



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Valutazione d'impatto sulla protezione dei dati

Valutazione d'impatto trasversale su studi osservazionali retrospettivi con promotore IOV

29/03/2023



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)
C.F. - P.IVA 04074560287 04074560287

T. 0498215849
F.
W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)
DIRETTORE@IOV.VENETO.IT

Indice

Sommario

Valutazione d'impatto sulla protezione dei dati	1
Validazione.....	5
DPO e parere degli interessati	5
Nome del DPO/RPD	5
Posizione del DPO/RPD	5
Parere del DPO/RPD	5
Richiesta del parere degli interessati	5
Motivazione della mancata richiesta del parere degli interessati	5
Contesto.....	6
Panoramica del trattamento	6
Quale è il trattamento in considerazione?	6
Quali sono le responsabilità connesse al trattamento?	6
Ci sono standard applicabili al trattamento?	7
Contesto.....	7
Dati, processi e risorse di supporto.....	7
Quali sono i dati trattati?	7
Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?	7
Quali sono le risorse di supporto ai dati?	8
Principi Fondamentali	8
Proporzionalità e necessità.....	8
Gli scopi del trattamento sono specifici, espliciti e legittimi?	8
Quali sono le basi legali che rendono lecito il trattamento?	8
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	9
I dati sono esatti e aggiornati?	9
Qual è il periodo di conservazione dei dati?	10
Principi Fondamentali	10
Misure a tutela dei diritti degli interessati.....	10
Come sono informati del trattamento gli interessati?	10
Ove applicabile: come si ottiene il consenso degli interessati?	10



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?	11
Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	11
Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	12
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	12
In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	12
Rischi	13
Misure esistenti o pianificate	13
Anonimizzazione	13
Controllo degli accessi logici	13
Sicurezza dei documenti cartacei	14
Minimizzazione dei dati	14
Gestione postazioni	14
Sicurezza dei siti web	15
Backup	15
Sicurezza dei canali informatici	15
Controllo degli accessi fisici	16
Gestione delle politiche di tutela della privacy	16
Gestione del personale	16
Crittografia	17
Lotta contro il malware	17
Politica di tutela della privacy	17
Accesso illegittimo ai dati	17
Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	17
Quali sono le principali minacce che potrebbero concretizzare il rischio?	18
Quali sono le fonti di rischio?	18
Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	18
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	18
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	18
Modifiche indesiderate dei dati	19
Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?	19
Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	19
Quali sono le fonti di rischio?	19
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	19
Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?	19



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?	
.....	20
Perdita di dati	20
Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	20
Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	20
Quali sono le fonti di rischio?	20
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	20
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	20
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	21



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Validazione

DPO e parere degli interessati

Nome del DPO/RPD

Cristina Canella

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

La stima della probabilità del rischio porta a ritenere che lo stesso, alla luce delle misure tecniche e organizzative attualmente in atto, tenuto conto della natura del trattamento, possa essere implementato.

Al fine di diminuire ulteriormente la probabilità di accadimento del rischio è opportuno tuttavia che vi sia:

- una continua revisione delle policy aziendali per l'utilizzo del sistema informatico aziendale;
- una valutazione e verifica periodica sulla sicurezza dei sistemi aziendali;
- un'adeguata formazione del personale sull'utilizzo degli strumenti aziendali (hardware e software);
- un adeguamento dei protocolli adottati per ciascun progetto di ricerca che tenga conto dei principi di minimizzazione, privacy by default e privacy by design.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Il parere degli interessati non è necessario ai sensi dell'art. 110 co 1 prima parte del Codice Privacy, così come meglio specificato dal parere reso dall'Ufficio Privacy e da questo RPD sulla base giuridica degli studi osservazionali retrospettivi in cui sia promotore IOV.



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)
C.F. - P.IVA 04074560287 04074560287

T. 0498215849
F.
W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)
DIRETTORE@IOV.VENETO.IT

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

L'Istituto Oncologico Veneto è stato istituito con L.R. 22 dicembre 2005 n.26 ed è stato riconosciuto Istituto di Ricovero e Cura a Carattere ai sensi del d.lgs.288/2003, con DM 06.06.2017. Pertanto, l'Istituto svolge, nella disciplina dell' oncologia, attività di prevalente ricerca biomedica e sanitaria e di assistenza sanitaria di tipo clinico e traslazionale.

Pertanto, centrale per l'Istituto è l'attività di ricerca scientifica, perseguito nell'ambito dell'oncologia secondo standard di eccellenza.

In linea con la normativa regionale nazionale, IOV svolge attività di studio e di ricerca, trasferendo i dati validati nei processi assistenziali del Sistema Sanitario Regionale.

La presente valutazione riguarda specifici progetti di ricerca, ovvero **studi osservazionali retrospettivi, con promotore IRCCS IOV**, che rientrano anche nell'ambito dei programmi di ricerca biomedica o sanitaria previsti ai sensi dell'articolo 12-bis del Dlgs 30 dicembre 1992 n. 502).

Per tali progetti, IRCCS propone al Ministero della Salute un piano di studi triennale, strutturato in linee di ricerca, e ciascuna di queste declinata in una serie di progetti che poi vengono sviluppati durante il triennio (c.d. *ricerca corrente*).

La norma citata riguarda sia la *ricerca finalizzata*, che il Ministero promuove e finanzia di propria iniziativa.

La presente valutazione considera i trattamenti svolti da IOV sia nell'ambito di studi monocentrici sia in quello di studi multicentrici di cui sia promotore.

Quali sono le responsabilità connesse al trattamento?

La titolarità del trattamento è in capo all'IRCCS - Istituto Oncologico Veneto, che in questo contesto opera come promotore sui progetti di ricerca.



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849
F.
W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)
DIRETTORE@IOV.VENETO.IT

Per questa tipologia di studi non sono previsti soggetti terzi coinvolti.

Ci sono standard applicabili al trattamento?

Attualmente non ci sono standard applicabili al trattamento in oggetto.

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati oggetto di trattamento sono già presenti in cartella clinica, raccolti per finalità di cura (ovvero in riferimento ad un percorso di cura che il paziente ha avuto con lo IOV).

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Per ogni singolo progetto di ricerca, i dati oggetto di ricerca sono quelli che sono presenti nella cartella clinica del paziente arruolato nel progetto di ricerca specifico.

I dati sono poi catalogati in modo da ottenere un risultato utile alla pubblicazione. Normalmente potrebbero poi essere mantenuti per un tempo congruo pari a 3 anni dalla chiusura dello studio (in caso di necessità di revisione degli stessi).

Per quanto riguarda i progetti finalizzati, il Ministero prevede poi l'obbligo di depositare i c.d. *raw data* che consentano anche l'accesso ai dati di ricerca da parte di altre strutture / ricercatori.



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Quali sono le risorse di supporto ai dati?

- Sistema RedCap;
- Files di office automation ad uso dei singoli ricercatori, sia conservati su singole postazioni client che su aree di *share* aziendali;
- Aree condivise messe a disposizione dall'azienda, con condivisione tra i ricercatori coinvolti nel singolo progetto;
- Specifiche piattaforme di pubblicazione dei *raw data*.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati sono trattati per finalità di ricerca scientifica.

L'Istituto Oncologico Veneto, avendo qualifica di IRCCS, persegue legittimamente finalità di ricerca scientifica in ambito oncologico, stante il D.M. 6.6.2017 e la legge regionale 26/2005 di istituzione dell'Istituto.

Le finalità sono rese esplicite perché dichiarate nelle informative e nei documenti predisposti per la ricerca scientifica (informativa, consenso informato e consenso al trattamento dei dati).

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Dati di natura comune: art. 6 par. I lettera e)

Dati particolari: art. 9 par. II lettera j), in combinato disposto con l'art. 89 GDPR e art. 110 comma 1 prima parte D.Lgs. 196/2003.



ISTITUTO ONCOLOGICO VENETO - IRCCS

VIA GATTAMELATA, 64

PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Si veda anche lo specifico documento redatto dal Titolare per la definizione delle basi giuridiche applicabili agli studi oggetto di questa valutazione.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti seguono un protocollo di ricerca che ne definisce gli obiettivi e il disegno, conseguentemente definisce i limiti e gli ambiti di trattamento dei dati.

Secondo quanto previsto nello studio specifico, i dati di partenza (dati clinici) vengono analizzati nella loro interezza, raccogliendo e catalogando poi solamente le informazioni che sono già state oggetto di valutazione del comitato etico.

Ne consegue che, anche avendo accesso ad un set di dati ampio, il soggetto che è autorizzato ad analizzare i dati di partenza andrà a raccogliere e trattare solamente dati già preventivamente concordati.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Da valutare la metodologia della ricerca: per loro natura, tali progetti danno un contributo molto limitato all'ambito della ricerca; pertanto, nei protocolli non è prevista una fase di verifica sulla correttezza dei dati che poi vengono analizzati.

Una ulteriore revisione dei dati di partenza, viene invece effettuata a fronte di successivi progetti di ricerca, pertanto la revisione del dato di partenza (dato clinico) ha effetti solamente su nuovi studi e non anche su quelli già conclusi.

Valutazione : Accettabile



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Qual è il periodo di conservazione dei dati?

Il tempo di conservazione dei dati contenuti nella cartella clinica, ovvero i dati di partenza, è illimitato.

I dati personali e relativi alla salute trattati per progetti di ricerca osservazionali sono conservati:

fino alla definizione della pubblicazione degli esiti della ricerca, ovvero secondo la definizione delle tempistiche valutate durante la stesura del progetto.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Nelle informative affisse nei principali luoghi di transito e disponibile nel sito web istituzionale, è esplicito il riferimento all'attività di ricerca scientifica svolta dall'Istituto.

Per questi specifici studi osservazionali, non è previsto il rilascio dell'informativa direttamente ai soggetti coinvolti nel progetto di ricerca, ma una specifica informativa è pubblicata - unitamente alla presente valutazione d'impatto - nella sezione privacy del sito istituzionale.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Si ritiene il consenso non necessario in quanto il titolare è un I.R.C.C.S. che effettua gli studi analizzati con la presente valutazione nell'ambito dei programmi "*...di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502..*" provvedendo inoltre a condurre e rendere pubblica la presente valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.

Si veda anche lo specifico documento redatto dal Titolare in riferimento alla non applicabilità del consenso.



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849
F.
W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)
DIRETTORE@IOV.VENETO.IT

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono esercitare il diritto di accesso:

- scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy dell'Istituto, reperibile sia nell'informativa generale che nel sito web istituzionale;
- direttamente presso il P.I. e la sua equipe (ciò avviene più frequentemente rispetto all'utilizzo della posta elettronica).

Il diritto alla portabilità non è applicabile per tale attività di trattamento.

L'istituto ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono esercitare il diritto di rettifica e di cancellazione - limitatamente a quanto applicabile:

- scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy dell'Istituto, reperibile sia nell'informativa generale che nel sito web istituzionale;
- manifestando la propria volontà direttamente al P.I. e alla sua equipe.

L'istituto ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione : Accettabile



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono esercitare il diritto di opposizione e limitazione:

- scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy dell'Istituto, reperibile sia nell'informativa generale che nel sito web istituzionale;
- manifestando la propria volontà direttamente al P.I. e alla sua equipe.

L'istituto ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Per questa tipologia di trattamenti, non sono previsti responsabili esterni del trattamento.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Di regola non è previsto - per gli studi in analisi - il trasferimento verso Paesi Extra UE.

Valutazione : Accettabile



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Rischi

Misure esistenti o pianificate

Anonimizzazione

- Relativamente ai dati che devono essere pubblicati su specifiche piattaforme, secondo le indicazioni del Ministero, vengono elaborati con specifici prodotti che consentano l'anonimizzazione dei *raw data*.

Allo studio ci sono alcuni prodotti open source (ARX e AMNESIA) e si stanno valutando altri prodotti (con licenza a pagamento);

- **Valutazione : Accettabile**

Controllo degli accessi logici

- Gli accessi in dominio sono concessi dal servizio di ICT, a seguito di richiesta scritta e firmata da parte del Direttore di Unità Operativa (ovvero direttamente dall'ufficio risorse umane per il personale contrattualizzato) presentata direttamente dal singolo interessato. Le richieste includono:
 - generalità del richiedente
 - natura del rapporto con l'Istituto Oncologico Veneto (dipendente o altro)
 - date di inizio/fine del rapporto con l'Istituto Oncologico Veneto
 - Il servizio abilitazioni vaglia ogni singola abilitazione, scartando quelle incoerenti o inappropriate.
 - L'accesso alle aree di share è consentito secondo le policy aziendali, in relazione all'U.O. di appartenenza.

L'accesso alle aree condivise viene autorizzato dal P.I. che coordina il singolo progetto di ricerca.

- **Valutazione : Accettabile**



ISTITUTO ONCOLOGICO VENETO - IRCCS

VIA GATTAMELATA, 64

PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Sicurezza dei documenti cartacei

- È onere di ogni singolo soggetto coinvolto nello specifico progetto di ricerca, condividere la poca documentazione prodotta con i soli appartenenti all'equipe di ricerca.

Normalmente la documentazione cartacea riguarda i dati del progetto e pochi limitati dati personali, essendo questi trattati principalmente in modalità informatizzata.

Gli uffici dispongono di armadi con chiusura a chiave, accessibili solo dal personale autorizzato.

- **Valutazione : Accettabile**

Minimizzazione dei dati

- Il protocollo condiviso e autorizzato con il Comitato Etico stabilisce sia il set di informazioni cui si può accedere, sia o il dataset di informazioni che devono essere poi successivamente raccolte, catalogate e valutate, oltre anche all'arco temporale di analisi.

L'accesso ai dati clinici è consentito solamente al personale medico, mentre al restante personale (ricercatori), è consentito il trattamento dei soli dati necessari all'attività di ricerca prevista dal singolo progetto.

- **Valutazione : Accettabile**

Gestione postazioni

- Le postazioni utilizzate sono principalmente in dominio aziendale e le misure adottate sono quelle previste da regolamenti e policy aziendali.
- I dispositivi esterni e personali non possono ottenere l'accesso all'intranet aziendale.

- **Valutazione : Accettabile**



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849
F.
W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)
DIRETTORE@IOV.VENETO.IT

Sicurezza dei siti web

- La pubblicazione dei raw data - unici dati ad essere resi disponibili su diversi portali web, secondo quanto previsto dal Ministero della Salute e da questo più volte ribadito anche con specifiche circolari e comunicazioni -, avviene secondo quanto previsto dalla procedura interna che descrive le modalità di raccolta, deposito e condivisione dei dati della ricerca

- **Valutazione : Accettabile**

Backup

- Secondo policy aziendali, i documenti che vengono memorizzati su specifiche aree di *share* aziendali sono oggetto di backup. Stessa politica viene adottata per i dati memorizzati su procedure aziendali.

Per il dettaglio, si rimanda a quanto documentato e disponibile su intranet aziendale.

- **Valutazione : Accettabile**

Sicurezza dei canali informatici

- L'intranet è protetta da sistemi di firewall aziendale in gestione ad AOPD: gli unici dispositivi autorizzati a poter aprire canali di comunicazione nell'intranet aziendale sono quelli preventivamente registrati e autorizzati (solamente dispositivi aziendali).

Qualora sia richiesta l'abilitazione per un dispositivo personale, questa viene attentamente vagliata, e prima di procedere alla connessione viene adeguato secondo lo standard di policy aziendale (es. antivirus aziendale)

- **Valutazione : Accettabile**



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Controllo degli accessi fisici

- L'accesso ai locali è bloccato da serrature con codice: il codice di accesso è rilasciato al solo personale che abbia necessità ad accedere a tali locali (anche se condivisi con altri professionisti), oltre al personale del servizio di pulizia.
- **Valutazione : Accettabile**

Gestione delle politiche di tutela della privacy

- Il Titolare ha adottato uno specifico "Regolamento concernente la protezione dei dati personali", periodicamente revisionato, disponibile su sito web aziendale e condiviso con tutto il personale.
- **Valutazione : Accettabile**

Gestione del personale

- Il personale viene adeguatamente formato in merito alle attività di trattamento e ai sistemi di sicurezza da adottare.
Per tale scopo:
 - sono redatti specifici regolamenti interni
 - vengono effettuate sessioni formative
 - vengono effettuati audit presso le strutture interessate
- **Valutazione : Accettabile**



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Crittografia

- Il sistema RedCap prevede la crittografia dei dati, che sono conservati su storage S3 crittografato sulla piattaforma Amazon AWS, Cluster di Milano.
- **Valutazione : Accettabile**

Lotta contro il malware

- Tutte le postazioni e i dispositivi aziendali sono equipaggiati con antivirus e antimalware aziendale in gestione ad AOPD; il servizio ICT sta attualmente valutando l'adozione di un nuovo sistema di protezione, migliorativo rispetto all'attuale.
- **Valutazione : Accettabile**

Politica di tutela della privacy

- Il titolare ha nominato un RPD. Il Titolare - da atto aziendale - ha individuato uno specifico servizio (ufficio privacy) incardinato nell'U.O. Affari Generali.
- **Valutazione : Accettabile**

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita di riservatezza, Perdita di integrità dei dati oggetti di studio, Perdita di disponibilità dei dati oggetto di studio



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F.- P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Comportamento improprio del personale interno, Utilizzo improprio di dispositivi non aziendali

Quali sono le fonti di rischio?

Perdita di dispositivi affidati a personale interno, Accesso a sistemi aziendali da soggetti terzi non autorizzati, Attacco ai sistemi aziendali

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Sicurezza dei canali informatici, Gestione delle politiche di tutela della privacy, Anonimizzazione, Gestione del personale, Gestione postazioni, Controllo degli accessi logici, Sicurezza dei documenti cartacei, Controllo degli accessi fisici, Crittografia, Sicurezza dei siti web

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, L'accesso indesiderato ai dati di ricerca (non i dati clinici dai quali si parte), determina la perdita di riservatezza su dati sanitari - rilevati ai fini dello studio - relativi ai pazienti coinvolti nello studio. La gravità è attenuata, dal momento che la catalogazione avviene con dati parzialmente aggregati o pseudonimizzati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Alla luce dei sistemi e procedure in essere, la probabilità di accadimento di un accesso illegittimo può essere ritenuto limitato perché:

- Dati e documenti sono conservati e gestiti solamente su sistemi aziendali;
- i dispositivi che accedono all'intranet aziendale sono forniti o controllati direttamente dall'U.O. Sistemi Informativi, che ha la possibilità di bloccare i dispositivi in remoto nel caso di furto o smarrimento.

Tuttavia, al fine di diminuire ulteriormente la probabilità di accadimento del rischio è opportuno che vi sia:

- una continua revisione delle policy aziendali per l'utilizzo del sistema informatico aziendale;
- una valutazione e verifica periodica sulla sicurezza dei sistemi aziendali;
- una adeguata formazione al personale sull'utilizzo degli strumenti aziendali (hardware e software);



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)
C.F. - P.IVA 04074560287 04074560287

T. 0498215849
F.
W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)
DIRETTORE@IOV.VENETO.IT

- un adeguamento dei protocolli adottati per ciascun progetto di ricerca, che tenga conto dei principi di minimizzazione, *privacy by default* e *privacy by design*.

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita di integrità dei dati oggetti di studio

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Comportamento improprio del personale interno, Impostazioni errate su dispositivi e sistemi aziendali

Quali sono le fonti di rischio?

Accesso a sistemi aziendali da soggetti terzi non autorizzati, Attacco ai sistemi aziendali

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Gestione postazioni, Controllo degli accessi fisici, Gestione delle politiche di tutela della privacy, Gestione del personale

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, la gravità del rischio, nel caso di modifica indesiderata dei dati oggetto di studio (non i dati clinici dai quali si parte), ai fini dei diritti e le libertà delle persone fisiche può essere considerato trascurabile.

Il rischio in analisi (perdita di integrità) eventualmente impatta sulla pubblicazione della ricerca e non tanto sui dati personali oggetto di trattamento.



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata alla luce dei sistemi e procedure in essere, la modifica impropria dei dati estratti dalla cartella clinica può ritenersi limitato in quanto l'accesso ai dati contenuti nell'intranet aziendale è limitato, regolamentato e profilato.

In ogni caso la modifica illegittima potrebbe riguardare soltanto i singoli dati estratti dalla cartella in quanto la cartella clinica è conservata in database crittografati e protetti da misure di sicurezza gestiti a livello centralizzato.

Valutazione : Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita di disponibilità dei dati oggetto di studio

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Comportamento improprio del personale interno, Utilizzo improprio di dispositivi non aziendali

Quali sono le fonti di rischio?

Attacco ai sistemi aziendali, perdita di dispositivi affidati a personale interno

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Gestione postazioni, Gestione del personale, Sicurezza dei siti web

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, La gravità del rischio, nel caso di perdita dei dati oggetto di studio (non i dati clinici dai quali si parte), ai fini dei diritti e le libertà delle persone fisiche può essere considerato trascurabile.



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Il rischio in analisi (perdita del dato) eventualmente impatta sulla pubblicazione della ricerca e non tanto sui dati personali oggetto di trattamento; in ogni caso l'attività può essere ripresa, partendo dai dati clinici iniziali.

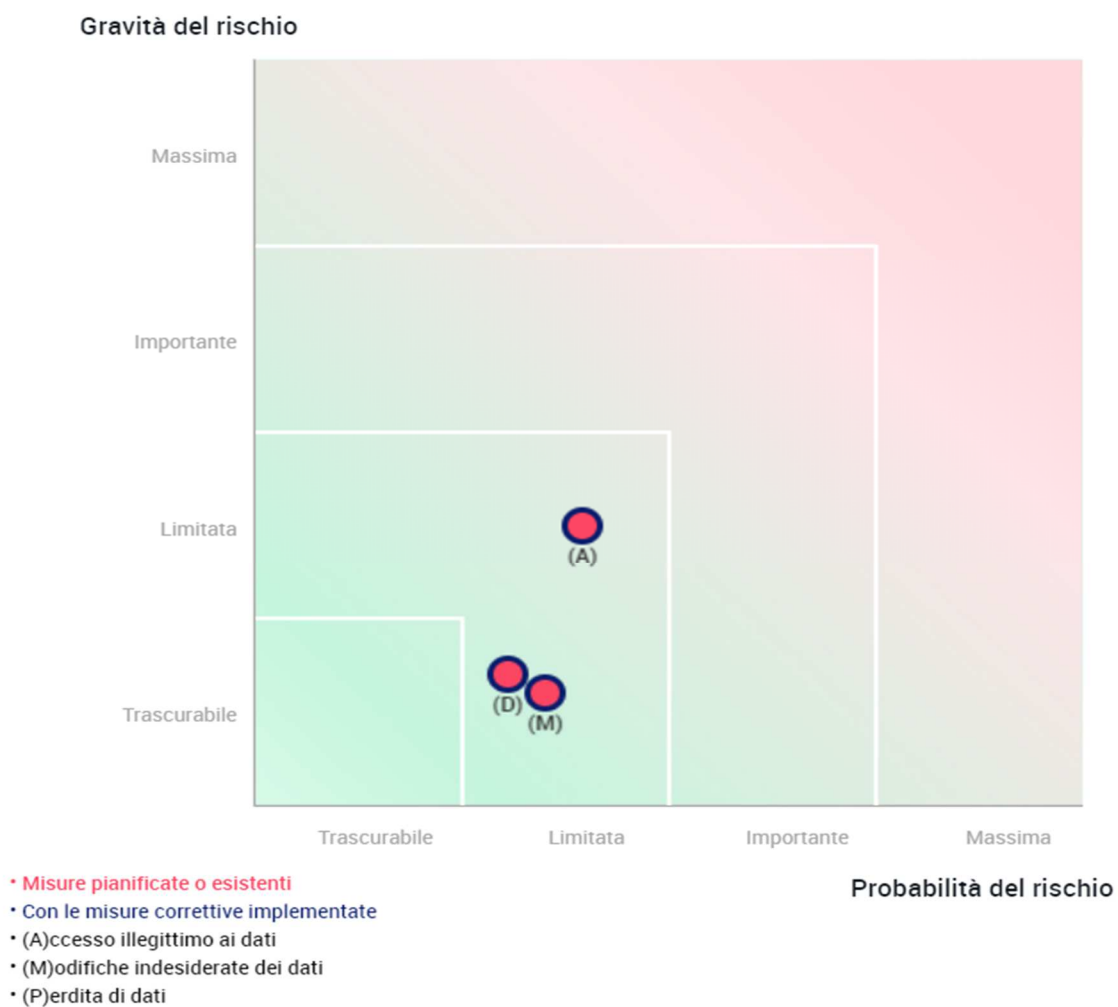
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata alla luce dei sistemi e procedure in essere, la perdita dei dati estratti dalla cartella clinica può ritenersi limitato in quanto l'accesso ai dati contenuti nell'intranet aziendale è limitato, regolamentato e profilato, sono presenti procedure e strumenti di backup adeguati.

In ogni caso la perdita potrebbe riguardare soltanto i singoli dati estratti dalla cartella in quanto la cartella clinica è conservata in database crittografati e protetti da misure di sicurezza gestiti a livello centralizzato.

Valutazione : Accettabile

Panoramica del rischio



13/03/23

Impatti potenziali

Perdita di riservatezza
Perdita di integrità dei da...
Perdita di disponibilità de...

Minaccia

Comportamento improprio
Utilizzo improprio di dispo
Impostazioni errate su disp

Fonti

Perdita di dispositivi affi...
Accesso a sistemi aziendali
Attacco ai sistemi aziendali

Misure

Sicurezza dei canali inform
Gestione delle politiche di.
Anonimizzazione
Gestione del personale
Gestione postazioni
Controllo degli accessi log.
Sicurezza dei documenti ca
Controllo degli accessi fis..
Crittografia
Sicurezza dei siti web

Accesso illegittimo ai dati

Gravità : Limitata

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Trascurabile

Probabilità : Limitata

Perdita di dati

Gravità : Trascurabile

Probabilità : Limitata

Panoramica

Principi fondamentali

Finalità		
Basi legali		
Adeguatezza dei dati		
Esattezza dei dati		
Periodo di conservazione		
Informativa		
Raccolta del consenso		
Diritto di accesso e diritto alla portabilità dei dati		
Diritto di rettifica e diritto di cancellazione		
Diritto di limitazione e diritto di opposizione		
Responsabili del trattamento		
Trasferimenti di dati		

Misure esistenti o pianificate

		Anonimizzazione
		Controllo degli accessi logici
		Sicurezza dei documenti cartacei
		Minimizzazione dei dati
		Gestione postazioni
		Sicurezza dei siti web
		Backup
		Sicurezza dei canali informatici
		Controllo degli accessi fisici
		Gestione delle politiche di tutela della privacy
		Gestione del personale
		Crittografia
		Lotta contro il malware
		Politica di tutela della privacy

Rischi

		Accesso illegittimo ai dati
		Modifiche indesiderate dei dati
		Perdita di dati

Misure Migliorabili
Misure Accettabili



ISTITUTO ONCOLOGICO VENETO - IRCCS
VIA GATTAMELATA, 64
PADOVA (PD)

C.F. - P.IVA 04074560287 04074560287

T. 0498215849

F.

W. [HTTPS://WWW.IOVENETO.IT/](https://www.ioveneto.it/)

DIRETTORE@IOV.VENETO.IT

Edizione:

ICRRS Istituto Oncologico Veneto / UNIS&F

Valutazione :

ICRRS Istituto Oncologico Veneto

Validazione :

IRCCS Istituto Oncologico Veneto

Stato :

Validata

100%