UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Privacy e Cybersecurity nelle Emergenze Sanitarie

SILVA MANA

Dipartimento di affiliazione

Ente di affiliazione

Contatti +39 3807587776

Lunedì 16 settembre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Rischi e misure di protezione nel trattamento dei dati da parte dei soccorritori delle associazioni di volontariato

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Il Contesto delle Emergenze Sanitarie

- Nel contesto delle emergenze sanitarie, il trattamento dei dati personali dei pazienti rappresenta una delle sfide più delicate per le organizzazioni di soccorso volontario. Le associazioni si trovano a gestire dati altamente sensibili in condizioni operative complesse.

- L'obiettivo di questa analisi è esaminare i principali rischi legati alla protezione dei dati personali nelle attività di emergenza e assistenza continuativa, con particolare riferimento al ruolo del DPO condiviso e alla gestione della corresponsabilità con enti pubblici.

Quadro Normativo di Riferimento

GDPR

- Regolamento UE 2016/679 - disciplina generale in materia di protezione dei dati personali

Codice Privacy Italiano

- D.Lgs. 196/2003, aggiornato con D.Lgs. 101/2018, integrato dai provvedimenti del Garante

Normativa Sanitaria

- Disciplina specifica sui dati sanitari (art. 9 GDPR) e linee guida del settore

Definizioni Chiave nel Trattamento Dati

Dati Personali -categorie particolari di dati personali

Informazioni che identificano una persona fisica, con particolare attenzione ai dati sanitari considerati "particolari" secondo l'art. 9 GDPR

Titolare e Responsabile

Il titolare determina finalità e mezzi del trattamento, mentre il responsabile agisce per conto del titolare secondo istruzioni specifiche

Data Protection Officer

Figura professionale che supervisiona la conformità al GDPR e può essere condivisa tra più associazioni di volontariato

Emergenza vs Assistenza

Il titolare determina finalità e mezzi del trattamento, mentre il responsabile agisce per conto del titolare secondo istruzioni specifiche

Criticità Operative nel Soccorso

Criticità Operative nel Soccorso	• Utilizzo di strumenti non sempre sicuri per la raccolta di informazioni sensibili durante gli interventi di emergenza • Moduli cartacei esposti a smarrimento • Dispositivi mobili non protetti Annotazioni su supporti temporanei
Comunicazioni Non Cifrate	• Trasmissione di dati sensibili attraverso canali di comunicazione non sicuri • Radio analogiche intercettabili Messaggistica • WhatsApp non conforme • Email non crittografate
Conservazione Inadeguata	• Problematiche nella gestione e archiviazione sicura della documentazione raccolta • Archivi fisici non protetti • Backup digitali insufficienti • Tempi di conservazione non definiti

Trasporti Sanitari Continuativi: Alto Rischio Privacy
Servizi ad Alto Rischio

- Trasporti regolari per pazienti in terapia dialitica con necessità di gestire dati sanitari specifici

DIALISI

- Accompagnamento per terapie oncologiche che richiedono particolare riservatezza

ONCOLOGIA

- Servizi continuativi presso il domicilio del paziente con accesso a informazioni personali

ASSISTENZA DOMICILIARE

Minacce Cyber alle Associazioni di Volontariato

- ## Phishing e Social Engineering
  Attacchi mirati ai volontari attraverso email fraudolente che mirano a sottrarre credenziali di accesso

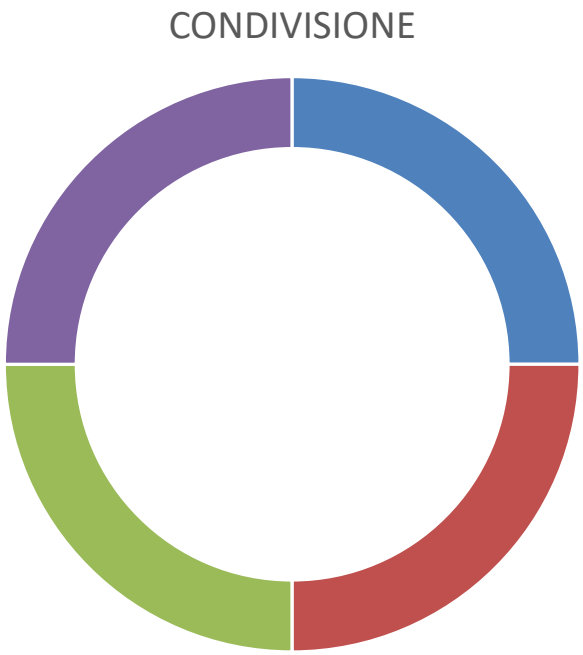
- ## Ransomware
  Malware che cripta i dati dell'associazione richiedendo un riscatto per il ripristino

- ## Vulnerabilità Sistemiche
  Assenza di sistemi di backup, protezioni endpoint inadeguate e mancanza di formazione informatica

Il DPO Condiviso: Una strategia di Governance per le Associazioni

Possibilità per più associazioni di nominare un unico DPO, riducendo i costi e aumentando l'expertise

Programmi di formazione uniformi per volontari e dipendenti di tutte le associazioni



Coordinamento della documentazione, DPIA e formazione attraverso un approccio standardizzato

Controllo delle informative, contratti e procedure di compliance per tutte le associazioni coinvolte

Governance Privacy nelle Strutture Miste

Responsabilità del Presidente

Nelle associazioni che operano con **dipendenti e volontari**, il **Presidente**, in qualità di rappresentante legale dell'associazione (Titolare del trattamento), **ha il compito di garantire l'adozione e il rispetto delle norme privacy**, assumendo responsabilità organizzative e gestionali:

Definizione delle policy privacy
Supervisione della compliance normative
Organizzazione della formazione
Gestione dei rapporti con il DPO

È fondamentale formalizzare un organigramma privacy che definisca chiaramente ruoli e responsabilità di ciascun attore coinvolto

Corresponsabilità con Enti Pubblici Sanitari

1. **Collaborazioni AST**
   Partnership con Aziende Sanitarie Uniche Regionali per servizi integrati di trasporto e assistenza

2. **Rapporti Ospedalieri**
   Convenzioni con strutture ospedaliere per trasporti programmati e servizi di supporto

3. **Contitolarità Trasporti**
   Gestione condivisa dei dati per trasporti dializzati e pazienti cronici con responsabilità definite

4. **Affidabilità Supply Chain**
   Obbligo di verifica dell'affidabilità informatica secondo le direttive ACN

Data Breach nel Settore Sanitario: Casi Significativi

1

ULSS 6 Euganea (2022)

Attacco ransomware che ha compromesso i dati di 39.852 CITTADINI nel sistema sanitario veneto

- Interruzione servizi digitali per settimane settimane
- Compromissione cartelle cliniche
- Impatto su prenotazioni e referti

2

ASL Napoli 3 Sud (2022)

Divulgazione online di documenti contenenti contenenti cartelle cliniche e dati sensibili dei dei pazienti

- Pubblicazione non autorizzata su dark web web
- Violazione massiva della privacy
- Sanzioni amministrative 30.000 EURO

3

Nel periodo 2023-2024, il numero di eventi cyber nel settore sanitario è aumentato drasticamente, con un incremento del 111%, passando da 27 eventi nel 2023 a 57 nel 2024. Le minacce più frequenti includono ransomware, attacchi malware e compromissioni tramite credenziali valide. Gli attacchi ransomware, in particolare, hanno avuto un impatto significativo, rappresentando il 36% degli eventi nel 2023.

A luglio 2024, un attacco alla supply chain ha colpito un fornitore di servizi IT, causando gravi danni a più enti sanitari interconnessi. Questo episodio ha messo in evidenza la vulnerabilità sistemica del settore, che è sempre più esposto a minacce sofisticate.

Trattamenti illeciti Associazione Volontariati: Casi Significativi Proveddimenti

Provvedimento 10070596 del Garante Privacy (26 settembre 2024)
Soggetto interessato
Si tratta di un'associazione non profit (ETS) che è stata oggetto di un accertamento da parte del Garante per la protezione dei dati personali per presunte violazioni del GDPR.

- **Violazioni rilevate**
  - Trattamento illecito dei dati personali in quanto alcune attività poste in essere non rispettavano i principi di liceità, correttezza e trasparenza previsti dall'art. 5 del GDPR.
  - Informative non sufficientemente complete o mancanti, rendendo poco chiaro agli interessati chi fosse il titolare, come venivano trattati i dati, con chi venissero condivisi, ecc.
  - Manca o è carente la documentazione formale: ad esempio un registro dei trattamenti, atti di nomina degli incaricati, moduli consenso appropriati laddove richiesti.
- **Impatto e rischio**
  - I dati coinvolti erano persone che avevano rapporti con l'associazione: utenti, beneficiari, volontari.
  - Il Garante ha rilevato che, anche se l'associazione non aveva intento malevolo, la mancanza di misure adeguate determina responsabilità.
  - È stato considerato il rischio per i diritti e le libertà degli interessati, che può aumentare in presenza di dati sensibili o categorie vulnerabili.
- **Decisione del Garante**
  - L'associazione è stata sanzionata, ma il Garante ha applicato una sanzione **ridotta**, tenendo conto del fatto che si tratta di un ente non profit e della natura delle violazioni.
  - È stato imposto un ordine di adeguamento: aggiornare l'informativa privacy, predisporre il registro dei trattamenti, formalizzare le nomine degli incaricati al trattamento, eventualmente fornire una formazione specifica sul GDPR.
- **Lezioni e obblighi**
  - Anche le organizzazioni del Terzo Settore devono prendere sul serio i propri obblighi sotto il GDPR, specialmente quando trattano dati personali in modo continuativo.
  - Non basta la buona volontà: serve una governance documentata, procedure scritte, e formazione delle persone coinvolte.
  - Il fatto di essere un ente non profit non esime dalle responsabilità, ma può incidere sull'ammontare della sanzione.

Impatto sui Servizi di Soccorso Volontario

Perdita di Fiducia

- Compromissione del rapporto con gli assistiti e riduzione della credibilità dell'associazione

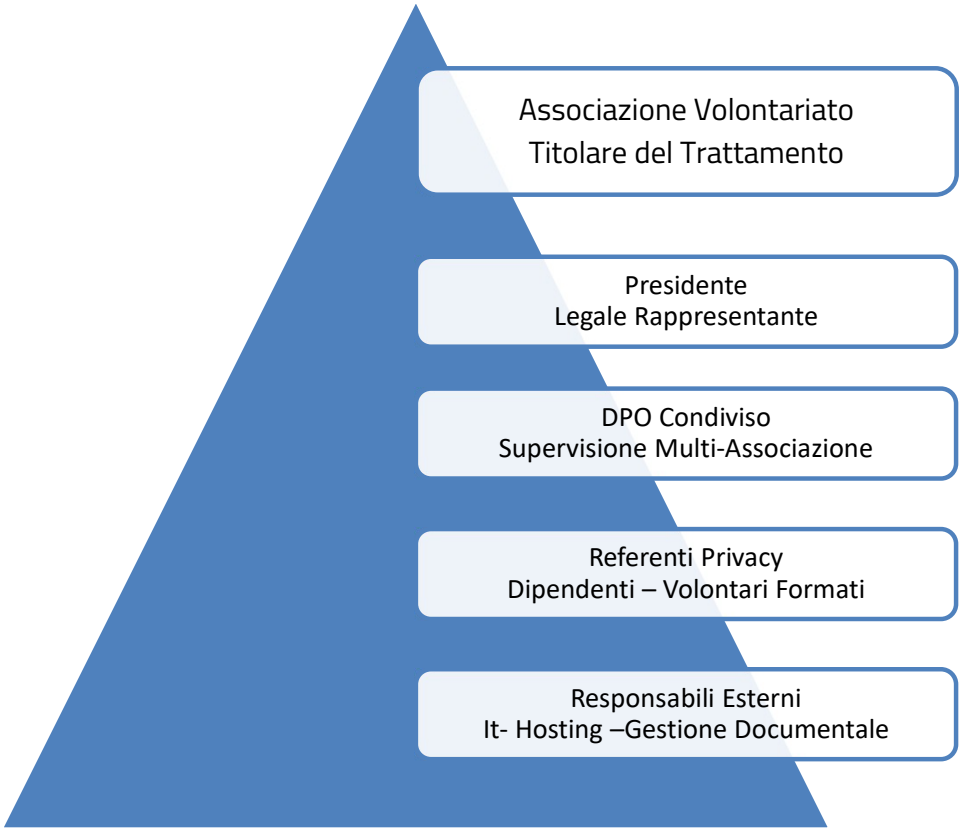
Sanzioni Economiche

- Multe amministrative e potenziali risarcimenti per danni causati dalla violazione

Interruzione Servizi

- Blocco temporaneo delle attività digitali e dei servizi essenziali

Modello Operativo: Organigramma Privacy Condiviso



Modello Operativo: Organigramma Privacy Condiviso

Informativa Semplificata per Servizi Continuativi

Formazione Annuale
Corsi privacy per volontari e dipendenti con aggiornamenti normative

Protocolli Operativi
Procedure standardizzate per dialisi, trasporti cronici e assistenza domiciliare

Verifica Documentazione
Controllo annuale della conformità e aggiornamento delle procedure

Bibliografia

1. **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR). *Gazzetta ufficiale dell'Unione europea*, L 119, 4.5.2016, p. 1–88.
2. **Garante per la protezione dei dati personali**. (2020). *Provvedimento n. 9459989 del 6 febbraio 2020 – Data breach in ambito associativo con dati su minori e soggetti fragili*. Disponibile su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10070596 (consultato: settembre 2025).

3. **Garante per la protezione dei dati personali**. (2022). *Violazione dei dati presso ULSS 6 Euganea: Dati sanitari accessibili per errore informatico*. Provvedimento pubblicato il 13 luglio 2022. Disponibile su: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9795348 (consultato: settembre 2025).

4. **Garante per la protezione dei dati personali**. (2022). *Data breach ASL Napoli 3 Sud: violazione dati sanitari – Provvedimento del 3 novembre 2022*. Disponibile su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9835849 (consultato: settembre 2025).

5. **ENISA - European Union Agency for Cybersecurity**. (2022). *Guidelines on Data Breach Notification under the GDPR*. Disponibile su: https://www.enisa.europa.eu (consultato: settembre 2025).
6. **CNIL - Commission Nationale de l'Informatique et des Libertés**. (2022). *Data Breach Notification Guidelines*. Parigi, CNIL. Disponibile su: https://www.cnil.fr (consultato: settembre 2025).
7. **Pizzetti, F.** (2018). *Privacy e il nuovo Regolamento europeo: Una guida alla lettura del GDPR per i soggetti pubblici e privati*. Milano: Giuffrè Francis Lefebvre.