MARSH

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

LEADERSHIP, KNOWLDGE, SOLUTIONS…WORDLWIDE.

MARSH & McLENNAN COMPANIES

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Nota: la polizza richiesta attraverso il presente questionario è una polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Si prega di leggere e compilare attentamente il seguente questionario.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Ragione Sociale:	Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico
Indirizzo:	Via Francesco Sforza 28 – 20122 Milano
Sede legale:	Fare clic qui per immettere testo.
Telefono:	02-55031
Indirizzo Web:	Www.policlinico.mi.it

1.2 La Proponente è continuamente in attività dal: 2005

1.3 Descrizione dell'attività svolta dalla proponente: Istituto di ricovero e cura a carattere scientifico di natura pubblica

1.4 Numero di Dipendenti: 3400

1.5 Si prega di allegare copia dell'ultimo bilancio: https://www.policlinico.mi.it/amministrazione_trasparente/12-bilanci

1.6 Fatturato della Proponente:

	Annualità		
	Precedente	Corrente	Prossima
Totale Fatturato	€ 427,160,000 (valore della produzione)	€ 427,070,533 (valore della produzione)	€ 427,333,000.(valore della produzione)

Ripartizione geografica del fatturato della Proponente (%)			
Unione Europea	€ 427,160,000 (valore della produzione)	€ 427,070,533 (valore della produzione)	€ 427,333,000.(valore della produzione)
USA/CANADA	€ 0.	€ 0,00	€ 0.
Resto del Mondo	€ 0.	€ 0.	€ 0.

1.7 Si prevedono cambiamenti significativi nella natura o nella dimensione del business della proponente nei prossimi dodici (12) mesi? SI☐ NOX

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

1.8 Vi sono stati cambiamenti di questo genere negli ultimi 12 mesi (12) mesi? SI☐ NOX

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

1.9 Negli ultimi dodici (12) mesi, la Proponente ha completato o concordato una fusione, acquisizione o consolidamento? (sia che queste operazioni siano state portate a termine o meno) SI☐ NOX

1.10 La Proponente ha intenzione di portare a termine operazioni di questo tipo nei prossimi dodici (12) mesi? SI☐ NOX

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

Sezione 2. Carte di Pagamento

2.1 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☒ NO☐

Se si:

2.1.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: Fare clic qui per immettere testo.

<10%

2.2 La proponente è dotata di un e-commerce attraverso il quale effettua attività di vendita? SI☐ NO☒

Se si:

2.2.1 Indicare la percentuale di fatturato derivante da vendite effettuate tramite l'e-commerce: Fare clic qui per immettere testo.

2.3 La proponente(se soggetta) è conforme alle vigenti norme di sicurezza emesse dalle istituzioni finanziarie con le quali è convenzionata (Payment Card industry Data Security Standards PCI DSS)?

NON SOGGETTA ☒

CONFORME ☐

NON CONFORME ☐

Se non conforme:

2.3.1 Si prega di descrivere lo stato attuale di qualsiasi opera di adeguamento e la relativa data di completamento prevista: Fare clic qui per immettere testo.

2.4 La proponente processa pagamenti per conto di altri, comprese transazioni e-commerce? SI☐ NO☒

Se si:

2.4.1 Si prega di fornire il numero di clienti per cui vengono gestiti i pagamenti e una stima del numero di transazioni per cliente: Fare clic qui per immettere testo.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI ☒ NO ☐

3.2 Negli ultimi due anni, la Proponente ha effettuato verifiche interne o esterne relative alla privacy o ha ottenuto un certificato di adeguatezza dei sistemi adottati per la privacy? SI ☒ NO ☐

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.
Audit ARIA

3.3 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? SI ☒ NO ☐

3.4 La Proponente prevede che le terze parti con cui condivide dati personali o informazioni confidenziali risarciscano la Proponente per responsabilità derivanti da diffusione di tali informazioni dovuta a colpa o a negligenza di tali terze parti? SI ☐ NO ☒

3.5 Indicare quale tipo di informazioni, e in che quantità, sono registrate nel database:

Tipologia	Barrare se registrate	Numero di record
Informazioni su carte di credito/debito	☐	Fare clic qui per immettere testo.
Informazioni sanitarie	☒	1.088.897 / anno.
Carta di identità		Fare clic qui per immettere testo.
Informazioni sulla previdenza (es. INPS)	☒	4972.
Informazioni riguardo conti corrente	☒	6110.
Dati generali del cliente		Fare clic qui per immettere testo.
Proprietà Intellettuali del cliente	☐	Fare clic qui per immettere testo.
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La proponente pubblica e distribuisce ai propri dipendenti le policy sui sistemi informativi? SI X NO☐

4.2 La Proponente esige un feedback positivo da ciascun dipendente sulla comprensione ed accettazione delle policy di cui sopra? SI☐ NO X

I corsi erogati in modalità FAD prevedono un test finale con punteggio

---

4.3 La Proponente fornisce corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI X **NO☐**

Se si, si prega di indicare la frequenza di tali corsi: annua

---

4.4 La Proponente dispone di un:

Piano di disaster recovery	SI X	NO☐
Piano di business continuity	SI X	NO☐
Piano di risposta alle intrusioni di rete e infezioni da virus	SI X	NO☐

Se si dispone di uno o più dei sopra-citati documenti, *si prega di allegarne copia.*

4.5 La Proponente dispone di un programma che metta alla prova e testi periodicamente i controlli di sicurezza? SI X NO☐

Se si, si prega di fornire informazioni su tali test: Fare clic qui per immettere testo.

4.6 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda? SI X NO☐

4.7 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Controlli di accesso alla rete	X
Anti virus	X
Firewall	X
Rilevatori di intrusione	X

4.8 Indicare se la Proponente ha svolto un security audit negli ultimi 24 mesi SI X NO☐

Se si, si prega di fornire maggiori dettagli: svolto da ARIA spa nell'ambito delle attività del centro di competenza sulla sicurezza informatica rivolto alle aziende sanitarie regionali

4.9 Indicare se la Proponente incoraggi l'uso di password complesse ed effettui verifiche periodiche sulle modalità di accesso degli utilizzatori SI X NO☐

4.10 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale SIX NO☐

4.11 La Proponente esegue il backup quotidiano di tutti i dati rilevanti/sensibili? SI X NO☐

Se no, si prega di indicare le eccezioni: Fare clic qui per immettere testo.

4.12 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni? SI X NO☐

è attiva la procedura di backup con dati salvati in un sito remoto gestito da ARIA spa nell'ambito del servizio denominato Disater Recovery Tier III .

4.13 La Proponente possiede e applica una regolamentazione in materia di crittografia

della comunicazione interna ed esterna?

SI☐ NO X

4.13.1 I computer e i dispositivi portatili (come ad esempio le chiavi USB) sono protetti da crittografia?

SI☐ NO X

4.13.2 La Proponente cripta i dati custoditi all'interno delle banche dati informatiche?

SI☐ NO X

4.13.3 La Proponente cripta le informazioni in uscita?

SI☐ NO X

4.14 Si prega di fornire una descrizione di tutte le tecnologie di protezione dei dati personali (PET) che il proponente ha implementato o che prevede di implementare:

accesso solo ad utenti nominativi in corrispondenza di un evento di cura o di un atto amministrativo

4.15 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch?

SI X NO☐

Se si:

4.15.1 Le patch critiche sono installate entro 30 giorni dal rilascio? SI X NO☐

4.16 Si prega di indicare in che quantità la Proponente dispone dei seguenti dispositivi:

	< 100	101 - 1000	> 1001
Computer fissi	☐	☐	X
Dispositivi portatili	☐	X	☐
Numero di server	☐	X	☐

3200 computer desktop

520 computer portatili

100 server per i quali è in corso la migrazione nel Data Center di ARIA spa

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI X NO☐

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	X
Raccolta dati e/o processo	☐
Call center / Service desk	X
Operational business process	☐
Altro *(specificare sotto)*	X

Manutenzione postazioni di lavoro informatiche, Fornitura e manutenzione software

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	X
Esternalizzati in Host	X
Esternalizzati in Cloud	☐

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate? SI X NO☐

5.3 La Proponente richiede ai fornitori di sottoscrivere una polizza per l'assicurazione della responsabilità civile professionale o una polizza di RC per la protezione dei dati? SI☐ NO X

5.4 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☐ NO X

5.5 Indicare se la Proponente contrattualizza un Service Level Agreement (SLA) con terzi fornitori in grado di facilitare il monitoraggio degli incidenti, il reporting e le azioni per mitigare i danni SI☐ NO X

5.6 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT SI X NO☐

Sezione 6. Interdipendenza IT e piani di emergenza

6.1 Indicare se la Proponente ha implementato, testato e gestito piani di emergenza IT e di emergenza aziendale SI X NO☐

Sono stati predisposti documenti e modelli per la gestione di emergenze causate dalla mancanza dei normali supporti informatici.
Sono state predisposte procedure di evacuazione e procedure di disaster recovery per le biobanche.
Vengono regolarmente effettuati test di interruzione di energia elettrica.

6.2 Si prega di indicare quali tipi di test sono stati svolti o sono programmati:

Table Top Testing	☐	Data dell'ultimo test: Fare clic qui per immettere testo.
Simulazione	X	Data dell'ultimo test: giugno 2019
Test di interruzione parziale	X	Data dell'ultimo test: 18-2-2020
Test di interruzione totale	☐	Data dell'ultimo test: Fare clic qui per immettere testo.

6.3 Si prega di indicare quale tipo di misure di emergenza la Proponente ha installato:

Accordi reciproci	☐	Data di ultima attivazione: Fare clic qui per immettere testo.
Cold Standby Site	X	Data di ultima attivazione: Fare clic qui per immettere testo.
Hot Standby Site	☐	Data di ultima attivazione: Fare clic qui per immettere testo.
Continuous Replication Sites	☐	

E' iniziata l'attività che porterà entro la fine del 2020 al trasferimento dei server nel Data Center di Aria che prevede un Hot Standby site. I test verranno fatti al completamento della migrazione.

6.4 Si prega di indicare il tempo dopo il quale l'impossibilità per i vostri dipendenti / appaltatori di accedere ai sistemi informatici della Proponente avrebbe un impatto significativo sulla vostra attività:

Immediatamente X	Dopo 4 ore ☐	Dopo 8 ore ☐	Dopo 24 ore ☐	Mai ☐

6.5 Nel caso di interruzione di rete o di guasto del sistema, si prega di indicare se l'impossibilità per i clienti ad accedere ai sistemi informatici della Proponente avrebbe un impatto significativo sulla sua attività:

Immediatamente X	Dopo 4 ore ☐	Dopo 8 ore ☐	Dopo 24 ore ☐	Mai ☐

6.6 Nel caso di interruzione di rete o di guasto del sistema, si prega di indicare una stima della massima perdita finanziaria per ogni ora di interruzione:

Fare clic qui per immettere testo.

6.7 Si prega di indicare se la Proponente considera la propria dipendenza da infrastrutture IT, sistemi e reti essenziale alla propria attività

SI X NO ☐

Sezione 7. Contenuti multimediali, Website e Social Network

7.1 La proponente dispone di una procedura di risposta ad eventuali accuse che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☐ NO X

7.2 La proponente dispone di un legale qualificato che vagli tutti i contenuti prima della loro pubblicazione sul sito internet dell'assicurato? SI☐ NO X

Se si, la vagliatura comprende i seguenti punti:

7.2.1	Violazione della privacy	SI☐	NO☐
7.2.2	Violazione del copyright	SI☐	NO☐
7.2.3	Violazione del marchio	SI☐	NO☐
7.2.4	Problematiche di denigrazione	SI☐	NO☐

Se no, si prega di descrivere le procedure per evitare la pubblicazione di contenuti impropri o illegali: le pubblicazioni sono gestite centralmente dall'UO Comunicazione e gli utenti non sono autonomi nelle pubblicazioni sul sito.
E' stato redatto e distribuito un regolamento sull'uso delle comunicazioni con strumenti informatici.

7.3 La Proponente dispone di un sito internet aziendale? SI X NO☐

Se si, sono previste:

7.4.1	Procedure di opt in / opt out durante la raccolta di informazioni personali degli utenti?	SI X	NO☐
7.4.2	Procedure per la tracciabilità dei visitatori (cookies, ecc.)	SI X	NO☐

7.4 La Proponente dispone di profili su Social Network? SI X NO☐

Se si, si prega di fornire maggiori dettagli: **Twitter e YouTube**.

Sezione 8. Sinistri e circostanze

8.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☐ NO ☒

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa: Fare clic qui per immettere testo.

8.2 Negli ultimi tre anni, la Proponente ha mai ricevuto lamentele o richieste di cessione o sospensione in seguito a violazioni di marchi registrati, copyright, privacy o diffamazione riguardo a qualsiasi contenuto pubblicato, esposto o distribuito da o per conto della Proponente? SI☐ NO ☒

Se si, si prega di fornire maggiori dettagli sulle richieste ricevute: Fare clic qui per immettere testo.

8.3 La Proponente è mai stata oggetto di azioni investigative riguardo a una presunta violazione di qualsiasi legge sulla privacy? SI☐ NO ☒

Se si, si prega di fornire dettagli di ciascun azione o investigazione: Fare clic qui per immettere testo.

8.4 La Proponente ha mai subito un tentativo di estorsione dei suoi sistemi informatici? SI☐ NO ☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

8.5 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza) o attacchi DDoS ai propri sistemi informatici nei tre anni precedenti a questa richiesta? SI☐ NO ☒

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o per ricostruire i database o i software: Fare clic qui per immettere testo.

8.6 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO ☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

Sezione 9. Precedenti Assicurazioni

9.1 La Proponente è attualmente in possesso di una polizza che copra danni tecnologici, violazione della privacy o sicurezza della rete? SI☐ NO ☒

Se si, si prega di fornire le seguenti informazioni:

Assicuratore:	Fare clic qui per immettere testo.
Massimale aggregato annuo:	Fare clic qui per immettere testo.
Franchigia:	Fare clic qui per immettere testo.
Durata della polizza.	Fare clic qui per immettere testo.
Premio:	Fare clic qui per immettere testo.
Retroattività	Fare clic qui per immettere testo.

9.2 La Proponente si è mai vista rifiutare o cancellare una polizza che copra danni tecnologici, violazione di privacy o di sicurezza della rete? SI☐ NO ☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

AVVISO IMPORTANTE

La persona autorizzata a sottoscrivere il presente questionario dichiara, ai sensi degli artt. 1892 e 1893 c.c., che, per quanto in sua conoscenza in relazione alle funzioni espletate, le affermazioni precedentemente riportate sono veritiere e che qualora insorgano modifiche tra la data di firma del presente e la data di entrata in vigore della copertura, egli darà immediata notifica di tali modifiche, e la società assicuratrice potrà ritirare oppure modificare la propria proposta e/o conferma di copertura. Il presente questionario ed ogni suo allegato possono essere parti integranti della polizza.

Indicare nome e titolo della persona autorizzata a sottoscrivere in nome della Società Proponente.

Firmato: Angelo Luigi Caroli

Direttore f.f. UOC Sistemi Informativi

Data: Milano 20-2-2020

Vi invitiamo ad inviare il documento ai seguenti contatti:

Marsh Contacts – FINPRO practice

Paolo Tagliabue

e-mail: paolo.tagliabue@marsh.com

Alessandro Vitullo

e-mail: alessandro.vitullo@marsh.com