VALUTAZIONE D'IMPATTO e DEI RISCHISULLA PROTEZIONE DEI DATI

(Art. 35 Regolamento UE 679/2016, "RGPD")

A. INTESTAZIONE

Valutazione di impatto e dei rischi sulla protezione dei dati personali attinenti ai dati personali trattati per la finalità "*di attività di ricerca scientifica*"

B. INFORMAZIONI GENERALI

Titolare del trattamento:

FONDAZIONE DON CARLO GNOCCHI ONLUS – ONG – IRCCS, (di seguito "Fondazione") persona giuridica privata, con sede legale in Milano, Via Carlo Girola n.30.

RPD – Responsabili della Protezione dei Dati:

- **Fondazione Don Carlo Gnocchi ONLUS:** privacy@dongnocchi.it, oppure rpd@dongnocchi.it
- Azienda Ospedaliera Nazionale SS. Antonio e Biagio e Cesare Arrigo:dpo@ospedale.al.it
- ARNAS "G.Brotzu":dpo@aob.it.
- AOU San Giovanni di Dio e Ruggi d'Aragona: dpo@pec.sangiovannieruggi.it.
- ASST Grande Ospedale Metropolitano Niguarda: dpo@ospedaleniguarda.it.
- Università Carlo Cattaneo LIUC: rpd@liuc.it
- Policlinico San Matteo:dpo@smatteo.pv.it
- Azienza Ospedaliera-Universitaria Senese:privacy@ao-siena.toscana.it.
- Humanitas Clinical and Research Center IRCCS:dataprotectionofficer@humanitas.it
- AOU Città della Salute e della Scienza: dpo@cittadellasalute.to.it
- Policlinico S. Orsola Malpighi:dpo@aosp.bo.it
- Ospedale San Giovanni Bosco: stefano.gallarato@pec.avvocati.torino.it, wan@salesianipiemonte.it
- Azienda Ospedaliera Universitaria Ospedali Riuniti di Ancona: urp@ospedaliriuniti.marche.it
- Ospedali Civili, Brescia: rpd@asst-spedalicivili.it
- Azienda Unità Sanitaria Locale di Piacenza:dpo@ausl.pc.it

Data di creazione della presente Valutazione:

27/10/2025

Date degli eventuali aggiornamenti successivi:

- -/--/----

C. CONTESTO

1. **TRATTAMENTO SOTTOPOSTO A VALUTAZIONE D'IMPATTO**
   I Contitolari per la realizzazione dello studio e soltanto nella misura in cui siano indispensabili in relazione all'obiettivo dello studio stesso, in accordo alle responsabilità previste dalle norme di buona pratica clinica (D. Lgs. 211/2003), sono Titolari delle operazioni di trattamento correlate all'effettuazione

dell'attività di ricerca scientifica e tratteranno i dati personali del paziente e/o della persona amministratrice/rappresentante legale, definiti comuni e particolari.
L'acquisizione di tali dati sarà finalizzata esclusivamente alla realizzazione dello "studio" e soltanto nella misura in cui siano indispensabili in relazione all'obiettivo dello studio stesso nonché ai fini di vigilanza.

I dati raccolti sono relativi al trattamento in emergenza nei pazienti con shock cardiogeno (dati comuni, personali, rilevazioni biochimiche) e anche alle condizioni di follow-up in particolare alla valutazione di qualità di vita e alle esperienze avute in ambito sanitario.
Trattandosi di una patologia purtroppo contraddistinta da elevata mortalità nella fase acuta e nel successivo follow up, per cui la spesa sanitaria è altissima e ancora improntata a gap importanti di conoscenza, i dati potranno essere condivisi con altre casistiche (ovviamente con il solito dato pseudonimo) e ai fini di researchoutcome e di valutazione di costo efficacia per informare i decisori.

La raccolta delle informazioni dei pazienti già inclusi può esitare in una delle seguenti possibilità:

- il paziente è deceduto
- il paziente è sopravvissuto, ma con gradi di disabilità che non gli consentono di prestare informativa e consenso scritta
- il paziente è in grado di fornire informativa e consenso, ma le condizioni logistiche (gli hub accolgono spesso pazienti che abitano in zone limitrofe) non glielo consentono
- il paziente è in grado di prestare informativa e consenso.

Includere solo i pazienti in grado di prestare informativa e consenso introdurrebbe un bias inaccettabile nella ricerca, ignorando anche il principio di equità, perché escluderebbe non solo i più gravi e deceduti, ma anche i pazienti con minore literacy e/o socialmente più fragili, che sono proprio i pazienti a maggiore disagio.
Pertanto si prevede di raccogliere il consenso sia in modalità cartacea, che in modalità telefonica quando la cartacea non è perseguibile. L'acquisizione del consenso in modalità telefonica dovrà avvenire secondo specifica proceduraadeguata perla raccolta di un consenso valido secondo le indicazioni del GDPR del Garante Privacy,che consiste nella registrazione della telefonata, lettura delle generalità del soggetto e dell'informativa sintetica, domanda specifica sul prestare o meno il consenso.
Potranno essere raccolti anche i dati acquisiti da caregiver nel caso in cui il paziente sia impossibilitato a rispondere.

Parte del progetto è una analisi approfondita con la LIUC (Business School Castellanza) per l'analisi dei flussi, ai fini della valutazione multidimensionale per informare successivamente i decisori.
Questo può fornire informazioni importanti e innovative (anche in termini di distribuzione della spesa sanitaria) per la presa in carico dei pazienti con sindrome post-critica nel paziente con shock cardiogeno.

2. **RESPONSABILITÀ CONNESSE AL TRATTAMENTO**

"Soggetti designati"

la Dr.ssa Nuccia Morici, Responsabile Cardiologia Riabilitativa in servizio presso il Dipartimento Cardio-Respiratorio del centro S.Maria Nascente, Fondazione Don Carlo Gnocchi, P.I. dello studio.

"Autorizzati/incaricati"I Responsabili e agli Incaricati/autorizzati della Fondazione appositamente nominati e/o individuati nel rispetto dei propri ambiti di competenza e comunque al solo personale coinvolto nello "studio"personale amministrativo e sanitario in carico presso i centri arruolanti

Dr. Marco Corda, ARNAS "G.Brotzu",
Dr.ssa Amelia Ravera, Azienda ospedaliera universitaria San Giovanni di Dio e Ruggi d'Aragona,
Dr.ssa Laura Garatti; ASST Grande Ospedale Metropolitano Niguarda, Milano.
Dr.ssa Emanuela Foglia Università Carlo Cattaneo LIUC,
Dr. Guido Tavazzi Policlinico San Matteo, Pavia

Dr.ssa Serafina Valente Azienza Ospedaliera-Universitaria Senese
Dr.ssa Martina Briani Humanitas Clinical and Research Center IRCCS
Dr. Simone Frea Ospedale AOU Città della Salute e della Scienza
Dr. Luciano Potena Policlinico S. Orsola Malpighi
Dr. Maurizio Bertaina Ospedale San Giovanni Bosco
Dr. Marco Marini Azienda Ospedaliera Universitaria Ospedali Riuniti di Ancona
Dr. Marco Metra Ospedali Civili, Brescia
Dr.ssa Daniela Aschieri Azienda Unità Sanitaria Locale di Piacenza

E' stato definito congiuntamente responsabile della raccolta dati un ricercatore di fondazione don gnocchi ingaggiato con i fondi della ricerca PNRR per supportare tutti i centri nelle informazioni della raccolta di follow-up.

3. **RESPONSABILI DEL TRATTAMENTO (art.28 RGPD)**
   n.a.

4. **SUB-RESPONSABILI DEL TRATTAMENTO (Art.28 paragrafo 4)**
   n.a.

5. **CONTITOLARI DEL TRATTAMENTO (Art.26 RGPD)**

- Fondazione Don Carlo Gnocchi ONLUS, persona giuridica privata, con sede legale in Milano, Via Carlo Girola n.30;
- L'Azienda Ospedaliera Nazionale SS. Antonio e Biagio e Cesare Arrigo, Alessandria 15121 in Via Venezia 16.
- ARNAS "G.Brotzu", P.le Ricchi 1 Cagliari. 09134
- Azienda ospedaliera universitaria San Giovanni di Dio e Ruggi d'Aragona, Via San Leonardo Salerno 8413.
- ASST Grande Ospedale Metropolitano Niguarda, Milano. Piazza Ospedale Maggiore 3, 20162
- Università Carlo Cattaneo LIUC, LIUC Business School, Castellanza Varese Corso Matteotti 22. 21053
- Policlinico San Matteo, Pavia Viale Camillo Golgi 19, 27100
- Azienza Ospedaliera-Universitaria Senese Via Strada delle Scotte 14 Siena 53100
- Humanitas Clinical and Research Center IRCCS, Via Manzoni 56 Rozzano, 20100 Milano
- Ospedale AOU Città della Salute e della Scienza, Corso Bramante 88Torino 10126
- Policlinico S. Orsola Malpighi, Via Pietro Albertoni 15 Bologna 40138
- Ospedale San Giovanni Bosco, Via Caboto 27 Torino 10129
- Azienda Ospedaliera Universitaria Ospedali Riuniti di Ancona Via Conca 71 Ancona
- Ospedali Civili, Brescia Piazzale Spedali
- Azienda Unità Sanitaria Locale, Piacenza Via Antonio Anguissola 15

6. **RISORSE DI SUPPORTO AI DATI**
   a) Supporti cartacei (Clinical Report Form ad-hoc)
   b) Sistemi applicativi di Fondazione (Office 365)
   c) Applicativo on-line per la ricerca RedCap- I dati saranno acquisiti utilizzando un software dedicato (REDCap, https://www.project-redcap.org/), che consente controlli di qualità. É un'applicazione web per la gestione di sondaggi online e database che garantirà adeguate pratiche di sicurezza. REDCAP multi-sito situato presso l'ASST Niguarda, Grande Ospedale Metropolitano di Milano, Italia

7. **PERIODO DI CONSERVAZIONE DEI DATI**
   I dati raccolti saranno trattati e conservati per il tempo necessario al raggiungimento delle finalità perseguite dallo specifico "studio", rispettando il principio di minimizzazione (art. 5, comma 1, lett. c del

GDPR) nonché gli obblighi di legge, dopodiché saranno conservati per 10 anni dalla conclusione dello studio stesso.

8. **TRASFERIMENTO ALL'ESTERO**
I dati personali saranno trattati unicamente all'interno dei territori dello Spazio Economico Europeo. Qualora, per esigenze tecniche o operative impreviste, si rendesse necessario un trasferimento verso Paesi terzi, questo avverrà solo previa adozione di garanzie adeguate ai sensi degli artt. 44-49 del GDPR e previa informazione agli interessati.

D. PRINCIPI FONDAMENTALI

9. **PROPORZIONALITÀ E NECESSITÀ**
I cotitolari utilizzeranno i dati personali forniti esclusivamente per le attività connesse alla realizzazione dello "studio" e soltanto nella misura in cui siano indispensabili in relazione all'obiettivo dello studio stesso nonché ai fini di vigilanza.
I dati saranno acquisiti utilizzando un software dedicato (REDCap, https://www.project-redcap.org/), che consente controlli di qualità e impedisce inserimenti di dati fuori range. Allo stesso modo, la soluzione proposta genererà avvisi in caso di dati mancanti e acquisizioni incomplete. La qualità dei dati sarà verificata periodicamente attraverso analisi preliminari per evitare il rischio di mancata informazione o dati anomali legati a un processo errato di inserimento dati. I dati identificabili contenuti nei file cartacei, come i moduli di consenso e di valutazione, verranno conservati in armadietti chiusi a chiave presso il sito dove vengono raccolti i dati.
I dati elettronici verranno inseriti in forma pseudonimizzata e conservati nel server centrale REDCap multi-sito situato presso l'ASST Niguarda Grande Ospedale Metropolitano di Milano, Italia.
L'associazione dei dati personali e dell'ID univoco sarà conservata in un file separato. Va notato che solo il principale investigatore e i responsabili di ciascun centro potranno associare il codice di pseudonimizzazione all'identità dei pazienti (per i rispettivi centri). Tale file verrà distrutto al termine della fase di acquisizione dati. L'accesso al database verrà effettuato dopo un processo di autenticazione/autorizzazione, quindi l'accesso sarà garantito solo ai membri del team con accesso autorizzato.
Al termine del progetto, un dataset anonimizzato, completamente documentato, verrà depositato in un repository dati adeguato alla conservazione a lungo termine e sarà conservato per 10 anni.

10. **BASI LEGALI DEL TRATTAMENTO**(art.6 e 9 del RGPD)
Globalmente, la base di legittimità per il trattamento dei dati del paziente, e/o della persona da amministratrice/rappresentante legale, per la suddetta finalità è il Suo libero, esplicito ed inequivocabile consenso, fornito in modalità cartacea o in modalità telefonica, ai sensi dell'articolo 6, comma 1, lettera a) e articolo 9, comma 2, lettera a) del Regolamento UE 679/2016 (di seguito "GDPR") oltre che delle specifiche disposizioni correlate al progetto (Linee Guida per i trattamenti dei dati personali nell'ambito delle sperimentazioni cliniche dei medicinali - Deliberazione Garante Privacy n. 52 del 24.07.2008).
Per una parte dei soggetti arruolati, che si configurano quali: (i) deceduti; (ii) paziente non in grado di fornire consenso ma senza rappresentante legale assegnato, si fa riferimento al punto 5.3.3 dell'Autorizzazione Generale n. 9/2016, secondo cui NON è prevista l'acquisizione del consenso specifico a causa della sussistenza delle seguent iagioni indicate:
- motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso;
- lo studio è volto al miglioramento dello stesso stato clinico in cui versa l'interessato.

Si specifica che i pazienti arruolati nel presente studio apparterranno alle varie categorie secondo la seguente percentuale:
50% non in grado di fornire il consenso perché deceduti o in grave disabilità
25% non in grado di fornire consenso scritto per impossibilità di raggiungere la sede dello studio
25% in grado di fornire consenso

Si evidenzia l'importanza di arruolare tutti i pazienti sopracitati in quanto includere solo i pazienti in grado di prestare informativa e consenso introdurrebbe un bias inaccettabile nella ricerca, ignorando anche il principio di equità, perché escluderebbe non solo i più gravi e deceduti, ma anche i pazienti con minore literacy e/o socialmente più fragili, che sono proprio i pazienti a maggiore disagio

11. **MINIMIZZAZIONE DEI DATI PERSONALI**(art.5 RGPD)
I dati selezionati per la raccolta saranno scelti seguendo il principio di minimizzazione dei dati per essere adeguati, rilevanti e limitati a quanto necessario per gli scopi dichiarati del progetto.

12. **AGGIORNAMENTO DEI DATI PERSONALI**
I dati personali saranno mantenuti aggiornati
I dati saranno verificati secondo il principio di esattezza (Data Accuracy)e mantenuti aggiornati fino al completamento dello studio dai contitolari del trattamento dallo study coordinator.I dati inesatti saranno eliminati o rettificati tempestivamente, senza ritardi.
Saranno svolte mensilmente verifiche della qualità del dato, al fine di verificarne la corretta acquisizione e archiviazione. Eventuali errori saranno corretti dal partner responsabile della raccolta del dato specifico secondo apposite modalità.

13. **MISURE A TUTELA DEGLI INTERESSATI**
Nell'informativa privacy allo studio e nella informativa alla partecipazione allo studio clinico sono indicati tutti i riferimenti a cui l'interessato può rivolgere le sue richieste

E. MISURE DI SICUREZZA

14. **CONTROLLO DEGLI ACCESSI LOGICI/INFORMATICI**
I dati saranno acquisiti utilizzando un software dedicato (REDCap, https://www.project-redcap.org/). Molta della sicurezza legata a REDCap si basa sull'infrastruttura IT e sull'ambiente in cui REDCap è stato installato.I dati elettronici verranno conservati su server protetti da password delll'ASST Grande Ospedale Metropolitano Niguarda. L'accesso al database verrà effettuato dopo un processo di autenticazione/autorizzazione; quindi, l'accesso sarà garantito solo ai membri del team con accesso autorizzato. Le autorizzazioni per gli accessi al database, e la creazione delle relative utenze saranno gestite unicamente dall'ASST Grande Ospedale Metropolitano Niguarda. Il REDCap multi-sito sarà strutturato in modo che ciascun sito abbia accesso solo all'interfaccia di inserimento dati e ai dati del proprio sito.

15. **PROFILI DI AUTORIZZAZIONE**
La profilazione degli utenti (ovvero la definizione dei permessi di accesso e utilizzo dei sistemi) è di competenza del team IT dell'ASST GOM Niguarda.
In caso di necessità di modifica delle autorizzazioni, lo study Coordinator di ASST Niguarda invierà una richiesta di autorizzazione ai sistemi IT dell'ASST GOM Niguarda per garantire l'accesso secondo procedura interna.

Relativamente al sistema REDCap,solo il principale investigatore e i responsabili di ciascun centro potranno associare il codice di pseudonimizzazione all'identità dei pazienti (per i rispettivi centri). Tale file verrà distrutto al termine della fase di acquisizione dati. L'accesso al database verrà effettuato dopo un processo di autenticazione/autorizzazione; quindi, l'accesso sarà garantito solo ai membri del team con accesso autorizzato. Il REDCap multi-sito sarà strutturato in modo che ciascun sito abbia accesso solo all'interfaccia di inserimento dati e ai dati del proprio sito. Il sito di coordinamento e il gruppo di analisi dei dati avranno accesso a tutti i dati in forma non identificabile.

16. **SISTEMI ANTIVIRUS – FIREWALL**
- adozione di un sistema antivirus che include anche la funzionalità di personal firewall, con aggiornamento costante;
- adozione di un sistema antispam dotato di funzionalità antimalware;

In generale, tutta l'infrastruttura è protetta da un firewall perimetrale. Un'area di Fondazione particolarmente sensibile (CITT) è ulteriormente protetta da un firewall interno dedicato.

17. BACKUP

Verrà effettuato il backup periodico dei dati sui sistemi ASST GOM Niguarda.

***18.* CIFRATURA DEI DATI**

I PC utilizzati saranno protetti da username e password ed i dati personali saranno salvati sulla memoria del server che gode di crittografia e sicurezza della linea di trasmissione
Un ID univoco, specifico per ciascun centro, sarà automaticamente assegnato dal software alla creazione di ogni nuovo record. L'associazione dei dati personali e dell'ID univoco sarà conservata in un file separato. Va notato che solo il principale investigatore e i responsabili di ciascun centro potranno associare il codice di pseudonimizzazione all'identità dei pazienti (per i rispettivi centri). Tale file verrà distrutto al termine della fase di acquisizione dati

19. PSEUDONIMIZZAZIONE

Sia in supporto cartaceo che in formato digitale verrà utilizzato un codice di pseudonimizzazione che verrà associato all'identità dei pazienti

20. SICUREZZA DEI SUPPORTI CARTACEI

Saranno seguite le procedure di pseudonimizzazione del dato e conservazione sicura descritte nei punti precedenti.
I dati personali e dati particolari (clinici) contenuti su supporti cartacei sono trattati seguendo le specifiche procedure di sicurezza come segue:

- Sono trattati esclusivamente da soggetti incaricati/autorizzati;
- Sono conservati in un luogo definito e chiuso a chiave, la chiave sarà estratta e conservata dal soggetto incaricato/autorizzato
- La stanza di riferimento viene chiusa a fine lavoro o in caso di momentanea assenza.

L'identificazione delle sedi di conservazione ed archiviazione è definita nella procedura interna dell'ASST GOM Niguarda.

21. TRACCIABILITÀ

Saranno tracciate tutte le modifiche effettuate in forma cartacea e digitale tramite monitoraggio settimanale degli sperimentatori coinvolti per quanto riguarda il cartaceo

22. CONTROLLO DEGLI ACCESSI FISICI

Il controllo degli accessi fisici alle locazioni di deposito dei dati cartacei avverrà tramite primo accesso mediante badge personale di riconoscimento, attraverso serratura a chiave per accedere alla stanza di archiviazione dei dati e attraverso ulteriore serratura con chiave per accedere all'armadietto dedicato suddetto.

23. ADOZIONE DI MISURE DI SICUREZZA FISICHE CONTRO EVENTUALI FONTI DI RISCHIO NON UMANE

All'interno della struttura ASST GOM Niguarda sono presenti i seguenti sistemi:
- sistemi antincendio;
- protezioni da allagamento;
- sistemi di continuità erogazione energia elettrica;
- sistemi di climatizzazione dei locali contenenti apparecchiature elettroniche;
- procedure di emergenza;
- rapporti con nuclei di pronto intervento

24. ADOZIONE DI POLICY E PROCEDURE INTERNE

Per ognuna delle misure sopracitate ASST GOM Niguarda ha prodotto e pubblicato una policy specifica.

Il soggetto designato e gli autorizzati al trattamento possono prendere visione di tali policy direttamente dal proprio pc (sono disponibili in apposita cartella dedicata) oppure tramite la Intranet aziendale.

25. FORMAZIONE DEL PERSONALE

La formazione del personale avviene attraverso riunioni dedicate, periodiche tramite presentazioni su slides e affiancamenti.

26. ESISTENZA DI UNA PROCEDURA PER TESTARE, VERIFICARE E VALUTARE L'EFFICACIA DELLE MISURE TECNICHE E ORGANIZZATIVE

Viene svolta una manutenzione costante gestita internamente da ASST Niguarda.

27. VALUTAZIONE SISTEMATICA DEI RISCHI E DELLE RELATIVE MISURE DI MITIGAZIONE

la sperimentazione in oggetto prevede la raccolta di dati in forma pseudonimizzata su applicativo REDCAp dell'ASST Grande Ospedale Metropolitano Niguarda.

Rischi individuati:

Rischio	Descrizione	Gravità	Probabilità	Livello di rischio
R1. Riconducibilità indiretta all'identità dell'interessato	Possibilità che, tramite dati combinati (es. età, patologia rara, centro di raccolta), sia possibile risalire all'identità	Alta	Bassa	Basso
R2. Accessi non autorizzati alla eCRF	Possibile accesso da parte di soggetti non autorizzati alla piattaforma	Alta	Bassa	Bassa
R3. Esfiltrazione dei dati durante la trasmissione	Possibili attacchi man-in-the-middle o intercettazioni	Media	Bassa	Bassa
R4. Uso improprio dei dati da parte di soggetti autorizzati	Accessi ai dati oltre quanto necessario ("overprivilege")	Media	Bassa	Bassa
R5. Errori nella pseudonimizzazione o mancata separazione delle chiavi	Ricollegabilità involontaria ai dati identificativi	Alta	Bassa	Bassa

Misure di mitigazione implementate

Rischio	Misure di mitigazione	Efficacia stimata
R1	- Revisione della struttura dei dataset per minimizzare i dati indirettamente identificabili - Verifica della rarità delle combinazioni (Data Minimization) - Accesso ai dati secondo il principio del minimo privilegio	Alta
R2	- processo di autenticazione/autorizzazione. - Policy di gestione degli account e formazione	Alta
R3	- Cifratura dei dati in transito (TLS 1.2 o superiore) - VPN o rete sicura per accesso alla eCRF	Alta
R4	- Profilazione granulare degli accessi sulla base dei ruoli - Logging e monitoraggio degli accessi - Procedure disciplinari per uso improprio	Media-Alta
R5	- Separazione fisica e logica delle chiavi di pseudonimizzazione - Procedure documentate e test di integrità - Accesso alle chiavi solo da parte di personale specificamente autorizzato	Alta

F. VALUTAZIONE DEI RISCHI

1. ACCESSO ILLEGITTIMO AI DATI

- **Principali possibili impatti**

  - furto d'identità;
  - perdita del controllo sui dati;
  - impossibilità di esercizio dei diritti;
  - danno reputazionale

- **Principali minacce che potrebbero concretizzare il rischio**

  - accesso fisico non autorizzato nei locali e archivi fisici;
  - accesso fisico non autorizzato nei locali server;
  - intercettazione elettronica;
  - furto di documenti o supporti di memorizzazione (HD, pc, cell);
  - furto di credenziali di autenticazione;
  - recupero di informazioni da apparati, componenti dismessi (pc, cellulari, elettromedicali);
  - rivelazione di informazioni (da lavoratori o fornitori);
  - azione di virus informatici o codici malefici,
  - malfunzionamento di apparati di rete;
  - malfunzionamento di software applicativi;
  - modifica deliberata e non autorizzata o involontaria dei dati di configurazione del sistema;
  - utilizzo non conforme alle finalità di raccolta dei dati;
  - degrado/obsolescenza della strumentazione (memorie di massa).

- **Fonti di rischio**

  - fonti umane interne;
  - fonti umane esterne;
  - fonti non umane.

- **Misure, tra quelle individuate, che contribuiscono a mitigare il rischio**

  - controllo degli accessi logici;
  - profili di autorizzazione;
  - sistemi antivirus – firewall;
  - cifratura dei dati;
  - pseudonimizzazione;
  - sicurezza dei supporti cartacei;
  - tracciabilità;
  - controllo degli accessi fisici;
  - adozione di policy e procedure interne;
  - formazione del personale;
  - esistenza di una procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative;
  - controllo degli accessi fisici ai locali dedicati alla ricerca scientifica;
  - conservazione, utilizzo e trasporto dei campioni biologici in modalità sicura;
  - trasferimento dei dati genetici in formato elettronico in modalità sicura.

GRAVITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA GRAVITA' EFFETTIVA ELIDENDO LE ALTRE)

La gravità effettiva dei rischi derivanti da accesso illegittimo ai dati è ritenuta, mediamente:
"**basso**" (punteggio di __1__ in una scala di criterio di giudizio che si riassumono in un punteggio da 1 a 4), in quanto potrebbe determinare effetti lievi (p.e. fastidio), sulla vita sociale o personale degli interessati in termini di:
"

PROBABILITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA PROBABILITA'' EFFETTIVA ELIDENDO LE ALTRE)

La probabilità effettiva del rischio, anche alla luce delle misure di sicurezza esistenti o pianificate, è ritenuta, mediamente,
"**rara**" (punteggio di _1__, in una scala di criteri di giudizio che si riassumono in un punteggio da 1 a 4), in quanto il verificarsi del danno ipotizzato susciterebbe una grande sorpresa e incredulità. La gestione dell'attività, in termini di sicurezza, è ritenuta buona, salvo qualche lacuna.

INDICE DI RISCHIO: R X P = G = ___1_____(molto alto – alto – Medio – basso)

Tutti i centri condividono i contenuti dell'attuale documento, la descrizione del trattamento e i presupposti di legittimità degli stessi, la natura e la valutazione dei rischi per diritti e libertà degli interessati. Valutano il rischio residuo come basso e riservano l'applicazione di ulteriori misure di sicurezza secondo le misure tecnico-amministrative di cui ciascun titolare dispone internamente, sempre in conformità con il livello adeguati delle stesse, secondo quanto previsto dal regolamento UE 619 del 2016.

2. MODIFICHE INDESIDERATE DEI DATI

- **Principali possibili impatti**

  - furto d'identità;
  - perdita del controllo sui dati;
  - impossibilità di esercizio dei diritti;
  - danno reputazionale.

- **Principali minacce che potrebbero concretizzare il rischio**
  - accesso fisico non autorizzato nei locali e archivi fisici;
  - accesso fisico non autorizzato nei locali server;
  - disturbi elettromagnetici;
  - intercettazione elettronica;
  - furto di credenziali di autenticazione;
  - azione di virus informatici o codici malefici;
  - malfunzionamento apparati di rete;
  - malfunzionamento software applicativi;
  - degrado/obsolescenza della strumentazione (memorie di massa).

- **Fonti di rischio**
  - fonti umane interne;
  - fonti umane esterne;
  - fonti non umane.

- **Misure, tra quelle individuate, che contribuiscono a mitigare il rischio**
  - controllo degli accessi logici;
  - profili di autorizzazione;
  - sistemi antivirus;

- firewall;
- backup;
- cifratura dei dati;
- pseudonimizzazione;
- sicurezza dei supporti cartacei;
- tracciabilità;
- controllo degli accessi fisici;
- adozione di policy e procedure interne;
- formazione del personale;
- esistenza di una procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative;
- controllo degli accessi fisici ai locali dedicati alla ricerca scientifica;
- conservazione, utilizzo e trasporto dei campioni biologici in modalità sicura;
- trasferimento dei dati genetici in formato elettronico in modalità sicura.

GRAVITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA GRAVITA' EFFETTIVA ELIDENDO LE ALTRE)

La gravità effettiva dei rischi derivanti da accesso illegittimo ai dati è ritenuta, mediamente:
"**basso**" (punteggio di __1__ in una scala di criterio di giudizio che si riassumono in un punteggio da 1 a 4), in quanto potrebbe determinare effetti lievi (p.e. fastidio), sulla vita sociale o personale degli interessati in termini di:
- furto d'identità;
- perdita sul controllo dei dati;
- impossibilità di esercizio dei diritti;
- danno reputazionale.

PROBABILITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA PROBABILITA'' EFFETTIVA ELIDENDO LE ALTRE)

La probabilità effettiva del rischio, anche alla luce delle misure di sicurezza esistenti o pianificate, è ritenuta, mediamente,
"**raro**" (punteggio di _1__, in una scala di criteri di giudizio che si riassumono in un punteggio da 1 a 4), in quanto il verificarsi del danno ipotizzato susciterebbe una grande sorpresa e incredulità. La gestione dell'attività, in termini di sicurezza, è ritenuta buona, salvo qualche lacuna.
.

INDICE DI RISCHIO: R X P = G = __1_____ (molto alto – alto – Medio – basso)

3. PERDITA DEI DATI

- **Principali possibili impatti**
  - furto d'identità;
  - danni fisici o psicologici;
  - perdita del controllo sui dati;
  - impossibilità di esercizio dei diritti.

- **Principali minacce che potrebbero concretizzare il rischio**
  - incendio dei locali server;
  - allagamento dei locali server;
  - accesso non autorizzato nei locali e archivi fisici;
  - accesso fisico non autorizzato nei locali server;

- distruzione di strumentazione da parte di persone malintenzionate;
- attacchi (bombe, terroristi);
- uragani, trombe d'aria;
- terremoti, eruzioni vulcaniche;
- fulmini e scariche atmosferiche;
- guasto sistemi di raffreddamento locali server;
- intercettazione elettronica;
- furto di documenti o supporti di memorizzazione (HD, pc, cellulari);
- furto di credenziali di autenticazione;
- azione di virus informatici o codici malefici;
- malfunzionamento apparati di rete;
- malfunzionamento software applicativi;
- errori di manutenzione hardware;
- comportamenti sleali o fraudolenti;
- errore materiale;
- modifica deliberata e non autorizzata o involontaria dei dati di configurazione del sistema;
- degrado/obsolescenza della strumentazione (memorie di massa).

- **Fonti di rischio**
  - fonti umane interne;
  - fonti umane esterne;
  - fonti non umane.

- **Misure, tra quelle individuate, che contribuiscono a mitigare il rischio**
  - controllo degli accessi logici;
  - profili di autorizzazione;
  - sistemi antivirus – firewall;
  - backup;
  - cifratura dei dati;
  - pseudonimizzazione;
  - sicurezza dei supporti cartacei;
  - tracciabilità;
  - controllo degli accessi fisici;
  - adozione di policy e procedure interne;
  - formazione del personale;
  - esistenza di una procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative;
  - controllo degli accessi fisici ai locali dedicati alla ricerca scientifica;
  - conservazione, utilizzo e trasporto dei campioni biologici in modalità sicura;
  - trasferimento dei dati genetici in formato elettronico in modalità sicura.

GRAVITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA GRAVITA' EFFETTIVA ELIDENDO LE ALTRE)

La gravità effettiva dei rischi derivanti da accesso illegittimo ai dati è ritenuta, mediamente, "**basso**" (punteggio di __1__ in una scala di criterio di giudizio che si riassumono in un punteggio da 1 a 4), in quanto potrebbe determinare effetti lievi (p.e. fastidio), sulla vita sociale o personale degli interessati in termini di:
- furto d'identità;
- perdita sul controllo dei dati;
- impossibilità di esercizio dei diritti;
- danno reputazionale.

PROBABILITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA PROBABILITA'' EFFETTIVA ELIDENDO LE ALTRE)

La probabilità effettiva del rischio, anche alla luce delle misure di sicurezza esistenti o pianificate, è ritenuta, mediamente,
"**raro**" (punteggio di __1_, in una scala di criteri di giudizio che si riassumono in un punteggio da 1 a 4), in quanto il verificarsi del danno ipotizzato susciterebbe una grande sorpresa e incredulità. La gestione dell'attività, in termini di sicurezza, è ritenuta buona, salvo qualche lacuna.

INDICE DI RISCHIO: R X P = G = _____1___ (molto alto – alto – Medio – basso)

4. DISTRUZIONE DEI DATI

- **Principali possibili impatti**
  - danni fisici o psicologici;
  - perdita del controllo sui dati;
  - impossibilità di esercizio dei diritti;
  - danno reputazionale.

- **Principali minacce che potrebbero concretizzare il rischio**
  - incendio dei locali server;
  - allagamento dei locali server;
  - accesso non autorizzato nei locali e archivi fisici;
  - accesso fisico non autorizzato nei locali server;
  - distruzione di strumentazione da parte di persone malintenzionate;
  - attacchi (bombe, terroristi);
  - uragani, trombe d'aria;
  - terremoti, eruzioni vulcaniche;
  - fulmini e scariche atmosferiche;
  - guasto sistemi di raffreddamento locali server;
  - disturbi elettromagnetici;
  - intercettazione elettronica;
  - furto di documenti o supporti di memorizzazione (HD, pc, cellulari);
  - furto di credenziali di autenticazione;
  - azione di virus informatici o codici malefici;
  - malfunzionamento apparati di rete;
  - malfunzionamento software applicativi;
  - errori di manutenzione hardware;
  - comportamenti sleali o fraudolenti;
  - modifica deliberata e non autorizzata o involontaria dei dati di configurazione del sistema;
  - degrado/obsolescenza della strumentazione (memorie di massa).

- **Fonti di rischio**
  - fonti umane interne;
  - fonti umane esterne;
  - fonti non umane.

- **Misure, tra quelle individuate, che contribuiscono a mitigare il rischio**
  - controllo degli accessi logici;
  - profili di autorizzazione;
  - sistemi antivirus – firewall;
  - backup;

- cifratura dei dati;
- pseudonimizzazione;
- sicurezza dei supporti cartacei;
- tracciabilità;
- controllo degli accessi fisici;
- adozione di misure di sicurezza fisiche contro eventuali fonti di rischio non umane;
- adozione di policy e procedure interne;
- formazione del personale;
- esistenza di una procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative;
- controllo degli accessi fisici ai locali dedicati alla ricerca scientifica;
- conservazione, utilizzo e trasporto dei campioni biologici in modalità sicura;
- trasferimento dei dati genetici in formato elettronico in modalità sicura.

GRAVITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA GRAVITA' EFFETTIVA ELIDENDO LE ALTRE)

La gravità effettiva dei rischi derivanti da accesso illegittimo ai dati è ritenuta, mediamente,
"**basso**" (punteggio di __1__ in una scala di criterio di giudizio che si riassumono in un punteggio da 1 a 4), in quanto potrebbe determinare effetti lievi (p.e. fastidio), sulla vita sociale o personale degli interessati in termini di:
- furto d'identità;
- perdita sul controllo dei dati;
- impossibilità di esercizio dei diritti;
- danno reputazionale.

PROBABILITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA PROBABILITA'' EFFETTIVA ELIDENDO LE ALTRE)

La probabilità effettiva del rischio, anche alla luce delle misure di sicurezza esistenti o pianificate, è ritenuta, mediamente,
"**raro**" (punteggio di __1_, in una scala di criteri di giudizio che si riassumono in un punteggio da 1 a 4), in quanto il verificarsi del danno ipotizzato susciterebbe una grande sorpresa e incredulità. La gestione dell'attività, in termini di sicurezza, è ritenuta buona, salvo qualche lacuna.

INDICE DI RISCHIO: R X P = G = __1_____ (molto alto – alto – Medio – basso)

5. INDISPONIBILITÀ DEI DATI

- **Principali possibili impatti**
  - furto d'identità;
  - perdita del controllo sui dati;
  - impossibilità di esercizio dei diritti;
  - danno reputazionale.

- **Principali minacce che potrebbero concretizzare il rischio**
  - accesso non autorizzato nei locali e archivi fisici;
  - accesso fisico non autorizzato nei locali server;
  - perdita di energia;
  - malfunzionamento nei componenti di rete;
  - interruzione nei collegamenti di rete (inclusi danni alle linee TLC);

- disturbi elettromagnetici;
- intercettazione elettronica;
- furto di documenti o supporti di memorizzazione (HD, pc, cellulari);
- furto di credenziali di autenticazione;
- azione di virus informatici o codici malefici;
- malfunzionamento apparati di rete;
- malfunzionamento software applicativi;
- errori di manutenzione hardware;
- comportamenti sleali o fraudolenti;
- degrado/obsolescenza della strumentazione (memorie di massa).

- **Fonti di rischio**
  - fonti umane interne;
  - fonti umane esterne;
  - fonti non umane.

- **Misure, tra quelle individuate, che contribuiscono a mitigare il rischio**
  - controllo degli accessi logici;
  - profili di autorizzazione;
  - sistemi antivirus – firewall;
  - backup;
  - cifratura dei dati;
  - pseudonimizzazione;
  - sicurezza dei supporti cartacei;
  - tracciabilità;
  - controllo degli accessi fisici;
  - adozione di misure di sicurezza fisiche contro eventuali fonti di rischio non umane;
  - adozione di policy e procedure interne;
  - formazione del personale;
  - esistenza di una procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative;
  - controllo degli accessi fisici ai locali dedicati alla ricerca scientifica;
  - conservazione, utilizzo e trasporto dei campioni biologici in modalità sicura;
  - trasferimento dei dati genetici in formato elettronico in modalità sicura.

GRAVITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA GRAVITA' EFFETTIVA ELIDENDO LE ALTRE)

La gravità effettiva dei rischi derivanti da accesso illegittimo ai dati è ritenuta, mediamente, "**basso**" (punteggio di __1__ in una scala di criterio di giudizio che si riassumono in un punteggio da 1 a 4), in quanto potrebbe determinare effetti lievi (p.e. fastidio), sulla vita sociale o personale degli interessati in termini di:
- furto d'identità;
- perdita sul controllo dei dati;
- impossibilità di esercizio dei diritti;
- danno reputazionale.

PROBABILITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA PROBABILITA'' EFFETTIVA ELIDENDO LE ALTRE)

La probabilità effettiva del rischio, anche alla luce delle misure di sicurezza esistenti o pianificate, è ritenuta, mediamente,

"**raro**" (punteggio di _1_, in una scala di criteri di giudizio che si riassumono in un punteggio da 1 a 4), in quanto il verificarsi del danno ipotizzato susciterebbe una grande sorpresa e incredulità. La gestione dell'attività, in termini di sicurezza, è ritenuta buona, salvo qualche lacuna.

INDICE DI RISCHIO: R X P = G = ___1_____ (molto alto – alto – Medio – basso)

6. DIVULGAZIONE DEI DATI

- **Principali possibili impatti**
  - discriminazione;
  - furto d'identità;
  - perdita del controllo sui dati;
  - impossibilità di esercizio dei diritti;
  - danno reputazionale.

- **Principali minacce che potrebbero concretizzare il rischio**
  - accesso non autorizzato nei locali e archivi fisici;
  - accesso fisico non autorizzato nei locali server;
  - perdita di energia;
  - intercettazione elettronica;
  - furto di documenti o supporti di memorizzazione (HD, pc, cellulari);
  - furto di credenziali di autenticazione;
  - recupero di informazioni da apparati, componenti dismessi (pc, cellulari, elettromedicali, ecc.);
  - rivelazione di informazioni (da lavoratori o fornitori);
  - azione di virus informatici o codici malefici;
  - malfunzionamento apparati di rete;
  - malfunzionamento software applicativi;
  - errori di manutenzione hardware;
  - comportamenti sleali o fraudolenti;
  - modifica deliberata e non autorizzata o involontaria dei dati di configurazione del sistema;
  - utilizzo non conforme alle finalità della raccolta;
  - degrado/obsolescenza della strumentazione (memorie di massa).

- **Fonti di rischio**
  - fonti umane interne;
  - fonti umane esterne;
  - fonti non umane.

- **Misure, tra quelle individuate, che contribuiscono a mitigare il rischio**
  - controllo degli accessi logici;
  - profili di autorizzazione;
  - sistemi antivirus – firewall;
  - cifratura dei dati;
  - pseudonimizzazione;
  - sicurezza dei supporti cartacei;
  - tracciabilità;
  - controllo degli accessi fisici;
  - adozione di misure di sicurezza fisiche contro eventuali fonti di rischio non umane;
  - adozione di policy e procedure interne;
  - formazione del personale;
  - esistenza di una procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative;
  - controllo degli accessi fisici ai locali dedicati alla ricerca scientifica;

- conservazione, utilizzo e trasporto dei campioni biologici in modalità sicura;
- trasferimento dei dati genetici in formato elettronico in modalità sicura.

GRAVITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA GRAVITA' EFFETTIVA ELIDENDO LE ALTRE)

La gravità effettiva dei rischi derivanti da accesso illegittimo ai dati è ritenuta, mediamente,
"**basso**" (punteggio di __1__ in una scala di criterio di giudizio che si riassumono in un punteggio da 1 a 4), in quanto potrebbe determinare effetti lievi (p.e. fastidio), sulla vita sociale o personale degli interessati in termini di:
- furto d'identità;
- perdita sul controllo dei dati;
- impossibilità di esercizio dei diritti;
- danno reputazionale.

PROBABILITÀ DEL RISCHIO STIMATA

(MANTENERE SOLAMENTE LA PROBABILITA'' EFFETTIVA ELIDENDO LE ALTRE)

La probabilità effettiva del rischio, anche alla luce delle misure di sicurezza esistenti o pianificate, è ritenuta, mediamente,
"**raro**" (punteggio di _1__, in una scala di criteri di giudizio che si riassumono in un punteggio da 1 a 4), in quanto il verificarsi del danno ipotizzato susciterebbe una grande sorpresa e incredulità. La gestione dell'attività, in termini di sicurezza, è ritenuta buona, salvo qualche lacuna.

INDICE DI RISCHIO: R X P = G = ____1____ (molto alto – alto – Medio – basso)

G. AZIONI CORRETTIVE

Azioni di Miglioramento Azioni Correttive	
Rischi	**Azioni di mitigazione del Rischio Molto altro - alto**
Accesso non autorizzato	
Modifica	
Perdita	
Distruzione	
indisponibilità	
Divulgazione	

Le Azioni correttive e di miglioramento intraprese devono essere registrate tramite la scheda "MGF65 Scheda registrazione AC-AdM".

H. PARERE DEL RPD

In data 17 luglio 2025, il Responsabile della Protezione dei Dati di Fondazione Don Carlo Gnocchi – onlus, anche in ossequio al disposto dell'art. 39, Regolamento UE 2016/679, esprime parere positivo in merito alla conformità del trattamento analizzato in relazione ai risultati della DPIA effettuata.

Il trattamento di dati oggetto di analisi è connesso alla conduzione di un progetto di ricerca scientifica inerente al trattamento in emergenza nei pazienti con shock cardiogeno e anche alle condizioni di follow-up, in particolare alla valutazione di qualità di vita e alle esperienze avute in ambito sanitario.

Si rileva che, nell'ambito della Valutazione di Impatto, tutte le misure esistenti o pianificate per garantire un'adeguata protezione dei dati hanno ricevuto valutazione positiva.

Non di meno, le soluzioni adottate per il rispetto dei principi fondamentali posti alla base della protezione dei dati e per far fronte ai rischi per le libertà e i diritti degli interessati, sono state considerate idonee al fine di poter valutare come "bassi" (valore 1, in una scala da 1 a 4) tutti i rischi connessi al trattamento dei dati (accesso illegittimo ai dati, modifiche indesiderate dei dati, perdita dei dati, distruzione dei dati, indisponibilità dei dati, e divulgazione dei dati).

Le pregresse considerazioni consentono, come anticipato, di esprimere un parere favorevole in ordine alla conformità del trattamento analizzato.

I. OPINIONE DEGLI INTERESSATI

L. CONSULTAZIONE PREVENTIVA

M. CONSIDERAZIONE SULLE VALUTAZIONI CONDOTTE

I. CONSULTAZIONE PREVENTIVA

L. CONSIDERAZIONE SULLE VALUTAZIONI CONDOTTE

Fondazione Don Carlo Gnocchi
Firma del titolare del trattamento
(Direttore Generale – Dr. Francesco Converti)

FRANCESCO CONVERTI
09.03.2026 15:57:30
GMT+01:00