Comunicazione di violazione dei dati all'interessato ex art. 34 GDPR da parte della Casa di cura privata Malatesta novello s.r.l.

In ossequio all'art. 34 del Regolamento UE 2016/679 (GDPR), si avvisa che il responsabile esterno Synlab Italia s.r.l. ha rilevato sulla propria infrastruttura informatica, a partire 18 aprile 2024, una cifratura dei dati personali e successivamente un attacco cybercriminale di tipo ransomware con conseguente sottrazione illecita, da Synlab rilevata in data 12 giugno 2024 e dalla scrivente appresa in data 13 giugno 2024, di dati anagrafici e relativi allo stato di salute - nonchè la pubblicazione sul c.d. dark web degli stessi- relativi a pazienti di cui questa Casa di cura è titolare del trattamento.

Soggetti interessati coinvolti dalla violazione

Si tratta approssimativamente di n. 385 interessati, numero che Synlab consiglia di ridurre ulteriormente tenendo conto che uno stesso soggetto interessato potrebbe avere effettuato, nel periodo di riferimento ricompreso tra gennaio 2015 e febbraio 2024, più di un prelievo. Alla data di comunicazione SYNLAB, in particolare, ha rilevato che la violazione riguarda n. 1153 registrazioni contenenti dati personali trattati da SYNLAB in qualità di nostro Responsabile esterno. Il numero approssimativo di interessati sopra riportato è calcolato tenendo in considerazione il rapporto 1/3, in considerazione che per ciascun campione sono prodotte tre registrazioni. L'attacco è stato notificato all'Autorità Garante. Synlab riferisce altresì di aver prontamente messo in sicurezza il sistema isolando e neutralizzando il malware. - allo stato non risulta possibile escludere tentativi di furto d'identità o frode nei confronti degli interessati.

Misure di sicurezza adottate dal responsabile esterno a seguito della violazione

Quanto alle misure adottate dal responsabile esterno a seguito della violazione si precisa come lo stesso abbia confermato di essere tempestivamente intervenuta con iniziative coordinate dal proprio team informatico per addivenire alla messa in sicurezza del sistema, scollegandolo dalla rete internet e spegnendo le macchine ed attivando l'accesso ad internet in modo tale che fosse raggiunta esclusivamente la piattaforma cloud "EDR" onde consentire la gestione, la verifica dell'attacco informatico ed il monitoraggio dell'infrastruttura IT. SYNLAB conferma di aver isolato e neutralizzato il malware, che è ad oggi confinato in due postazioni, utilizzate per le verifiche IT interne. SYNLAB conferma altresì di aver adottato misure volte a garantire la business continuity, nonché una procedura di messa in sicurezza della strumentazione di laboratorio e di servizi polidiagnostici propedeutica al ripristino delle attività. Alla data della comunicazione, Synlab ha confermato l' avvenuto ripristino in sicurezza del sistema di accettazione e download referti nell'ambito del service analisi di laboratorio, su cui è stata completata l'implementazione delle misure per l'autenticazione dei clienti del suddetto service.

MISURE CHE LA CASA DI CURA RACCOMANDA AI PAZIENTI DI ADOTTARE

Si raccomandano tutti i soggetti interessati di provvedere a quanto segue:

• valutare attentamente ogni e-mail, SMS, messaggio o telefonata in cui Vi venissero richiesti codici di accesso o ulteriori dati personali, valutando con attenzione l'attendibilità del richiedente; gli Istituti bancari e, più in generale, i fornitori di servizi, non richiedono mai codici di accesso o password tramite SMS, E-mail o telefonate.

• valutare attentamente e-mail, SMS e di altri fonti di messaggistica contenenti collegamenti ipertestuali (link) o allegati sospetti-inusuali: potrebbero essere usati per indirizzare l'utente verso siti web dannosi o fargli scaricare software malevoli;

• sostituire le password dei propri account (e-mail, Social Network, forum, etc...) e, se il sistema lo permette, attivare l'autenticazione a più fattori. I meccanismi di autenticazione multifattoriale (es. i codici OTP che ricevete dalla banca dopo aver inserito username e password per accedere all'home banking) rafforzano la protezione da accessi indesiderati. I principali fornitori di servizi online offrono questo sistema: per attivarlo è sufficiente entrare nelle impostazioni di sicurezza dell'account.

• Informare i propri amici e familiari di essere stati vittima di questa violazione, suggerendo loro di porre attenzione al rischio di ricevere false richieste che paiono pervenire da Voi.

Si invitano i soggetti interessati di prendere visione delle seguenti pagine informative dell'Autorità Garante per la Protezione dei dati personali:

- ✓ PHISHING https://www.garanteprivacy.it/temi/cybersecurity/phishing
- ✓ VISHING https://www.garanteprivacy.it/temi/cybersecurity/vishing
- ✓ SMISHING https://www.garanteprivacy.it/temi/cybersecurity/phishing
- ✓ SIM SWAPPING
- ✓ https://www.garanteprivacy.it/home/docweb/-/docwebdisplay/docweb/9572143

Si evidenzia come ad oggi la scrivente Casa di cura non sia in grado di conoscere l'identità dei soggetti interessati dalla violazione giacchè detti dati specifici non sono stati forniti da Synlab Italia s.r.l. Si precisa che gli interessati potranno richiedere informazioni scrivendo al Titolare del trattamento - con l'assistenza del rpd dpo@malatestanovello.it - al seguente punto di contatto privacy@malatestanovello.it