INSURANCE Daily

LUNEDÌ 01 APRILE 2019 N. 1520

PRIMO PIANO

L'Rc auto sempre più tassata

Il premio medio Rc auto effettivamente pagato per i contratti stipulati o rinnovati nel quarto trimestre 2018 è pari a 415 euro. È ciò che rivela l'ultimo bollettino statistico Iper pubblicato dall'Ivass, da cui emerge anche che il 50% degli assicurati paga meno di 372 euro e il 10% meno di 235 euro. Nel corso dello scorso anno, spiega l'Ivass, è proseguito il trend di stabilizzazione dei prezzi: la variazione del prezzo medio su base annua è lievemente negativa (–0,5%).

I 415 euro del premio medio pagato si suddividono in 52 euro di imposte, 34 di contributo al Servizio sanitario nazionale e 329 di premio netto. L'imposta sull'Rc auto è costituita da un'aliquota compresa tra il 9 e il 16% sul premio imponibile, fissata ogni anno dalle province. Il contributo al Ssn è pari al 10,5% sul premio imponibile.

"L'effetto combinato della diminuzione del premio e dell'aumento delle aliquote – si legge nel bollettino – ha comportato negli anni un aumento dell'incidenza della fiscalità sul premio pagato. A partire dal 2011 si registra, infatti, a livello provinciale un progressivo spostamento dall'aliquota intermedia (12,5%) verso l'aliquota massima (16%).

Per leggere la news completa, clicca qui.

Beniamino Musto

RISK MANAGEMENT

Gdpr, il primo ospedale multato è portoghese

La multa di 400mila euro comminata dall'Authority locale, la Comissão Nacional de Protecção de Dados (CNPD), ha colpito il Barreiro Montijo, una struttura ospedaliera vicino a Lisbona, per non essere stato in grado di proteggere l'accesso ai dati dei pazienti contenuti nel suo archivio digitale

Che il sistema sanitario sia tra i primi obbiettivi degli hackers è cosa nota.

Nel corso degli ultimi anni è salito vertiginosamente il numero degli assalti ai danni di strutture e operatori sanitari, ed è tristemente famoso il caso dell'attacco *ransomware* che nel maggio del 2017 ha bloccato per alcuni giorni l'**Nhs**, il sistema sanitario britannico.

In quel caso, nel giro di poche decine di minuti, la quasi totalità dei computer degli ospedali presenti nell'arcipelago britannico subì un arresto della rete informatica, che rese inutilizzabili anche le linee telefoniche. Per evitare il caos, l'Nhs dovette invitare i cittadini a non recarsi negli ospedali e nei pronto soccorso, se non per casi di emergenza grave, e molte direzioni sanitarie dovettero rinviare le operazioni di routine per accordare la precedenza alle situazioni più difficili.


© monkeybusinessimages – iStock

Si sarebbe trattato allora di una variante del virus *cryptolocker Wanna*, lo stesso che aveva appena messo fuori uso le reti di **Telefonica** in Spagna e attaccato altre istituzioni in Russia, Ucraina e anche nel nostro Paese. Pare anche che gli hackers avessero chiesto un riscatto, ma non è mai stata nota l'entità della richiesta né se sia stata accolta.

In questo caso, però, è interessante notare come le motivazioni del garante portoghese siano particolarmente aderenti allo spirito del *Gdpr*, dal momento che riguardano un'infrazione di tipo organizzativo.

CONTROLLI INSUFFICIENTI E MANCANZA DI PROTEZIONE DEI DATI

Su segnalazione del personale medico dell'ospedale, che ha notato una serie di accessi non autorizzati ai dati dei pazienti da parte di altri dipendenti non sanitari, lo scorso aprile sono infatti partite le prime indagini su eventuali falle del sistema informatico.

Il **Cnpd** ha quindi condotto un audit interno all'ospedale, verificando che ben 985 impiegati avevano accesso ai dati sensibili (incluse le informazioni sanitarie) dei pazienti, a fronte di un personale medico di appena 296 unità.

Com'è noto, perché vengano rispettate le disposizioni del Gdpr, soltanto il personale medico può accedere ai dati sensibili concernenti la salute dei pazienti, mentre in questa struttura il personale amministrativo di ogni livello poteva leggerne la gran parte, inclusi quelli confidenziali.

Pertanto, nello scorso dicembre, non avendo garantito controlli adeguati alla protezione delle informazioni sanitarie trattate, l'ospedale portoghese ha subìto una multa di 400mila euro. Una cifra cospicua, ma poteva andare anche peggio, dal momento che la massima sanzione prevista dal Gdpr ammonta a 20 milioni di euro o al 4% del giro d'affari globale.

(continua a pag. 2)

INSURANCE Daily
LUNEDÌ 01 APRILE 2019 N. 1520

(continua da pag. 1)

POLITICHE DI RISK MANAGEMENT ADEGUATE

Nelle strutture sanitarie vengono trattate molte categorie di dati, spesso gestite da più di un sistema informatico: dalla prenotazione, accettazione e dimissione del paziente, alla produzione di esami di laboratorio e diagnostica di ogni genere, all'erogazione di cure e prestazioni varie, fino all'effettiva gestione amministrativa dei servizi erogati.

Essendo spesso installati in tempi diversi, raramente questi sistemi sono integrati fra loro, tuttavia gli utenti collegati possono avere la necessità di accedervi, per consultarli a vario titolo.

Il rispetto della normativa corrente sulla privacy impone ora una grande attenzione nella gestione di queste informazioni e ogni struttura ha l'obbligo di tenere costantemente sotto controllo le modalità di accesso ai dati da parte di tutto il personale, indipendentemente dalla mansione e dal ruolo di ciascuno.

Soprattutto, è necessario rendere conto per iscritto delle procedure adottate, il che richiede un certo sforzo organizzativo e l'adozione di strumenti tecnologici in grado di garantire una protezione efficace, abbandonando il concetto comune in base al quale la sicurezza dei dati ostacolerebbe l'efficienza nella loro gestione.

Le misure organizzative in grado di supportare questi processi sono varie, dal controllo degli accessi ai locali ove sono conservati i documenti cartacei, all'obbligo di registrarsi per accedere alla consultazione degli archivi informatizzati, fino al tracciamento di tutte le operazioni effettuate su di essi, tramite identificazione edautenticazione degli utenti.

Ogni accesso dovrebbe essere autorizzato e dovrebbero essere presenti vari livelli di autorizzazione, in base alle mansioni effettivamente svolte.

Spesso non si tratta di strumenti o procedure costosi, ma è necessario del tempo per elaborarli e servono un'analisi e una conoscenza approfondita di ogni processo che impatti strutture altamente complesse come quelle cliniche.

La corretta gestione delle informazioni, insomma, non costituisce un problema insolubile, ma per essa occorre uno sforzo organizzativo tale da non consentire alibi o tentennamenti. Nel caso trattato, gran parte del personale dell'ospedale sanzionato accedeva ai dati personali e sensibili dei pazienti, pur non essendovi autorizzato, presumibilmente per l'assenza di una politica di risk management adeguata al tipo di rischio corso.

Veniva infatti constatata la mancanza di documenti o procedure nei quali fossero definiti i criteri per stabilire la corrispondenza tra le competenze funzionali degli utenti e i relativi profili di accesso, dal momento che nel corso dell'ispezione risultavano quasi 1.000 utenti ai quali era associato il profilo di accesso riservato ai medici, a fronte di soli 296 medici in servizio.

Il Garante ha quindi contestato la violazione del principio di minimizzazione (accesso indiscriminato ai dati personali dei pazienti, anche da parte di soggetti che non ne avrebbero avuto alcuna necessità per svolgere i propri compiti professionali), la violazione dei principi di integrità e riservatezza (mancata adozione di misure tecniche e organizzative per impedire l'accesso indiscriminato ai dati) e la mancata adozione da parte del titolare del trattamento di misure tecniche e organizzative adeguate al rischio e di procedure idonee a garantire un monitoraggio costante del sistema di trattamento dei dati.

Cinzia Altomare

INSURANCE Daily
LUNEDÌ 01 APRILE 2019 N. 1520

MARKETING

Mifid 2: come consolidare la relazione col cliente

La direttiva sulla trasparenza può essere l'occasione di modificare alcuni aspetti del rapporto con l'assicurato e, sul lungo periodo, anche del modello di servizio

La direttiva **Mifid 2** richiede una maggiore trasparenza in tutte le fasi della relazione con il cliente, evidenziando i costi sia degli strumenti finanziari, sia dei servizi forniti. Nel settore assicurativo, possiamo notare come le modalità di rappresentazione dei costi siano influenzabili da diversi fattori.

Un primo punto rilevante è rappresentato dall'orizzonte temporale su cui viene analizzato il portafoglio, dove l'estensione del periodo di valutazione permette di normalizzare la pressione dei costi. Un secondo aspetto riguarda l'eventuale presenza di operazioni effettuate sulla polizza e il timing del loro avvenimento, che possono influenzare significativamente i costi nell'anno. Inoltre, sono da considerare anche le differenze tra prodotti appartenenti alla stessa macro-famiglia, ad esempio fra polizze di ramo I e ramo III. Infine, è necessario mantenere i dati costantemente aggiornati con un elevato grado di dettaglio per avere una rappresentazione dei costi del prodotto veritiera e corretta.

Revisione del modello di servizio

Come agire in tale contesto? Sconsigliamo di definire un format univoco di rendicontazione per tutti gli strumenti finanziari. Noi proponiamo una strategia bifocale: da un lato sul breve/medio periodo, dall'altro sul lungo. Quella nel breve/medio si articola in due fasi: la prima, programmare l'invio delle comunicazioni con il parziale recupero dei mercati nel 1Q 2019. La seconda fase prevede di formare la rete delle agenzie sulle logiche del dato (per saper spiegare ai clienti i razionali che sottendono ai dati rappresentati nei rendiconti), sugli elementi distintivi dei prodotti (natura, obiettivi e orizzonte temporale dei prodotti, ulteriori elementi di valore aggiunto, etc.) e infine sulla commercializzazione della consulenza (essere in grado di valorizzare il proprio supporto, soprattutto in termini di gestione di un contesto di mercato sfidante).


© Jano jrk – Fotolia


© LuminaStock – iStock

Nel più lungo termine suggeriamo invece di lavorare sull'evoluzione del modello di servizio, focalizzando l'attenzione degli interventi su due punti: in primo luogo, la definizione di un nuovo approccio commerciale ed eventualmente di nuove logiche di pricing, in modo da ottenere un migliore equilibrio tra i costi di servizio del cliente e i ricavi; secondariamente, l'evoluzione della retribuzione della rete: una maggiore trasparenza dei costi significherà anche la presa di coscienza da parte dell'agenzia dell'effettivo costo sostenuto dal cliente. Potrebbe quindi essere il momento giusto per realizzare un ripensamento complessivo del modello di retribuzione della rete agenziale sui prodotti e servizi oggetto di Mifid 2.

Maurizio Primanni,
ceo Excellence Consulting

INSURANCE Daily

LUNEDÌ 01 APRILE 2019 N. 1520

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 01 aprile di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577