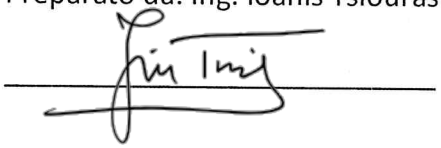
Risk Assessment
e
Data Protection Impact Assessment (DPIA)
Sistema: Bionano Saphyr

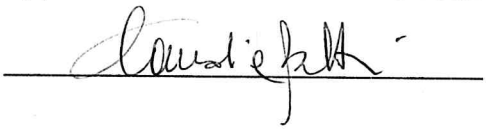
Fornitore del sistema: Bionano Genomics Inc

Preparato da: Ing. Ioanis Tsiouras



Verificato da: Dott.ssa Aurora Lucchi

Approvato da: Dott.ssa Claudia Balbi



Applicazione SW utilizzata per Risk Assessment e DPIA: CNIL v. 3.0.3

INDICE

1. Contesto - Panoramica

1.1 Trattamento dei dati presi in considerazione

Voden Medical Instruments S.p.A. fornisce e gestisce il sistema BIONANO GENOMICS presso **Ospedale Pediatrico Bambino Gesù (OPBG).**
Titolare del trattamento: Ospedale Pediatrico Bambino Gesù (OPBG).
Responsabile trattamento: Voden Medical Instruments S.p.A.
Sub-Responsabile: Bionano Genomics Inc
Doc. di riferimento di Bionano Genomics Inc: CG-30292-Data-Security-Guidelines Rev. E del 23/01/2024.

1.2 Responsabilità connesse al trattamento

Responsabile del trattamento ai sensi dell'articolo 28 (C81) del Regolamento UE 2016/679 la **Voden Medical Instruments S.p.A. (Responsabile)**, in persona del legale rappresentante pro-tempore Dott. Daniele Cesana con sede legale in Casorezzo (MI), Via Roma 2/a, codice fiscale/Partita IVA 03784450961.
Sub-Responsabile: Bionano Genomics Inc.
Il Responsabile e il Sub-responsabile del trattamento garantiscono la corretta applicazione delle misure di sicurezza adeguata che si dovesse rendere necessaria ex artt. 25 e 32 RGPD, tale da soddisfare, nella loro totalità, i requisiti posti dal Regolamento, dal D. Lgs. 196/2003 e dai provvedimenti del Garante per la Protezione dei dati Personali ("GPDP") (art. 28.1).

1.3 Standard applicabili al trattamento

Non esistono norme applicabili per il trattamento.

2. Contesto - Dati, processi e risorse di supporto

2.1 Dati trattati

Categorie di interessati: I Dati Personali riguardano: dipendenti, collaboratori e comunque ogni persona che opera in nome e per conto di ciascuna Parte.

Tipo di Dati Personali oggetto di trattamento: I dati oggetto di trattamento appartengono: alla categoria di dati comuni: dati identificativi, anagrafici e di contatto.

Natura e finalità del trattamento: Il trattamento dei dati personali viene effettuato per conto del Titolare del trattamento e in ragione dell'esecuzione delle finalità perseguite dallo stesso ossia: garantire la fornitura di n. 1 strumento Sistema Saphyr Optical Genome Mapping (OGM), giusto Contratto stipulato tra le Parti.

Il trattamento dei dati per le suddette finalità ha natura: Facoltativa, tuttavia necessaria per le finalità perseguite.

Durata del trattamento: Il trattamento sarà effettuato per tutta la durata del Contratto tra le Parti.

Modalità di Trattamento: In relazione alle indicate finalità, il trattamento dei dati personali avviene mediante: strumenti manuali e informatici.

I dati di identificazione personale sono informazioni non sanitarie che possono essere ricondotte a un individuo. Quando i dati personali vengono legati alle informazioni sanitarie, diventano informazioni sanitarie protette, come definito dall'HIPPA. Bionano non richiede, trasmette o memorizza informazioni sanitarie protette. Nello specifico, Bionano archivia e trasmette solo dati genomici deidentificati. Di seguito abbiamo identificato i tipi di dati in Bionano Compute On Demand e Saphyr Assure che rientrano in queste categorie. Bionano fornisce funzionalità di sicurezza per proteggere tutti i seguenti dati.

Raccolta dati: Saphyr Assure è progettato per raccogliere solo informazioni relative alle prestazioni dello strumento e del chip utili per determinare lo stato attuale dello strumento e prevedere le future esigenze di manutenzione. Il servizio è stato attentamente progettato per garantire che non vengano raccolte informazioni personali protette. Le informazioni dettagliate di seguito vengono raccolte anche quando viene generata una richiesta diagnostica avviata dall'utente.

2.2 Trattamento dei dati (descrizione funzionale)

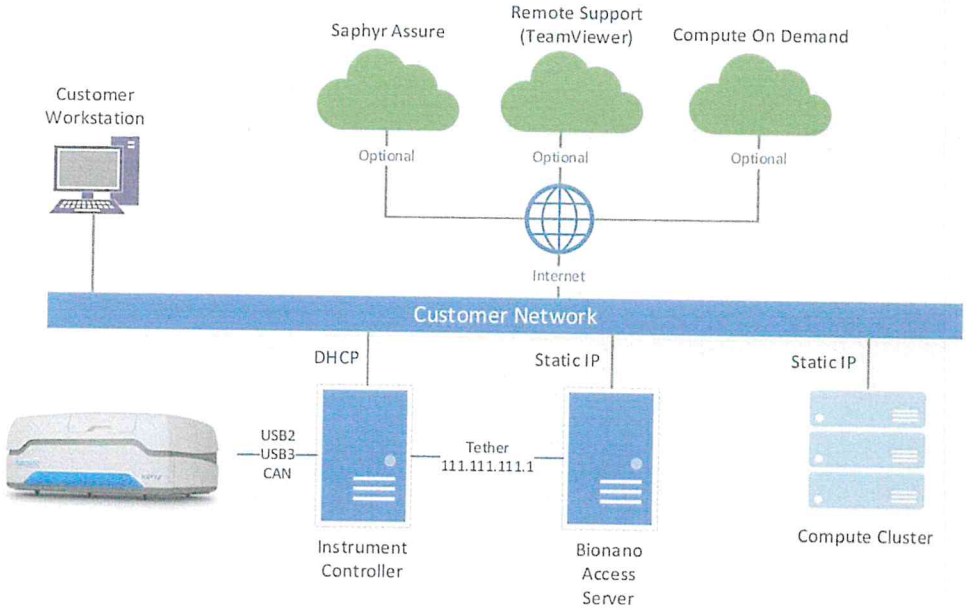
I dati che vengono raccolti dai servizi Bionano Compute On Demand e da Saphyr Assure sono quelli riportati nella seguente tabella.

Table 1. Information Categories

Service	Category	Data	Description
Bionano Compute On Demand	Personal	User Account	User account information, including email addresses, is used to track token and job ownership. Contact information is used to convey job and system status messages.
Bionano Compute On Demand	Personal	Jobs Metrics	General metrics regarding jobs such as the user, organization, job status, operation type, run time, and cost are tracked. This information is necessary to provide an accurate accounting of tokens spent, system health, and troubleshooting.
Saphyr Assure	Performance	Chip Metrics	General information about chip usage (i.e., throughput, data quality) is tracked to continuously improve instrument, chip performance, and provide enhanced support.
Saphyr Assure	Performance	System Alerts	Error conditions and alerts are tracked to monitor the health of the environment and to provide enhanced support.
Bionano Compute On Demand	Other	Genomic Data	De-identified genomic data is stored temporarily on the Bionano Compute On Demand service during the analysis. After the operation has been completed and downloaded the input files are deleted. All data transfers are encrypted.

2.3 Risorse di supporto al trattamento dei dati

Nello schema che segue è illustrato lo schema della rete e le risorse HW utilizzate al trattamento dei dati.



3. Principi Fondamentali - Proporzionalità e necessità

3.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali viene effettuato per conto del Titolare del trattamento e in ragione dell'esecuzione delle finalità perseguite dallo stesso ossia: garantire la fornitura di n. 1 strumento Sistema Saphyr Optical Genome Mapping (OGM), giusto Contratto stipulato tra le Parti.

Il trattamento dei dati per le suddette finalità ha natura: Facoltativa, tuttavia necessaria per le finalità perseguite.

Valutazione: Accettabile

3.2 Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento è lecito per l'esecuzione del contratto con l'**Ospedale Pediatrico Bambino Gesù** di cui gli interessati sono i pazienti che richiedono le prestazioni all'Ospedale.
Valutazione: Accettabile

3.3 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 che vengono raccolti appartengono alla categoria di dati comuni: dati identificativi, anagrafici e di contatto stabiliti dal contratto.

Valutazione: Accettabile

3.4 I dati sono esatti e aggiornati?

I dati sono relativi agli account degli user e delle metriche di misurazione delle prestazioni del sistema.
Valutazione: Accettabile

3.5 Qual è il periodo di conservazione dei dati?

Il trattamento sarà effettuato per tutta la durata del Contratto tra le Parti. Questa durata non è specificata in quanto il contratto è di validità annuale e rinnovato automaticamente per l'anno successivo.
Valutazione: Accettabile.

4. Principi Fondamentali - Misure a tutela dei diritti degli interessati

4.1 Come sono informati del trattamento gli interessati?

Gli interessati sono gli user del sistema e si identificano nel System Administrator dell'Ospedale e gli altri utenti come gli operatori del laboratorio che utilizzano il Bionanao Gemìnomics.
Valutazione: Accettabile

4.2 Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso degli interessati è a carico dell'Ospedale.
Valutazione: Accettabile

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

Gli interessati esercitano i loro diritti di accesso e di portabilità verso l'Ospedale che è il Titolare del trattamento dei dati.
Valutazione: Accettabile

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

Gli interessati esercitano i loro diritti di rettifica e di cancellazione verso l'Ospedale che è il Titolare del trattamento dei dati.
Valutazione: Accettabile

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

Gli interessati esercitano i loro diritti di limitazione e di opposizione verso l'Ospedale che è il Titolare del trattamento dei dati.
Valutazione: Accettabile

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

Gli obblighi di Voden Medical Instruments S.p.A. come Responsabile sono definiti nel documento: **Atto di Nomina Responsabile del Trattamento per il Trattamento Saphyr System *(ai sensi dell'Articolo 28 del Regolamento UE 2016/679) del 21/02/2024.***
Gli obblighi di BIONANO GENOMICS Inc come Sub-Responsabile sono definiti nel documento: **Atto di Nomina Responsabile del Trattamento per il Trattamento Saphyr System *(ai sensi dell'Articolo 28 del Regolamento UE 2016/679) del 20/03/2024.***

Valutazione: Accettabile

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

I dati che vengono raccolti dal systema Saphyr Assure vengono trasferiti e conservate negli USA.
Ai sensi dell'accordo **Data Privacy Framework** (DPF) che è in vigore dall'**11 luglio 2023** gli Stati Uniti offrono un livello di protezione adeguato per i dati personali trasferiti dall'UE a organizzazioni che hanno sede in USA.

Valutazione: Accettabile.

5. Misure esistenti o pianificate

5.1 Crittografia

Trasferimento dati crittografati: Tutti i trasferimenti di dati sono crittografati. Ciò include tutte le comunicazioni locali tra i sistemi, nonché la comunicazione con i servizi Compute On Demand e Saphyr Assure ospitati.
Protezione tramite password: Le password degli utenti archiviate nel sistema vengono sottoposte ad hashing e archiviate in un database.
Supporto HTTPS: Tutti i server Bionano Access vengono forniti con un certificato SSL autofirmato a partire dalla versione 1.6 di Bionano Access. In ogni caso si consiglia di installare un certificato SSL valido della propria organizzazione la cui autorità di certificazione può essere verificata dal Bionano Access Server e dal controller dello strumento.
Tutte le comunicazioni con il servizio Saphyr Assure vengono eseguite tramite una connessione https crittografata utilizzando Transport Layer Security (TLS) V1.2. Tutti i dati archiviati nel servizio

Saphyr Assure vengono crittografati utilizzando la crittografia AES a 256 bit utilizzando l'infrastruttura Microsoft Azure.

Originating From	Target	Protocol
Bionano Access Server	Saphyr1a Compute Node	SSH (port 22)
Bionano Access Server	Amazon SES Email service	SMTP (port 587)
Saphyr Instrument Controller Customer Workstations Compute Servers	Bionano Access Server	HTTPS (port 3005 or 3006)
Saphyr Instrument Controller	Saphyr Assure Service	HTTPS (port 443)
Bionano Access Server	Compute On Demand	HTTPS (ports 443 and 3000) HTTP (port 3001)
TeamViewer	Bionano Access Server	TCP port 5938

Valutazione: Accettabile

5.2 Anonimizzazione

Anonimizzazione: Vari elementi di dati all'interno del sistema richiedono un nome. Questi includono progetti, campioni, esperimenti e oggetti. Il cliente dovrebbe disporre di una procedura per la deidentificazione o la pseudonimizzazione di questi elementi di dati per impedire l'identificazione dei dati protetti.
Valutazione: Accettabile

5.3 Controllo degli accessi logici

Autenticazione a più fattori (Multi-Factor Authentication-MFA): L'accesso al monitoraggio dello stato del sistema e ai dati diagnostici è protetto tramite autenticazione a più fattori (MFA) e limitato al personale Bionano che richiede i dati per supportare adeguatamente il sistema.
Protezione tramite password: Le password degli utenti archiviate nel sistema vengono sottoposte ad hashing e archiviate in un database.
Scadenza password: Gli amministratori possono impostare la frequenza con cui devono scadere le password. Possono anche impostare per quanto tempo conservare le password precedenti.
Complessità della password: Gli amministratori possono anche controllare la complessità della password. Possono impostare la lunghezza minima, l'inclusione di numeri, caratteri speciali e modifiche alle maiuscole e minuscole in una password valida.
Rileva blocco MAIUSC: La pagina di accesso visualizzerà un messaggio se il blocco MAIUSC è attivo.
Primo accesso: Al primo accesso all'utente verrà richiesto di modificare la propria password.
Flusso di lavoro con password dimenticata: Dalla pagina di accesso gli utenti possono indicare di aver dimenticato la propria password. Il sistema consentirà all'utente di reimpostare la propria password da un collegamento inviato via e-mail. Il collegamento è valido per un periodo di tempo limitato.

Modifica password: Dalla schermata del profilo dell'account, gli utenti possono modificare la propria password in qualsiasi momento. Ciascuna password fornita verrà conservata nella cronologia delle password per il periodo di scadenza della password configurato.
Tentativi di accesso: Gli amministratori possono controllare il numero di tentativi di accesso consentiti prima che un account utente venga bloccato. Gli amministratori possono sbloccare gli account.
Controlli della sessione: Agli utenti non è consentito condividere account. Quando il sistema rileva un nuovo accesso su un account utente, tutte le sessioni precedenti vengono invalidate.
Inattività della sessione: Le sessioni verranno disattivate dopo un determinato periodo di inattività sul sito web. Bionano Access è in grado di rilevare l'attività su una determinata pagina; pertanto, l'attività non viene misurata esclusivamente in base al caricamento della pagina.
Ruoli utente: I privilegi di sistema sono controllati dall'assegnazione di un ruolo a un account utente. Ci sono quattro ruoli nel sistema; *Amministratore, Responsabile del progetto, Utente e Sola lettura*. Agli account utente può essere assegnato un solo ruolo. Questi ruoli sono descritti in dettaglio nella Guida Utente di Bionano Access.
Disattivazione dell'account: È possibile eliminare solo gli account a cui non sono associati dati. Gli account utente che hanno eseguito operazioni non possono essere eliminati; possono solo essere disattivati. Ciò garantisce che tutti i record dell'attività del sistema vengano conservati correttamente. Solo gli amministratori possono eliminare o disattivare gli account. Gli utenti non possono accedere agli account che sono stati disattivati.

Valutazione: Accettabile

5.4 Tracciabilità

Registrazione (Event log): Tutta l'attività del sistema viene registrata. La configurazione di sistema predefinita eseguirà il rolling dei registri ogni giorno e li conserverà per cinque giorni. Questi file di registro possono essere archiviati o configurati per rimanere per periodi di tempo più lunghi (per esempio 6 mesi). I log sono in formato JSON in modo che possano essere analizzati facilmente.
Valutazione: Accettabile

5.5 Archiviazione

Cancellazione dei dati diagnostici: Quando vengono generati i dati diagnostici dello strumento, tutti gli identificatori vengono automaticamente cancellati per rimuovere eventuali dati personali o protetti. Il set di dati disinfettati può quindi essere condiviso con il supporto Bionano per diagnosticare i problemi dello strumento. Tutti i set di dati di monitoraggio automatizzato dello stato del sistema trasmessi a Saphyr Assure vengono inoltre rimossi per rimuovere eventuali dati personali o protetti.

Valutazione: Accettabile

5.6 Minimizzazione dei dati

Raccolta dati: Saphyr Assure è progettato per raccogliere solo informazioni relative alle prestazioni dello strumento e del chip utili per determinare lo stato attuale dello strumento e prevedere le future esigenze di manutenzione. Il servizio è stato attentamente progettato per garantire che non vengano raccolte informazioni personali protette. Le informazioni dettagliate di seguito vengono raccolte anche quando viene generata una richiesta diagnostica avviata dall'utente.

Valutazione: Accettabile

5.7 Vulnerabilità

Validazione del sistema: Tutte le funzionalità dei sistemi Bionano vengono testate per ogni versione. I test di regressione garantiscono che le funzionalità di sicurezza esistenti non vengano compromesse a causa di modifiche al codice. I casi di test vengono generati per ciascuna storia utente. Per ogni versione viene generato un piano di convalida per documentare ciò che è stato testato.
Mitigazione delle minacce: I test di mitigazione delle minacce vengono condotti tenendo presente la sicurezza. Difetti, problemi di usabilità e problemi di sicurezza vengono registrati come ticket che lo sviluppo deve affrontare.
Controllo del cambiamento: Tutti i sistemi Bionano sono sotto il controllo del codice sorgente. I check-in del codice fanno riferimento al ticket che determina la modifica e ai ticket vengono forniti i numeri di impegno in modo che possano essere incrociati.
Patch di sicurezza: Bionano esamina tutte le librerie e i pacchetti in uso e determina quali devono essere aggiornati. Strumenti come retire.js per Nodejs o Safety per Python vengono utilizzati per automatizzare questa revisione ove possibile. Le librerie vengono quindi aggiornate nella base di codice e testate durante lo sviluppo per garantirne la stabilità.
Scansioni di sicurezza: Strumenti come Qualys vengono utilizzati per eseguire scansioni di sicurezza sui nostri sistemi configurati per ogni ciclo di rilascio. I problemi di sicurezza identificati vengono sottoposti a ticket per la risoluzione.
Aggiornamenti di Windows Bionano Genomics: si impegna a fornire tempestivamente aggiornamenti di sicurezza testati e convalidati. Il controller dello strumento non consente gli aggiornamenti automatici di Windows poiché spesso provocano il riavvio del sistema che interromperebbe il funzionamento dello strumento. Saphyr ICS è stato progettato per gestire il rilevamento, la convalida e l'installazione degli aggiornamenti di Windows per garantire che il sistema sia mantenuto aggiornato con gli ultimi aggiornamenti di sicurezza garantendo al tempo stesso la compatibilità con i nostri sistemi. Saphyr ICS controlla (giornalmente) la disponibilità di aggiornamenti Windows dai server Microsoft. Quando viene rilevato un aggiornamento, viene inviato al servizio Saphyr Assure per verificare se è stato testato e convalidato per funzionare correttamente con il controller dello strumento Saphyr. Quando un aggiornamento è stato testato e rilasciato, all'utente verranno notificati gli aggiornamenti in sospeso da installare. Quando lo

strumento è inattivo e non elabora un chip, l'utente può fare clic sull'icona di aggiornamento e installare gli aggiornamenti in sospeso.

Valutazione: Accettabile

5.8 Lotta contro il malware

Windows Defender: Il controller dello strumento include il programma antivirus e di rilevamento malware Windows Defender ed è configurato per proteggere il sistema senza influire negativamente sulle prestazioni del software Saphyr ICS. Gli aggiornamenti di Security Intelligence per Windows Defender vengono scaricati e installati tramite il meccanismo di Windows Update descritto nella sezione precedente. L'uso di altri prodotti può interferire con il funzionamento e le prestazioni dell'applicazione Saphyr ICS e non è consigliato.
Valutazione: Accettabile

5.9 Sicurezza dei siti web

Supporto HTTPS: Tutti i server Bionano Access vengono forniti con un certificato SSL autofirmato a partire dalla versione 1.6 di Bionano Access. In ogni caso si consiglia di installare un certificato SSL valido della propria organizzazione la cui autorità di certificazione può essere verificata dal Bionano Access Server e dal controller dello strumento.
Tutte le comunicazioni con il servizio Saphyr Assure vengono eseguite tramite una connessione https crittografata utilizzando Transport Layer Security (TLS) V1.2. Tutti i dati archiviati nel servizio Saphyr Assure vengono crittografati utilizzando la crittografia AES a 256 bit utilizzando l'infrastruttura Microsoft Azure.

Originating From	Target	Protocol
Bionano Access Server	Saphyr1a Compute Node	SSH (port 22)
Bionano Access Server	Amazon SES Email service	SMTP (port 587)
Saphyr Instrument Controller Customer Workstations Compute Servers	Bionano Access Server	HTTPS (port 3005 or 3006)
Saphyr Instrument Controller	Saphyr Assure Service	HTTPS (port 443)
Bionano Access Server	Compute On Demand	HTTPS (ports 443 and 3000) HTTP (port 3001)
TeamViewer	Bionano Access Server	TCP port 5938

Valutazione: Accettabile

5.10 Contratto con il responsabile del trattamento

BIONANO GENOMICS Inc è stata nominata Sub-Responsabile del trattamento attraverso il documento: *BIONANO Data Processor nomination for Saphyr System* del 21/03/2024
Valutazione : Accettabile

5.11 Sicurezza dei canali informatici

Firewall: tutti i computer forniti da Bionano hanno i firewall abilitati e sono impostati per consentire solo il traffico nativo.
L'immagine "Risorse e schema della rete.jpeg" illustra l'architettura di alto livello della tipica soluzione dati per l'installazione di uno strumento Saphyr. Il Saphyr è collegato tramite USB3, USB2 e CAN-BUS al controller dello strumento. L'Instrument Controller e il server di accesso Bionano sono stati progettati per essere posizionati accanto al Saphyr in laboratorio. L'Instrument Controller è connesso al Bionano Access Server tramite rete. Includiamo un cavo di collegamento in modo che l'elaborazione del chip possa continuare in caso di interruzione della rete del cliente. I server di calcolo sono installati nel data center del cliente e la comunicazione tra Bionano Access Server e i server di calcolo avviene sulla rete del cliente. La comunicazione tra il Instrument Controller e il server di accesso Bionano è HTTPS. C'è anche traffico HTTPS proveniente dai nodi di calcolo al Bionano Access Server. Per impostazione predefinita forniamo un certificato SSL autofirmato. Raccomandiamo che il cliente installi un certificato SSL valido sul Bionano Access Server quando possibile. Gli indirizzi IP statici sono richiesti per Bionano Access Server e ciascun nodo nel cluster di calcolo.

Il Instrument Controller è stato progettato per limitare e ridurre la superficie di attacco disabilitando i servizi non necessari del sistema operativo e disabilitando tutto il traffico di rete in entrata non richiesto. Saphyr può essere configurato per funzionare in modalità kiosk che blocca l'accesso dell'utente al sistema operativo e consente solo l'interazione con il software Instrument Control. Questa è la modalità operativa consigliata in ambienti ad alta sicurezza.
Valutazione: Accettabile

5.12 Controllo degli accessi fisici

I dispositivi Saphyr, Instrument Controller, Bionano Access Server e Computer Cluster sono presso la sede dell'Ospedale e il controllo degli accessi fisici alla sala server è regolato dall'Ospedale stesso.
Saphyr Assuree il Computer On Demand sono in hosting presso il datacenter di Bionano e il controllo degli accessi fisici è regolato da datacenter.
Valutazione: Accettabile

5.13 Prevenzione delle fonti di rischio

Nel documento CG-30292_Rev. E_Data-Security-Guidelines, Bionano Genomics specifica quali sono le misure messe in atto allo scopo di prevenire le fonti di rischio (vedi cap. 7)
Valutazione: Accettabile

5.14 Politica di tutela della privacy

Bionano si impegna a tutelare la sicurezza dei dati personali e protetti. Adotta ragionevoli misure di sicurezza fisiche, digitali e amministrative per proteggere le informazioni personali da accessi non autorizzati o inappropriati. Bionano non vende né condivide dati personali o protetti con terzi senza esplicita autorizzazione. Bionano Compute On Demand non conserva alcun dato protetto sui sistemi ospitati oltre la durata del lavoro come indicato nei suoi termini di utilizzo. Saphyr Assure non raccoglie alcun dato protetto; raccoglie solo dati diagnostici e sullo stato del sistema.

Valutazione: Accettabile

5.15 Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Sistema di ticket: internamente viene utilizzato un sistema di ticket per tenere traccia di tutti i difetti e le richieste di funzionalità. Il sistema di ticketing garantisce che tutte le modifiche siano visibili al team di Bionano Software Quality Assurance (SQA). Il sistema di ticketing inoltre applica e documenta il flusso di lavoro necessario per convalidare ogni modifica del sistema completata.
In Voden Medical Intruments è in atto il processo di gestione dei Data Breach.
Valutazione: Accettabile

6. Rischi - Accesso illegittimo ai dati

- *Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?*
  Compromissione della riservatezza, dell'integrità e della disponibilità dei dati personali dei pazienti.
- *Quali sono le principali minacce che potrebbero concretizzare il rischio?*
  Spoofing, Tampering, Denial of service, Elevantion of Privilege
- *Quali sono le fonti di rischio?*
  Lo spoofing è legato a tutte le tattiche utilizzate dagli aggressori per ottenere informazioni sensibili come le credenziali direttamente dall'utente o per impersonare l'utente., I dati possono essere modificati durante il transito, I dati possono essere rubati durante il trasporto, Azione di minaccia intesa ad ottenere un accesso privilegiato alle risorse al fine di ottenere un accesso non autorizzato alle informazioni o di compromettere un sistema
- *Quali misure fra quelle individuate contribuiscono a mitigare il rischio?*
  Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Sicurezza dei siti web, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- *Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?*
  Limitata.
- *Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?*
  Limitata.

Valutazione: Accettabile

7. Rischi - Modifiche indesiderate dei dati

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

Compromissione della riservatezza, dell'integrità e della disponibilità dei dati personali dei pazienti.

- *Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?*
  Denial of service, Elevantion of Privilege, Spoofing, Tampering
- *Quali sono le fonti di rischio?*
  Azione di minaccia intesa ad ottenere un accesso privilegiato alle risorse al fine di ottenere un accesso non autorizzato alle informazioni o di compromettere un sistema, I dati possono essere modificati durante il transito, I dati possono essere rubati durante il trasporto, Lo spoofing è legato a tutte le tattiche utilizzate dagli aggressori per ottenere informazioni sensibili come le credenziali direttamente dall'utente o per impersonare l'utente.
- *Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?*
  Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Archiviazione, Vulnerabilità, Lotta contro il malware, Sicurezza dei siti web, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Controllo degli accessi fisici, Prevenzione delle fonti di rischio, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- *Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?*
  Trascurabile. Gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente, in quanto il database dei loro dati è criptato.
- *Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?*
  Trascurabile.

Valutazione: Accettabile

8. Rischi - Perdita di dati

- *Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?*
  Compromissione della riservatezza, dell'integrità e della disponibilità dei dati personali dei pazienti.
- *Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?*
  Denial of service, Elevantion of Privilege, Spoofing, Tampering
- *Quali sono le fonti di rischio?*
  Azione di minaccia intesa ad ottenere un accesso privilegiato alle risorse al fine di ottenere un accesso non autorizzato alle informazioni o di compromettere un sistema, I dati possono essere modificati durante il transito, I dati possono essere rubati durante il trasporto, Lo spoofing è legato a tutte le tattiche utilizzate dagli aggressori per ottenere informazioni sensibili come le credenziali direttamente dall'utente o per impersonare l'utente.
- *Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?*
  Crittografia, Anonimizzatine, Controllo degli accessi logici
- *Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?*

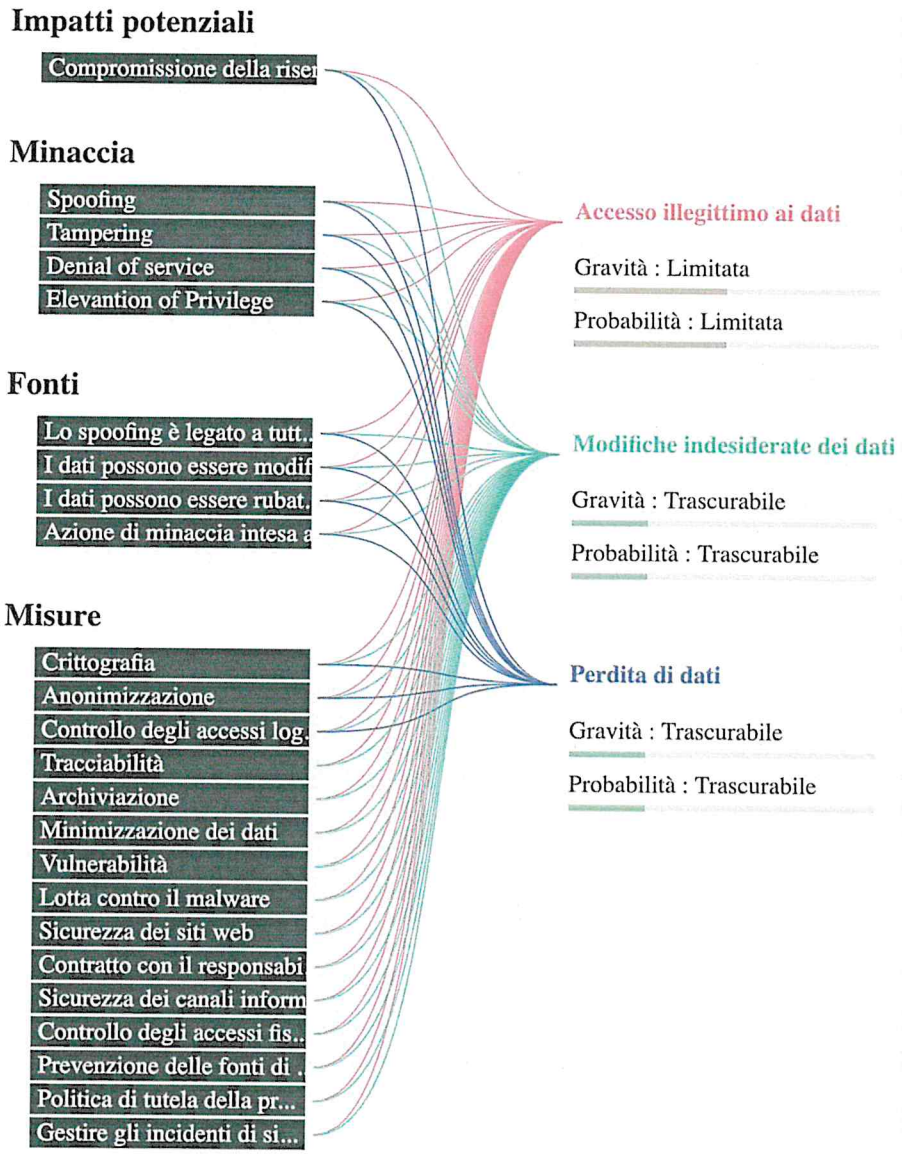
Trascurabile.

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

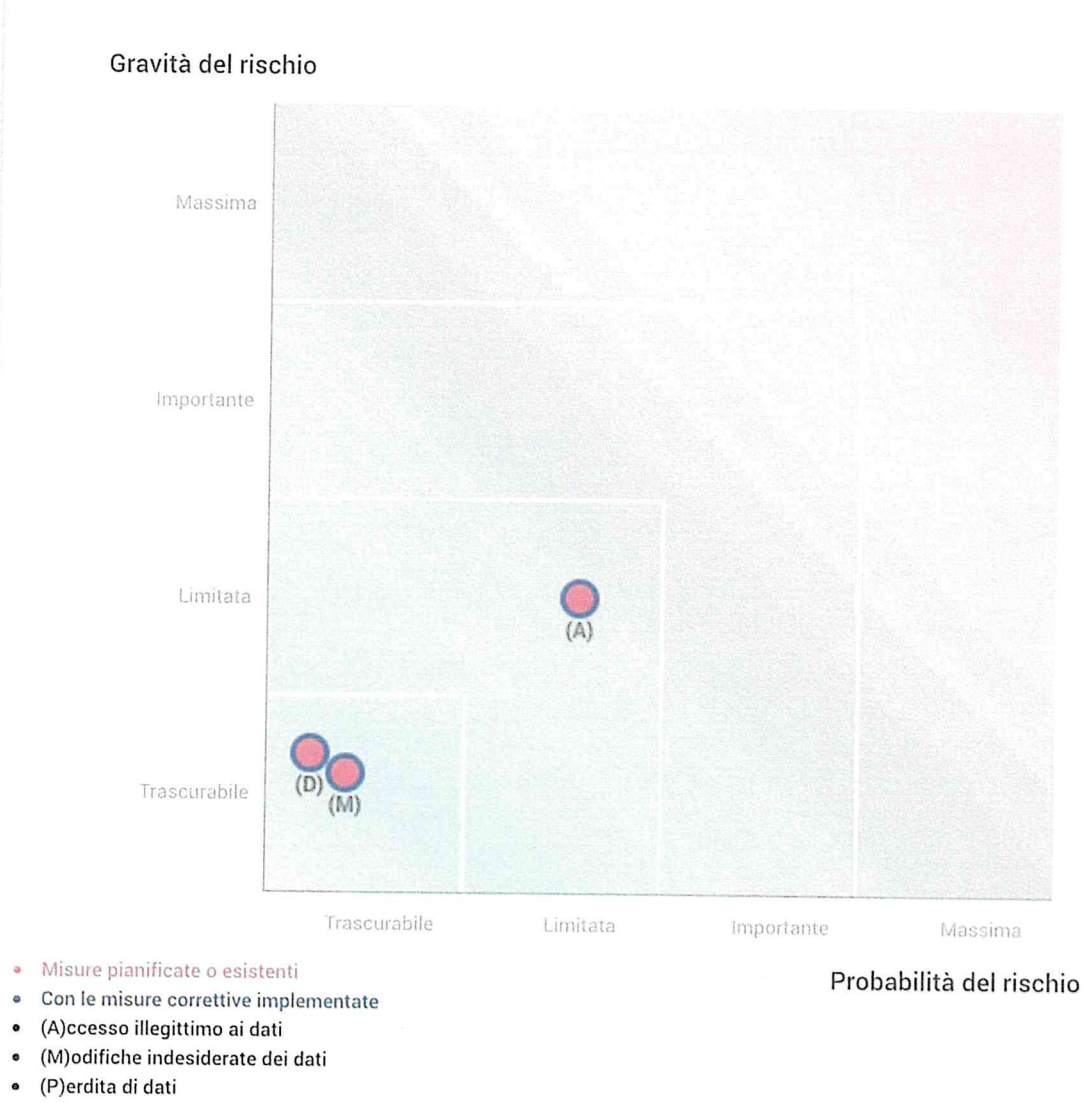
Valutazione: Accettabile

9. Rischi – Rappresentazione grafica

9.1 Panoramica dei rischi



9.2 Mappa dei rischi



10. Piano di trattamento dei rischi