Addendum al Contratto del Responsabile IT del Trattamento dei dati in ambito sanitario del Medical Center LDB

Misure di sicurezza

L'art. 5 del Regolamento europeo aggiunge, tra i vari principi da osservare nell'operare un trattamento di dati, il principio di responsabilizzazione (accountability) del titolare del trattamento.

Il principio di responsabilizzazione (accountability) pur non essendo una misura di sicurezza in sé è sempre un principio base intorno al quale deve essere costruita qualsiasi politica di sicurezza dei dati.

Il principio di sicurezza prevede l'obbligo di riservatezza, integrità e disponibilità dei dati.

L'art. 5, par. 1, lett. f), stabilisce che i dati personali devono essere *"trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza)."* E' importante notare che è l'intero trattamento a dover essere sicuro, non solo i dati come prodotto finale. Ciò comporta anche che le valutazioni di sicurezza vanno sviluppate per ogni tipo di trattamento.

L'art. 32, invece, fissa alcuni principi fondamentali. In particolare le misure di sicurezza devono essere approntate tenendo conto dei seguenti criteri:

1. lo stato dell'arte;
2. i costi di attuazione delle misure di sicurezza;
3. la natura, l'oggetto, il contesto e le finalità del trattamento;
4. il rischio di varia probabilità e gravità di compressione o violazione dei diritti e delle libertà delle persone fisiche.

Le misure di sicurezza, quindi, devono essere adeguate, imponendo non un'obbligazione di risultato, bensì un'obbligazione di mezzi, in modo che siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

In tale quadro si richiama ai contenuti della Direttiva NIS[1] che impone obblighi di sicurezza per determinate categorie di servizi.

La sicurezza non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo, a coprire eventi quali la sottrazione o la perdita di documenti.

Le misure di sicurezza, quindi devono garantire che:

- i dati possano essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscono solo nell'ambito dell'autorità che gli viene concessa);
- i dati trattati siano accurati e completi in relazione al motivo per cui lo stai elaborando;

[1] https://protezionedatipersonali.it/direttiva-nis-network-information-security

- i dati rimangano accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

La predisposizione delle misure di sicurezza richiede la conoscenza da parte del **Responsabile IT** e il luogo e i supporti su cui sono custoditi i dati personali, informazione senza le quali è probabile che le misure implementate risultino inadeguate. Tale conoscenza, che può apparire ovvia, non è purtroppo scontata, in particolare modo in organizzazioni complesse, dove può accadere che dispositivi informatici accesi o servizi attivi vengano "dimenticati" per lunghi periodi di tempo, oppure che l'organizzazione dei dispositivi sia realizzata nel tempo stratificandola senza tenere realmente conto di come viene attuata.

Per quanto alle misure di sicurezza giova ricordare la suddivisione in due categorie: misure organizzative e misure tecniche, che, sempre secondo l'art. 32, comprendono, tra le altre:

- misura tecnica: la pseudonimizzazione e la cifratura dei dati personali;
- requisiti di sicurezza :
  a) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  c) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Analisi del rischio

Il regolamento europeo ha un approccio basato sulla valutazione del rischio piuttosto che sulla protezione dell'utente. Per cui occorre una corretta analisi dei rischio del trattamento dei dati personali per poter implementare le misure di sicurezza adeguate. Per ogni rischio occorre individuare la probabilità dell'evento, nonché la gravità dello stesso, in modo da stabilire le misure di sicurezza adeguate per mitigare il rischio. Un esempio classico riguarda la dismissione delle stampanti con memoria, senza aver provveduto a cancellare la memoria, e quindi con l'astratta possibilità che un terzo possa acquisire le immagini ottiche degli ultimi documenti stampati o scansionati.

Codici di condotta e certificazioni

Sempre in base all'art. 32, *"l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo"*.

I codici di condotta sono, quindi, delle misure di garanzia, che vengono sottoposti all'approvazione delle autorità di controllo nazionali, incaricate di vigilare sull'attuazione dei medesimi codici. Ovviamente il **Responsabile IT del Trattamento dei dati**, dovrò tenersi sempre aggiornati sulla disponibilità e l'evoluzione dei codici di condotta.

Analogamente, l'adozione di processi di trattamento certificati può essere utilizzato a dimostrazione del concreto impegno da parte del **Responsabile IT del Trattamento dei dati** nell'attuazione del regolamento.

Sia i codici di condotta che le certificazioni non esimono i Titolari da responsabilità, ma sicuramente possono essere degli elementi di valutazione nel momento in cui si debba stabilire la quantità di responsabilità e quindi il risarcimento del danno (art. 83 lett. J GDPR).

Vulnerabilità e misure di sicurezza

Per scendere nel concreto, con riferimento alle principali vulnerabilità evidenziate nei provvedimenti dei Garanti europei, emergono le seguenti misure di sicurezza.

- Gestione degli accessi

È una misura non di natura esclusivamente informatica, ma in primo luogo di tipo organizzativo.

Una corretta gestione degli accessi permette di limitare l'accesso a determinati dati (tra cui ovviamente anche dati personali) unicamente agli utenti che ne hanno necessità per lo svolgimento delle proprie mansioni lavorative. La gestione degli accessi non distingue tra categorie di persone che accedono ad un dato, e si applica tanto ad utenti interni ad un'organizzazione (come, ad esempio, dipendenti e consulenti) quanto ad utenti esterni (fornitori, clienti o semplici visitatori).

Per quanto attiene ai dati personali di cui è Titolare il Medical Center LDB, questi sono resi disponibili all'esterno con limitazioni alla necessità di conoscere.

- Autenticazione degli utenti

Con riferimento agli utenti interni all'organizzazione, l'autenticazione presuppone che ciascun utente di un sistema sia dotato di un proprio account individuale, specialmente quando tale utente abbia responsabilità aziendali particolari. In tal modo è possibile verificare univocamente l'identità del soggetto, così riconducendo a lui con certezza le azioni compiute all'interno del sistema, facilitando il rispetto del principio di accountability. La connessione fra autenticazione e accountability è stata sottolineata dal Garante italiano, per il quale *"la condivisione delle credenziali impedisce di attribuire le azioni compiute in un sistema informatico a un determinato incaricato, con pregiudizio anche per il titolare, privato della possibilità di controllare l'operato di figure tecniche così rilevanti"* (provvedimento 4/4/2019). In conseguenza "*l'avvenuta condivisione delle credenziali di autenticazione tra più soggetti legittimati alla gestione della piattaforma rappresenta una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate"*. Tale adempimento è, d'altra parte, incluso negli standard di sicurezza pubblicati dalle organizzazioni internazionali più prestigiose, e non richiede alcun costo aggiuntivo.

In caso di accesso dall'esterno, occorre che l'utente sia autenticato in modo corretto. Un'errata o mancata configurazione di un'applicazione permetterebbe a terzi non autorizzati (o peggio ancora al pubblico) di prendere conoscenza di dati riservati. L'accesso di terzi non autorizzati a dati personali contenuti in aree clienti riservate, costituisce secondo il CNIL francese una violazione grave della sicurezza in quanto astrattamente sfruttabile da qualunque persona, anche non esperta in informatica.

I meccanismi di autenticazione possono essere vari: password, smart card, certificati digitali, tecniche biometriche, ecc. Devono comunque essere oggetto di specifiche politiche di generazione, utilizzo, custodia, aggiornamento e distruzione. Ad esempio, occorre impartire precise istruzioni agli autorizzati al trattamento affinché adottino le necessarie cautele per assicurare la segretezza delle loro credenziali e la sicurezza dei dispositivi necessari per l'autenticazione. Ancora, occorre prevedere delle procedure per la sostituzione degli incaricati nel caso di prolungata assenza o impedimento, al fine di assicurare la disponibilità di un particolare trattamento di dati. E così via.

- Autorizzazione degli utenti

L'assegnazione di account individuali o l'autenticazione di un utente costituisce solo una prima misura di sicurezza, che deve essere naturalmente seguita dall'individuazione delle categorie di dati accessibili dagli account rilevanti, e, dunque, dalle autorizzazioni assegnate. La necessità di prevedere autorizzazioni specifiche (quantomeno interne ad un'organizzazione) emerge implicitamente dall'articolo 29 GDPR, ai sensi del quale chi agisce sotto l'autorità del titolare o del responsabile non può trattare dati personali se non è istruito in tal senso. Tale misura di sicurezza consente di restringere l'accesso ai soli dati essenziali per i quali viene effettuato l'accesso, ed è importante quanto l'autenticazione, in quanto quest'ultima sarebbe inutile se tutti gli utenti fossero autorizzati ad accedere a tutti i dati, circostanza che, secondo la CNIL, costituisce una violazione dell'art. 32 del GDPR. In maniera similare, secondo il Garante italiano, la mancata implementazione di sistemi di autorizzazione integra la violazione dell'articolo 5(1)(f) del GDPR.

A livello informatico, l'autorizzazione all'accesso a dati viene di regola impostata sulla base

dell'appartenenza di un utente ad un determinato gruppo, ma altre tecniche possono essere implementate, come ad esempio la restrizione di accesso al di fuori di determinati orari. I profili di autorizzazione devono definire in dettaglio tutte le azioni consentite. Le definizioni dei profili devono essere verificate periodicamente, e comunque almeno una volta l'anno.

- Aggiornamento degli applicativi

L'utilizzo di applicazioni non aggiornate o obsolete costituisce senza ombra di dubbio una violazione delle misure di sicurezza. Alla scoperta di vulnerabilità di una applicazione segue il rilascio di aggiornamenti. Il mancato aggiornamento rende il sistema vulnerabile, non solo perché esiste la vulnerabilità dell'applicativo, ma soprattutto perché tale vulnerabilità diventa di dominio pubblico e quindi sfruttabile da un gran numero di malintenzionati.

Altro pericolo deriva dalle applicazioni obsolete. Al termine del ciclo di vita di una applicazione, questa non viene più aggiornata, e presenta vulnerabilità di vario genere che non vengono più corrette. A meno che non vi siano sviluppatori interni all'azienda in grado di correggere tali vulnerabilità, cosa dispendiosa e complessa, il rischio di compromissione di un sistema IT sarebbe incrementato, perciò, anche l'utilizzo di applicazioni obsolete è idoneo a configurare una violazione dei criteri di sicurezza del trattamento dei dati personali.

Il continuo aggiornamento delle applicazioni costituisce una misura di sicurezza idonea a correggere vulnerabilità di volta in volta rese note al pubblico e corrette dagli sviluppatori. in aggiunta alla regolare installazione di patch e aggiornamenti, può essere opportuno implementare una procedura di tipo organizzativo che permetta di verificare il regolare e corretto svolgimento di tali operazioni.

- Conservazione e condivisione dei dati

Un'altra categoria di vulnerabilità riguarda la conservazione e la condivisione dei dati. Nonostante esista una grandissima varietà di misure di sicurezza implementabili per proteggere i dati, come ad esempio la pseudonimizzazione o la cifratura, che sono espressamente citate dall'articolo 32(1)(a) del GDPR, per motivi pratici o tecnici non sempre è possibile implementarle o garantire il massimo livello di sicurezza possibile. Come ad esempio nel caso della cifratura asimmetrica che richiede una notevole potenza di calcolo che mal si presta all'invio di dati di grande quantità. Non dimentichiamo che la tecnica di protezione dei dati dovrebbe essere adeguata al trattamento dei dati che viene effettuato.

Nell'ambito della sicurezza informatica si suole catalogare i dati a seconda che siano correntemente usati nelle operazioni quotidiane, che siano in trasmissione a terzi, o che siano invece archiviati.

- La protezione dei dati trattati attivamente

I dati trattati attivamente da un'azienda non possano essere né pseudonimizzati né cifrati (essendo necessario utilizzarli), ma devono spesso essere disponibili "in chiaro". In tali casi le misure di sicurezza sono per lo più relative all'accesso ai dati. Per questo motivo la maggior parte delle decisioni delle autorità si focalizzano sulla sicurezza dei dati in trasmissione o archiviazione.

- La protezione dei dati trasmessi a terzi

Il dato che viene trasmesso a terzi può essere intercettato, il dato condiviso può subire una violazione di confidenzialità. Benché ormai la maggior parte delle comunicazioni via Internet avvenga tramite modalità criptate, esistono ancora servizi che non prevedono la cifratura dei dati, come ad esempio il protocollo http, il quale ovviamente "non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato". Pertanto il Garante (provvedimento del 23 gennaio 2020) ha stabilito che "*il mancato utilizzo di strumenti di crittografia per il trasporto dei dati si pone in contrasto con l'articolo 32 del Regolamento"*. Tale argomento si applica, ovviamente, anche alle email. L'utilizzo di protocolli di cifratura, come il protocollo TLS e la cifratura end-to-end delle email in trasmissione costituisce, quindi, una misura di sicurezza adeguata ai sensi dell'articolo 32 del GDPR.

- La protezione dei dati archiviati

Quando un dato, a seguito del trattamento attivo, deve essere conservato, deve essere adeguatamente protetto. La prima misura di sicurezza può essere certamente l'implementazione e il rispetto di una data retention policy, poiché eliminando i dati non più necessari da un sistema è si riduce il rischio di violazioni. Ma anche i dati personali archiviati e non attivamente utilizzati dovrebbero essere cifrati. Ad esempio, secondo l'autorità danese (provvedimento del 10 marzo 2020), l'assenza di cifratura di un hard disk di un computer portatile che contiene dati personali costituisce una vulnerabilità che permette una facile violazione di dati. Tale misura è sempre prescritta (e la sua assenza sanzionata) dalle autorità di controllo per quanto riguarda credenziali e password o dati identificativi. Infine, la protezione dei dati con sistemi di cifratura è richiesta laddove il dato personale, per sua natura, sia particolarmente sensibile.

- Protezione di dati e sistemi

I dati e i sistemi elettronici devono essere protetti da accessi non consentiti. Si impone, quindi, l'utilizzo di software di contrasto ai virus e ai malware informatici, i quali devono essere aggiornati periodicamente. Ovviamente devono essere aggiornati periodicamente anche i sistemi operativi e gli applicativi utilizzati per il trattamento dei dati.

I soggetti autorizzati devono essere formati al fine di minimizzare il rischio di un utilizzo improprio degli strumenti elettronici.

- Procedure di continuità operativa

I dati e i sistemi sono protetti da incidenti o violazione dei dati tramite un sistema di backup dei dati giornaliero, e una conseguente procedura di ripristino degli stessi potenzialmente da effettuarsi in tempo reale rispetto al momento della conoscenza dell'incidente, o comunque nel termine massimo di 12 ore.

- Impostazione dei log dei sistemi

La conservazione e l'analisi dei messaggi di log costituisce una misura di sicurezza essenziale in quanto non solo permette al titolare di essere sempre a conoscenza degli eventi che si verificano nei propri sistemi (ad esempio, accessi o operazioni compiute dagli utenti), ma soprattutto di essere sempre in grado di dimostrare l'adeguatezza delle misure di sicurezza implementate.

Conseguentemente, la registrazione e la conservazione dei log è espressamente richiesta in diversi provvedimenti settoriali emanati dalle autorità di controllo. In assenza di log non è possibile individuare vulnerabilità, né per quanto riguarda il titolare, né per quanto riguarda le autorità di controllo. Inoltre, in assenza di log, non è possibile analizzare ex post le modalità di un attacco e, soprattutto, le conseguenze con riguardo ai dati personali conservati.

- Misure di Auditing

Il Vulnerability Scan è uno strumento imprescindibile per le organizzazioni complesse o per quelle che hanno server accessibili da Internet e che, dunque, espongono dati al pubblico. Secondo l'ICO e il Garante italiano i *Vulnerability Scan* dovrebbero essere effettuati regolarmente, e comunque a seguito di cambiamenti importanti.

I *Penetration Test* consiste nello sfruttamento delle vulnerabilità rilevate aiutando a determinare se le difese del sistema sono sufficienti o se invece sono presenti altre vulnerabilità elencando in questo caso quali difese il test ha sconfitto. Il test ha dunque come obiettivo quello di evidenziare le debolezze della piattaforma fornendo il maggior numero di informazioni sulle vulnerabilità che ne hanno permesso l'accesso non autorizzato, fornendo una stima chiara sulle capacità di difesa e del livello di penetrazione raggiunto nei confronti, delle vulnerabilità interne al sistema, delle vulnerabilità esterne al sistema, della sicurezza fisica.

Roma, 1 febbraio 2022

Il Data Protection Officer
Dr. Alessandro Pirrone