo procedura, verifica destinatario
ChatGPT Business	Prompt e output	Inserimento dati non necessario	Policy AI, account aziendale, minimizzazione, controllo umano
Archivio cartaceo	Documenti clinici/amministrativi	Accesso fisico / smarrimento	Armadi, accesso controllato, distruzione sicura

6. Matrice dei soggetti e degli accessi

Soggetto	Ruolo	Asset / accesso autorizzato
Dott.ssa Giulia Rossi	Titolare / medico	Gestionale sanitario, referti, ecografo, amministrazione nei limiti del ruolo
Marco Bianchi	Medico collaboratore	Cartella sanitaria, referti, immagini diagnostiche dei propri pazienti
Elena Verdi	Reception	Agenda, anagrafica, email, telefono; nessun accesso ai referti salvo necessità operativa autorizzata
Paolo Neri	Amministrazione	Fatturazione, contabilità, fornitori; niente cartelle cliniche
Sara Blu	Infermiere	Dati sanitari necessari all'assistenza; nessun accesso contabile
IT DEMO S.R.L.	Responsabile ex art. 28	Accesso tecnico occasionale secondo ticket e istruzioni documentate
ChatGPT Business	Provider tecnologico	DPA/termini del provider; nessuna nomina ImpresaAI da controfirmare

7. Politica di conservazione e cancellazione

Categoria	Criterio	Azione al termine
Referti e documentazione sanitaria	Secondo normativa sanitaria e finalità documentata	Riesame; conservazione obbligatoria o cancellazione sicura
Fatture	Di regola 10 anni	Archiviazione protetta e cancellazione quando consentita
Candidature	Selezione + termine proporzionato	Eliminazione / anonimizzazione
Account cessati	Immediata revoca accessi	Disabilitazione account e verifica dati locali
Prompt AI	Minimo necessario	Cancellazione/evitare archivi paralleli

8. Misure tecniche e organizzative ex art. 32 GDPR

• Credenziali individuali e divieto di condivisione account.

• MFA per email, cloud, gestionale e account critici quando disponibile.

• Separazione degli accessi per ruolo e principio del minimo privilegio.

• Backup giornaliero dei sistemi critici e test periodico di ripristino.

• Aggiornamenti, endpoint protection e gestione delle vulnerabilità.

• Cifratura o protezione equivalente per dispositivi mobili e supporti quando proporzionata.

• Procedure per onboarding/offboarding e revoca immediata degli accessi.

• Istruzioni scritte, formazione annuale e simulazioni phishing proporzionate.

• Procedure di data breach e registro degli incidenti.

• Policy AI: divieto di inserire dati sanitari in strumenti non autorizzati.

9. Trasferimenti internazionali

Servizio	Ruolo / verifica	Garanzia documentale
Google Workspace Business	Provider cloud - verificare localizzazione e subfornitori	DPA, SCC/DPF ove applicabile, impostazioni account
ChatGPT Business	Provider AI - verificare trattamento per conto e ulteriori finalità	DPA/termini business, SCC/DPF ove applicabile, minimizzazione
Sistema prenotazioni	Provider SaaS UE - esempio	DPA e data location documentata

10. Valutazione d’impatto sulla protezione dei dati (DPIA)

Esito: DPIA necessaria per il perimetro sanitario digitale e per l’uso combinato di dati relativi alla salute, sistemi diagnostici, cloud e strumenti AI.

Finalità e necessità. La valutazione considera i trattamenti indispensabili alla prestazione sanitaria e ai processi connessi. Sono escluse finalità non necessarie o sproporzionate.

Interessati: pazienti, minori quando presenti, dipendenti, candidati e professionisti.

Flusso principale: raccolta dati -> agenda/accettazione -> prestazione sanitaria -> refertazione -> consegna -> archiviazione -> eventuale fatturazione.

Minaccia	Prob.	Impatto	Rischio iniziale	Misure	Residuo
Accesso non autorizzato a cartelle sanitarie	Media	Molto alto	Alto	Ruoli, MFA, audit log, accessi nominativi	Medio
Invio referto al destinatario sbagliato	Media	Alto	Alto	Doppia verifica destinatario, canali sicuri, procedura consegna	Basso/Medio
Ransomware / indisponibilità gestionale	Media	Molto alto	Alto	Backup isolato, EDR, patching, test restore, piano continuità	Medio
Furto notebook / smartphone	Bassa	Alto	Medio	Cifratura, PIN forte, MDM/remote wipe, minimizzazione locale	Basso
Accesso tecnico non controllato a ecografo	Media	Alto	Alto	Assistenza su ticket, supervisione, account tecnico, log	Medio
Dismissione dispositivo con dati residui	Bassa	Alto	Medio	Cancellazione certificata / distruzione supporti	Basso
Inserimento dati sanitari in AI non autorizzata	Media	Molto alto	Alto	Policy AI, blocco procedure, formazione, account approvati	Medio
Trasferimento extra SEE non governato	Media	Alto	Alto	Mappatura provider, DPA, SCC/DPF, minimizzazione	Medio
Account condivisi tra operatori	Media	Alto	Alto	Account nominativi, revisione accessi, offboarding	Basso/Medio

10.1 Necessità e proporzionalità

Minimizzazione	Raccogliere solo i dati clinici e amministrativi necessari; evitare duplicazioni in email, chat e dispositivi personali.
Accessi	Ruoli distinti tra sanitario, reception, amministrazione e tecnico IT.
Conservazione	Termini differenziati per documentazione sanitaria, contabile, candidature e log.
Trasparenza	Informative integrate per categoria di interessato; consensi separati solo per finalità che li richiedono.
Diritti	Canale privacy dedicato e procedura interna per rispondere entro i termini GDPR.
AI	Solo uso assistivo; nessuna decisione clinica automatizzata; controllo umano obbligatorio.
Fornitori	DPA, ruolo privacy, subfornitori, data location e misure verificati prima dell'uso.

10.2 Piano di miglioramento

Priorità	Azione	Responsabile	Scadenza
Alta	Attivare MFA su tutti gli account critici	Titolare / IT	30 giorni
Alta	Verificare DPA e data location provider AI/cloud	Privacy owner	30 giorni
Media	Test documentato di ripristino backup	IT	60 giorni
Media	Formazione personale su data breach e AI	Titolare	60 giorni
Media	Revisione matrice accessi e account cessati	Amministrazione	Trimestrale

Conclusione DPIA: il trattamento può proseguire con le misure previste e il piano di miglioramento indicato. La DPIA deve essere riesaminata in caso di nuovi sistemi, nuove finalità, incidenti significativi, modifica dei provider o aumento rilevante della scala.

11. Procedura e Registro Data Breach

Una violazione di dati personali comprende distruzione, perdita, modifica, divulgazione non autorizzata o accesso illecito ai dati.

Esempi per il settore sanitario

• Referto inviato alla persona sbagliata.

• Accesso alla cartella di un paziente non assistito dall'operatore.

• Furto di credenziali email o gestionale.

• Ransomware che rende indisponibili cartelle o immagini.

• Smarrimento smartphone con chat di servizio.

• Esportazione non autorizzata di immagini diagnostiche.

Procedura interna

• Segnalazione immediata al Titolare/Privacy owner.

• Registrazione di data, ora, sistemi, categorie dati e interessati.

• Contenimento e conservazione delle evidenze.

• Valutazione probabilità e gravità del rischio.

• Notifica al Garante, se dovuta, senza ingiustificato ritardo e ove possibile entro 72 ore.

• Comunicazione agli interessati quando il rischio è elevato.

• Chiusura con cause, misure correttive e lesson learned.

N.	Data	Evento	Sistemi	Dati	Interessati	Rischio	Notifica	Azioni

12. Gestione dei diritti degli interessati

Diritto	Procedura interna
Accesso	Verifica identità; ricerca nei sistemi; copia comprensibile senza ledere diritti altrui.
Rettifica	Correzione e propagazione ai sistemi/fornitori pertinenti.
Cancellazione	Verifica obblighi sanitari, fiscali, difesa dei diritti ed eccezioni.
Limitazione	Contrassegno e blocco degli usi non consentiti.
Portabilità	Formato strutturato quando applicabile.
Opposizione	Valutazione motivi prevalenti; stop immediato del marketing.

13. Governance di consulenti, fornitori e piattaforme

Regola operativa. Non tutti i soggetti esterni firmano una nomina art. 28. Per cloud, SaaS e AI si conservano DPA e condizioni del provider quando applicabili; per professionisti autonomi non si genera una nomina impropria.

Soggetto	Qualificazione	Documento	Firma
Commercialista Demo	Professionista esterno: ruolo da verificare per i flussi concreti	Incarico + eventuale art. 28 solo se ricorrono i requisiti	Non automatica
Consulente lavoro Demo	Professionista esterno / possibile ruolo misto	Incarico + verifica flussi; art. 28 solo se necessario	Non automatica
Medico competente Demo	Titolare autonomo nelle funzioni proprie	Censimento rapporto e flussi	No nomina art. 28
IT DEMO S.R.L.	Responsabile ex art. 28 per assistenza con accesso ai dati	Accordo art. 28 o DPA conforme	Sì se si usa accordo ImpresaAI
Google Workspace Business	Provider SaaS/cloud	DPA/termini provider + verifica data location	No facsimile ImpresaAI
ChatGPT Business	Provider AI	DPA/termini business + verifica trasferimenti	No facsimile ImpresaAI
Booking Medical Demo	Provider prenotazioni	DPA e condizioni servizio	No duplicazione DPA valido

13A. Accordo ex art. 28 - Responsabile esterno diretto

IT DEMO S.R.L. - società informatica fittizia

P.IVA/C.F.	DEMO-IT-0001
Sede	Via Demo 20 - Lecce
Email/PEC	privacy@itdemo.example
Oggetto	Assistenza e manutenzione informatica con possibile accesso ai dati per conto del Titolare.
Qualificazione	Responsabile del trattamento ex art. 28 GDPR per le attività svolte per conto del Titolare.

• Trattamento solo su istruzioni documentate del Titolare.

• Obbligo di riservatezza del personale autorizzato.

• Misure tecniche e organizzative adeguate.

• Sub-responsabili soggetti a obblighi equivalenti.

• Assistenza per diritti, DPIA, sicurezza e data breach.

• Notifica degli incidenti senza ingiustificato ritardo.

• Restituzione/cancellazione dei dati a fine servizio, salvo obblighi legali.

Il Titolare - data e firma	Il Responsabile - data e firma
_____	_____

14. Atti di autorizzazione al trattamento - personale

Marco Bianchi - Medico collaboratore

Asset autorizzati: Gestionale sanitario, Referti, Immagini diagnostiche

• Accedere solo ai dati necessari alla mansione.

• Usare esclusivamente credenziali personali e non condividerle.

• Verificare il destinatario prima di inviare email, referti o messaggi.

• Non usare cloud, dispositivi o account personali non autorizzati.

• Bloccare il dispositivo quando ci si allontana.

• Segnalare immediatamente errori, phishing, perdita di dispositivi o altri incidenti.

• Non inserire dati sanitari in strumenti AI non autorizzati.

Titolare - data e firma	Persona autorizzata - data e firma
_____	_____

Elena Verdi - Reception

Asset autorizzati: Agenda, Anagrafica, Email/telefono

• Accedere solo ai dati necessari alla mansione.

• Usare esclusivamente credenziali personali e non condividerle.

• Verificare il destinatario prima di inviare email, referti o messaggi.

• Non usare cloud, dispositivi o account personali non autorizzati.

• Bloccare il dispositivo quando ci si allontana.

• Segnalare immediatamente errori, phishing, perdita di dispositivi o altri incidenti.

• Non inserire dati sanitari in strumenti AI non autorizzati.

Titolare - data e firma	Persona autorizzata - data e firma
_____	_____

Paolo Neri - Amministrazione

Asset autorizzati: Fatturazione, Fornitori, Home banking

• Accedere solo ai dati necessari alla mansione.

• Usare esclusivamente credenziali personali e non condividerle.

• Verificare il destinatario prima di inviare email, referti o messaggi.

• Non usare cloud, dispositivi o account personali non autorizzati.

• Bloccare il dispositivo quando ci si allontana.

• Segnalare immediatamente errori, phishing, perdita di dispositivi o altri incidenti.

• Non inserire dati sanitari in strumenti AI non autorizzati.

Titolare - data e firma	Persona autorizzata - data e firma
_____	_____

Sara Blu - Infermiere

Asset autorizzati: Cartella sanitaria necessaria, Agenda clinica

• Accedere solo ai dati necessari alla mansione.

• Usare esclusivamente credenziali personali e non condividerle.

• Verificare il destinatario prima di inviare email, referti o messaggi.

• Non usare cloud, dispositivi o account personali non autorizzati.

• Bloccare il dispositivo quando ci si allontana.

• Segnalare immediatamente errori, phishing, perdita di dispositivi o altri incidenti.

• Non inserire dati sanitari in strumenti AI non autorizzati.

Titolare - data e firma	Persona autorizzata - data e firma
_____	_____

Luca Gialli - Assistente

Asset autorizzati: Agenda, Documenti organizzativi

• Accedere solo ai dati necessari alla mansione.

• Usare esclusivamente credenziali personali e non condividerle.

• Verificare il destinatario prima di inviare email, referti o messaggi.

• Non usare cloud, dispositivi o account personali non autorizzati.

• Bloccare il dispositivo quando ci si allontana.

• Segnalare immediatamente errori, phishing, perdita di dispositivi o altri incidenti.

• Non inserire dati sanitari in strumenti AI non autorizzati.

Titolare - data e firma	Persona autorizzata - data e firma
_____	_____

15. Informative Privacy operative - stampabili singolarmente

15.1 Informativa Privacy pazienti e utenti - include i dati relativi alla salute

Voce	Informazione
Titolare	STUDIO MEDICO AURORA S.R.L. - dati fittizi
Dati trattati	Dati identificativi, contatti, amministrativi e, quando necessari alla prestazione, dati relativi alla salute, anamnesi, referti e immagini diagnostiche.
Finalità	Prenotazione, accettazione, diagnosi, assistenza, cura, refertazione, fatturazione e adempimenti.
Base giuridica	Art. 6.1.b/c GDPR; per i dati salute necessari alla prestazione sanitaria, art. 9.2.h GDPR quando applicabile. Il consenso non è richiesto quando il trattamento sanitario è necessario e ricorre tale presupposto.
Destinatari	Personale autorizzato, professionisti sanitari e fornitori strettamente necessari.
Conservazione	Secondo normativa sanitaria, fiscale e tutela dei diritti.
Trasferimenti	Solo se necessari e con garanzie artt. 44-49 GDPR.
Natura conferimento	I dati indispensabili alla prestazione e agli obblighi sono necessari; le finalità ulteriori sono facoltative.

Diritti. L'interessato può esercitare, quando applicabili, i diritti previsti dagli artt. 15-22 GDPR scrivendo a privacy@studioaurora.demo o via PEC a studioaurora@pec.demo. Il riscontro viene fornito di regola entro un mese, salvo proroghe consentite. È possibile proporre reclamo al Garante per la protezione dei dati personali.

Ricezione e presa visione. La firma attesta la consegna dell'informativa e non costituisce consenso ai trattamenti fondati su contratto, legge o altro presupposto.

Nome e cognome	Luogo e data	Firma
_____	_____	_____

15.2 Informativa Privacy dipendenti e collaboratori

Voce	Informazione
Titolare	STUDIO MEDICO AURORA S.R.L.
Dati	Anagrafici, contrattuali, retributivi, fiscali, previdenziali e dati salute necessari al lavoro/sicurezza.
Finalità	Gestione rapporto, paghe, presenze, sicurezza, formazione e obblighi.
Base giuridica	Art. 6.1.b/c GDPR; art. 9.2.b per dati particolari connessi al lavoro.
Destinatari	Consulente lavoro, enti, medico competente nei limiti del ruolo, fornitori necessari.
Conservazione	Rapporto + termini legali/previdenziali.
Consenso	Non richiesto per i trattamenti necessari al rapporto o agli obblighi di legge.

Diritti. L'interessato può esercitare, quando applicabili, i diritti previsti dagli artt. 15-22 GDPR scrivendo a privacy@studioaurora.demo o via PEC a studioaurora@pec.demo. Il riscontro viene fornito di regola entro un mese, salvo proroghe consentite. È possibile proporre reclamo al Garante per la protezione dei dati personali.

Ricezione e presa visione. La firma attesta la consegna dell'informativa e non costituisce consenso ai trattamenti fondati su contratto, legge o altro presupposto.

Nome e cognome	Luogo e data	Firma
_____	_____	_____

15.3 Informativa Privacy candidati

Voce	Informazione
Dati	CV, contatti, esperienze, titoli e informazioni spontanee.
Finalità	Valutazione della candidatura e selezione.
Base giuridica	Art. 6.1.b GDPR per misure precontrattuali richieste dall'interessato.
Natura	Conferimento facoltativo, ma senza i dati essenziali non è possibile valutare la candidatura.
Conservazione	Periodo della selezione + termine proporzionato e documentato.
Consenso	Non richiesto per la mera valutazione della candidatura quando opera l'art. 6.1.b.

Diritti. L'interessato può esercitare, quando applicabili, i diritti previsti dagli artt. 15-22 GDPR scrivendo a privacy@studioaurora.demo o via PEC a studioaurora@pec.demo. Il riscontro viene fornito di regola entro un mese, salvo proroghe consentite. È possibile proporre reclamo al Garante per la protezione dei dati personali.

Ricezione e presa visione. La firma attesta la consegna dell'informativa e non costituisce consenso ai trattamenti fondati su contratto, legge o altro presupposto.

Nome e cognome	Luogo e data	Firma
_____	_____	_____

15.4 Informativa Privacy fornitori e referenti professionali

Voce	Informazione
Dati	Identificativi, ruolo professionale, fiscali, amministrativi e bancari.
Finalità	Ordini, pagamenti, contabilità, adempimenti e gestione del rapporto.
Base giuridica	Art. 6.1.b/c GDPR; eventuale interesse legittimo documentato.
Destinatari	Personale autorizzato, banche, commercialista, enti e fornitori necessari.
Conservazione	Durata rapporto + termini civilistici/fiscali.
Consenso	Non previsto per i trattamenti necessari al rapporto o agli obblighi.

Diritti. L'interessato può esercitare, quando applicabili, i diritti previsti dagli artt. 15-22 GDPR scrivendo a privacy@studioaurora.demo o via PEC a studioaurora@pec.demo. Il riscontro viene fornito di regola entro un mese, salvo proroghe consentite. È possibile proporre reclamo al Garante per la protezione dei dati personali.

Ricezione e presa visione. La firma attesta la consegna dell'informativa e non costituisce consenso ai trattamenti fondati su contratto, legge o altro presupposto.

Nome e cognome	Luogo e data	Firma
_____	_____	_____

15.5 Informativa Privacy sito web e richieste online

Voce	Informazione
Dati	Dati inseriti nei moduli, dati tecnici di navigazione e prenotazione.
Finalità	Gestione richieste, sicurezza tecnica e servizi online.
Base giuridica	Art. 6.1.b/f GDPR; consenso per tecnologie che lo richiedono.
Destinatari	Hosting e fornitori tecnici necessari.
Conservazione	Secondo finalità e policy tecnica documentata.

Diritti. L'interessato può esercitare, quando applicabili, i diritti previsti dagli artt. 15-22 GDPR scrivendo a privacy@studioaurora.demo o via PEC a studioaurora@pec.demo. Il riscontro viene fornito di regola entro un mese, salvo proroghe consentite. È possibile proporre reclamo al Garante per la protezione dei dati personali.

Ricezione e presa visione. La firma attesta la consegna dell'informativa e non costituisce consenso ai trattamenti fondati su contratto, legge o altro presupposto.

Nome e cognome	Luogo e data	Firma
_____	_____	_____

15.6 Informativa e consenso marketing / newsletter

Voce	Informazione
Dati	Nome, email, telefono, preferenze e storico consenso.
Finalità	Newsletter e comunicazioni promozionali.
Base giuridica	Consenso ex art. 6.1.a GDPR quando richiesto.
Natura	Facoltativa; il rifiuto non incide sulla prestazione sanitaria.
Revoca	In qualsiasi momento via email/PEC o link di disiscrizione.

Diritti. L'interessato può esercitare, quando applicabili, i diritti previsti dagli artt. 15-22 GDPR scrivendo a privacy@studioaurora.demo o via PEC a studioaurora@pec.demo. Il riscontro viene fornito di regola entro un mese, salvo proroghe consentite. È possibile proporre reclamo al Garante per la protezione dei dati personali.

Ricezione e presa visione. La firma attesta la consegna dell'informativa e non costituisce consenso ai trattamenti fondati su contratto, legge o altro presupposto.

Nome e cognome	Luogo e data	Firma
_____	_____	_____

Consenso facoltativo - solo per la finalità specifica

■ ACCONSENTO alle comunicazioni promozionali descritte. ■ NON ACCONSENTO.
Data _____ Firma _____

16. AI Policy e Registro dei sistemi di Intelligenza Artificiale

Strumento dichiarato: ChatGPT Business - esempio dimostrativo.

Finalità: supporto alla redazione di comunicazioni e documenti amministrativi; nessuna decisione clinica automatizzata.

• Usare solo account aziendali autorizzati.

• Non inserire dati sanitari o documenti clinici salvo specifica procedura, necessità e configurazione contrattuale adeguata.

• Preferire anonimizzazione/pseudonimizzazione dei dati.

• Verificare sempre gli output prima dell'uso.

• Non usare AI per decisioni con effetti significativi sulle persone senza analisi specifica.

• Registrare provider, finalità, utenti autorizzati e data di riesame.

• Formare periodicamente il personale sugli usi consentiti e vietati.

Strumento	Finalità	Dati ammessi	Utenti	Riesame
ChatGPT Business	Supporto amministrativo	Dati minimizzati / no dati salute salvo procedura	Titolare + amministrazione autorizzata	Annuale o a modifica rilevante

17. Approvazione e riesame

Riesame almeno annuale e ogni volta che cambiano attività, sedi, personale, sistemi, provider, categorie di dati, finalità o si verifica un incidente significativo.

Titolare - approvazione	Data riesame successivo
_____	_____

FINE DEMO - Questo documento è un esempio commerciale con dati interamente fittizi. Il Fascicolo reale viene generato sulle informazioni confermate dal cliente.