STRUMENTI INFORMATICI PER I MEDICI: QUALI RISCHI?

Moderatori: Vincenzo Toscano (RM) - Agostino Paoletta (PD)

Cybersicurezza e dati sensibili

(Nunzia Ciardi, RM - Marco Valerio Cervellini RM)

Sicurezza informatica e privacy: la nuova normativa europea

(Giuseppe Bernieri, PD)

Nuove tecnologie e professione medica:aspetti medico-legali

(Mariagiovanna Savio, PD)

Take home messages

(Agostino Paoletta, PD)

Jiménez Aranda, Luis

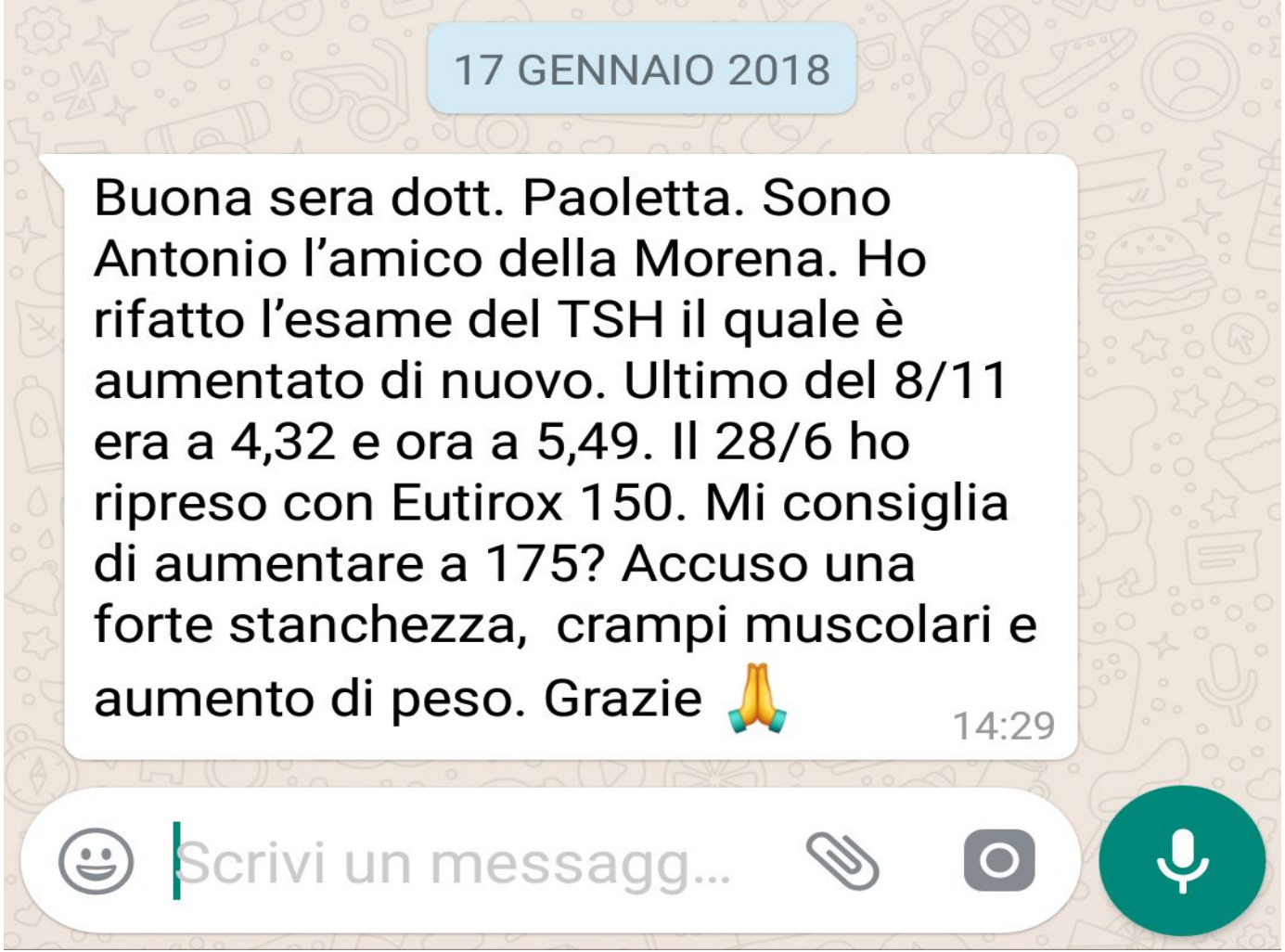
- Nuovo modo di esercitare la professione per lo specialista (legato alle nuove tecnologie)
- Non cambia la professione ed il suo contenuto, cambia il modo in cui essa viene esercitata
- Nuovi strumenti di organizzazione interna (PC, Server, Fascicolo Sanitario, Firma digitale, Strumenti di diagnosi che raccolgono dati personali)
- Nuovi strumenti di relazione con i pazienti (e-mail, PEC, Firma digitale, WhatsApp, SMS, Blog, Siti Internet)

Daniela

17/1/2018 20:30

Salve Dottore, Le scrivo utilizzando questo contatto trovato tramite internet.
Mia figlia, 20 anni, ha effettuato venerdì scorso l'ecografia alla tiroide;
il medico di base mi ha quindi prescritto l'agoaspirato che effettuerebbe il 5 febbraio.
Domani il medico di base mi darà inoltre l'impegnativa per prenotare la visita endocrinologica che, a suo parere, potrebbe essere fatta dopo la consegna del referto dell'agoaspirato, cioè a fine febbraio.
Essendo mia intenzione rivolgermi a Lei, Le chiedo intanto indicazioni/consulenza anche in sede privata; mia figlia è però in questo momento a Parigi e potrei farLe esaminare la documentazione o inviargliela via mail (Eco, esami del sangue).
Mia figlia sarebbe qui il 4 e 5 febbraio appunto per fare l'agoaspirato.
Ho bisogno di capire cosa è meglio fare prima e cosa dopo: se cioè va bene agoaspirato prima della visita specialistica oppure dopo (in questo caso lo sposterei più avanti). Se vuole ci sentiamo al telefono per definire; nel caso fosse opportuna prima la visita e poi agoaspirato, potremmo concordare la visita appunto il 5 febbraio se possibile, perchè poi mia figlia dovrebbe rientrare a Parigi.

Grazie per l'attenzione


17 GENNAIO 2018
Buona sera dott. Paoletta. Sono Antonio l'amico della Morena. Ho rifatto l'esame del TSH il quale è aumentato di nuovo. Ultimo del 8/11 era a 4,32 e ora a 5,49. Il 28/6 ho ripreso con Eutirox 150. Mi consiglia di aumentare a 175? Accuso una forte stanchezza, crampi muscolari e aumento di peso. Grazie 🙏
14:29
Scrivi un messagg...

9/10/2018

I messaggi che invii in questa chat e le chiamate sono protetti con la crittografia end-to-end.

Dottore buonasera , ci conosciamo perché ha seguito mio marito per mac
adenoma ipofisi che ha fatto operare a Treviso da dott
Questa volta la contatto perché da una settimana avevo un dolore esterno alla gola che si è poi gonfiata domenica sera , ieri sono stata dal medico il quale mi ha prescritto gli esami X tiroide che ho fatto sta mattina , ora sono stata con referti da medico di base il quale dice che ho un Ipertiroidismo e mi prescrive ecografia e visita da endocrinologo.
Le allego copia esami , quando mi può ricevere e dove ? Sono di Padova

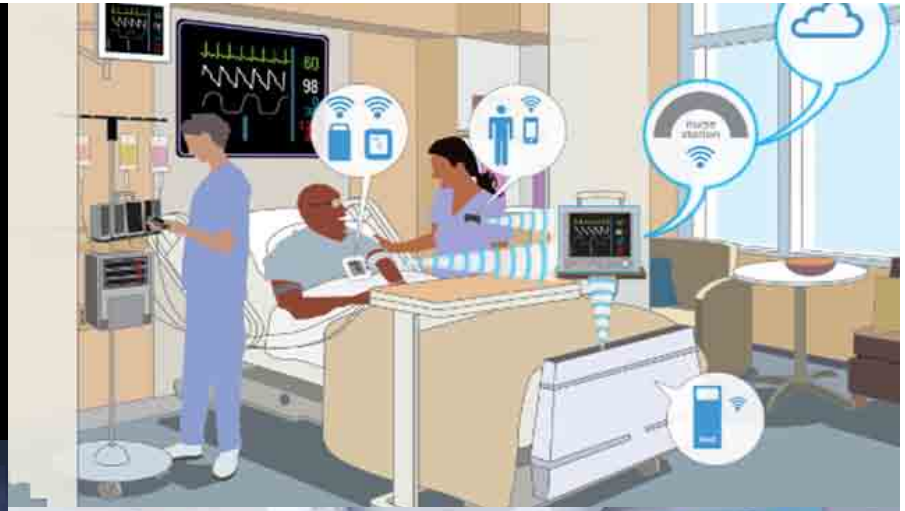
18:46

PDF 2018-10-09 REFERTI E...

2 pagine · PDF · 128 kB 18:48

RISCHI CONNESSI ALL'UTILIZZO DELLE NUOVE TECNOLOGIE NELLA PROFESSIONE SANITARIA

SICUREZZA INFORMATICA



Aspetti legali dell'uso delle nuove tecnologie nella professione medica

LEGGE PRIVACY

COME DIFENDERCI?

Roma, 8-11 novembre 2018

ITALIAN CHAPTER

CYBERSICUREZZA E DATI SENSIBILI

MARCO VALERIO CERVELLINI

Responsabile delle Relazioni Esterne e Comunicazioni
Servizio Polizia Postale e delle Comunicazioni

CYBERSICUREZZA E DATI SENSIBILI

PREMESSA

Negli ultimi anni la **minaccia cyber** ha raggiunto, in termini assoluti, **livelli di guardia mai sperimentati in passato**.

Lo **strumento informatico** è da un lato una **opportunità irrinunciabile** per piccole aziende, grandi imprese, pubbliche amministrazioni e cittadini a livello comunicativo ed economico.

Di contro la criminalità, comune ed organizzata, può oggi giovarsi, anche grazie alle tecniche di anonimizzazione della navigazione e dei pagamenti, di un accesso agevolato a strumenti e servizi criminali in rete, spesso distribuiti nelle pieghe del cosiddetto ***darkweb***.

CYBERSICUREZZA E DATI SENSIBILI

PREMESSA

La larga diffusione dei sistemi informatici **stimola sempre più la criminalità** che, con un salto generazionale, si è **premunita di risorse e tecniche informatiche** per il raggiungimento dei propri
scopi illeciti.

CYBERSICUREZZA E DATI SENSIBILI

PREMESSA

A rischio si trovano tutte le realtà che sfruttano lo strumento informatico, in particolare **l'anello debole** è costituito spesso da chi **non investe adeguate risorse in sicurezza informatica** (spesso piccole e medie imprese nonché ad esempio singoli utenti destinatari dei servizi)

CYBERSICUREZZA E DATI SENSIBILI

PREMESSA

Infatti, molti degli **attacchi più devastanti per le grandi imprese e P.A.** partono spesso da **piccole realtà connesse ad esse, con livelli di sicurezza inferiori** ma con accessi privilegiati ai servizi erogati, elevando esponenzialmente i livelli di rischio connessi.

GRANDI IMPRESE P.A.

PICCOLE / MEDIE IMPRESE

CYBERSICUREZZA E DATI SENSIBILI

ATTACCHI INFORMATICI

Le strategie CRIMINALI vincenti … rimangono le più banali !

non a caso, a livello globale, la somma delle **tecniche di attacco più banali** (SQLi, DDoS, phishing, semplici «malware») rappresenta il **56%** del totale. (fonte Rapporto CLUSIT 2018)

Il dato è allarmante !

poiché evidenzia la **facilità di azione dei cyber criminali** con **strumenti esigui e a basso costo**.

CYBERSICUREZZA E DATI SENSIBILI

DATI STATISTICI

Osservando i dati statistici di raffronto tra il 2016 ed il 2017 relativi all'incremento degli **attacchi gravi ai danni delle diverse categorie di settore,** si evince che la categoria **«Healthcare» è risultata una tra le più esposte.**

+ 9%

(fonte Rapporto CLUSIT 2018)

CYBERSICUREZZA E DATI SENSIBILI

PROBLEMATICHE DI CYBERSICUREZZA

CYBERSICUREZZA NAZIONALE

SICUREZZA NAZIONALE

Un **attacco cyber** alle reti informatiche che gestiscono i servizi sanitari, la distribuzione elettrica o i trasporti **genera problematiche del tutto simili** a quelle generate da un **attacco di tipo "fisico"** alle stesse infrastrutture.

CYBERSICUREZZA E DATI SENSIBILI

RISCHI PER LE SINGOLE REALTA'

Anche le **singole realtà**, come ad esempio un **piccolo studio medico**, sono soggette a **elevati rischi**, essenzialmente connessi ai dati memorizzati / trattati attraverso l'uso di sistemi informatici (personal computer, smartphone, ecc.)

CYBERSICUREZZA E DATI SENSIBILI

TIPOLOGIE POSSIBILI DI ATTACCO

- Phishing - Ransomware - Criptovalute
- Phishing - Spyware
- Man in the middle («B.E.C.» e «Ceo Frauds»)
- Ddos
- Apt

CYBERSICUREZZA E DATI SENSIBILI

TIPOLOGIE POSSIBILI DI ATTACCO

PHISHING

Tecnica che induce la vittima, mediante una falsa comunicazione di posta elettronica, a collegarsi verso un sito simile all'originale (ad esempio il sito di una banca), o a cliccare su allegati malevoli, per realizzare fini illeciti (furto credenziali di accesso, installazione di malware , ecc.)

RANSOMWARE

È una tipologia specifica di malware che cifra i dati informatici contenuti all'interno del sistema attaccato, impedendone l'accesso.
Segue la richiesta di un riscatto in denaro (spesso in criptovalute) per la decriptazione.

CRIPTOVALUTE

Sistema di valute «virtuali» libere ed anonime, utilizzate come mezzo di pagamento spesso anche dai cyber criminali.

CYBERSICUREZZA E DATI SENSIBILI

FOCUS : RANSOMWARE WANNACRY

WannaCry, chiamato anche **WanaCrypt0r**, è un virus informatico, responsabile di un'epidemia su larga scala avvenuta nel maggio 2017, colpendo i sistemi informatici di aziende e organizzazioni in tutto il mondo, **tra cui strutture sanitarie** ed università.

In esecuzione cripta i file presenti sul computer e chiede un riscatto, da pagare in bitcoin, di alcune centinaia di dollari per decriptarli. Dopo l'installazione infetta altri sistemi presenti sulla stessa rete e quelli vulnerabili esposti a internet, senza alcun intervento dell'utente.

CYBERSICUREZZA E DATI SENSIBILI

TIPOLOGIE POSSIBILI DI ATTACCO

PHISHING

Tecnica che induce la vittima, mediante una falsa comunicazione di posta elettronica, a collegarsi verso un sito simile all'originale (ad esempio il sito di una banca), o a cliccare su allegati malevoli, per realizzare fini illeciti (furto credenziali di accesso, installazione di malware , ecc.)

SPYWARE

È una tipologia specifica di malware che raccoglie informazioni sensibili sulle attività della vittima trasmettendole all'attaccante che a sua volta le utilizza per scopi illeciti.

CYBERSICUREZZA E DATI SENSIBILI

TIPOLOGIE POSSIBILI DI ATTACCO

MAN IN THE MIDDLE

Attacco informatico realizzato a seguito della compromissione di caselle di posta o utilizzando tecniche di social engineering, in cui l'attaccante, all'interno di una corrispondenza elettronica di carattere commerciale, assume l'identità digitale di una delle due parti, richiedendo pagamenti su conti correnti appositamente creati, spesso allocati all'estero.

B.E.C
(BUSINESS EMAIL COMPROMISE)

L'attaccante si frappone nel rapporto commerciale in essere tra due soggetti (ad esempio, nel rapporto cliente/fornitore), utilizzando caselle di posta elettronica del tutto simili a quelle in uso alla persona sostituita (dalle quale si differenziano per sottilissimi particolari), ovvero del tutto coincidenti con esse

CEO FRAUD

L'attaccante si sostituisce all'amministratore delegato (od altro top-level manager) dell'azienda, sfruttando la posizione di vantaggio ricoperta dalla persona sostituita all'interno della gerarchia aziendale. La vittima è prescelta tra soggetti ad essa sottoposti.

CYBERSICUREZZA E DATI SENSIBILI

TIPOLOGIE POSSIBILI DI ATTACCO

DOS
(DENIAL OF SERVICE)

Tipologia di attacco volta a rendere inaccessibile un determinato tipo di servizio fornito da un sistema informatico. L'attacco può essere realizzato o tramite la generazione di un numero di richieste superiore al massimo gestibile dal sistema o tramite la generazione di volumi di traffico superiori alla banda disponibile, causandone la saturazione.
Quando questa tipologia di attacco viene utilizzata da più elaboratori contemporaneamente essa prende il nome di DDOS *(Distributed Denial of Service)*

APT
(ADVANCED PERSISTENT TREATH)

Un tipo di attacco persistente e mirato, che permette di accedere al sistema informatico colpito. Si configura tipicamente attraverso l'invio una serie di e-mail di phishing e/o l'utilizzo di malware appositamente strutturati, con lo scopo di studiare la struttura dell'intera rete ed avere accesso a determinati computer con i relativi dati. La persistenza dell'attacco è garantita solitamente dall'apertura di una o più backdoor.

LA POLIZIA POSTALE E DELLE COMUNICAZIONI

La **Polizia Postale e delle Comunicazioni**, reparto specialistico della Polizia di Stato, opera in prima linea nella **prevenzione e nel contrasto della criminalità informatica**, a garanzia dei valori costituzionali della segretezza della corrispondenza e della **libertà di ogni forma di comunicazione.**

Il Servizio Centrale, vertice della struttura, é punto di riferimento nel coordinamento, nella programmazione e nella pianificazione operativa degli uffici periferici della specialità.

L'attività di prevenzione e contrasto viene supportata da un sistematico coinvolgimento degli organismi di cooperazione internazionale giudiziaria e di polizia attraverso la condivisione di strategie di monitoraggio e contrasto dei fenomeni concernenti il cybercrime.

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
DIRETTIVA SUI COMPARTI DI SPECIALITA' – 15 AGOSTO 2017

Competenza esclusiva della Specialità nei cinque settori:

- Attacchi cyber e protezione delle infrastrutture critiche
- Pedopornografia online
- Cyberterrorismo
- Hacking e Financial Cybercrime
- Reati postali

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
CENTRI DI ECCELLENZA

SERVIZIO CENTRALE

C N A I P I C
CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DI INFRASTRUTTURE CRITICHE

C N C P O
CENTRO NAZIONALE PER IL CONTRASTO DELLA PEDOPORNOGRAFIA ONLINE

Commissariato di PS on line

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
C.N.A.I.P.I.C.

Istituito con l'art. 7-bis , comma 1 del DPR 144/2005 il **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – C.N.A.I.P.I.C.**, incardinato nell'ambito del Servizio Polizia Postale e delle Comunicazioni, è **in via esclusiva** incaricato della **prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica**, che hanno per obiettivo le **infrastrutture informatizzate di natura critica e di rilevanza nazionale**.

CYBERSICUREZZA E DATI SENSIBILI

Roma, 8-11 novembre 2018

ITALIAN CHAPTER

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
C.N.A.I.P.I.C.

PREVENZIONE E CONTRASTO DELLA MINACCIA INFORMATICA DI MATRICE TERRORISTICA O CRIMINALE CHE HA PER OBIETTIVO LE INFRASTRUTTURE CRITICHE INFORMATIZZATE

SALA OPERATIVA	INTELLIGENCE	ANALISI	INVESTIGAZIONE	UNITA' TECNICA
PUNTO DI CONTATTO UNIVOCO DISPONIBILE 24 ORE SU 24 7 GIORNI SU 7 DEDICATO ALL'INTERSCAMBIO INFORMATIVO CON LE I.C.	• RACCOLTA INFORMAZIONI • PREVENZIONE • CONDIVISIONE INFORMATIVA CON ALTRI ORGANI DI POLIZIA, ENTI E AZIENDE CONVENZIONATE	• ANALISI DELLE INFORMAZIONI IN CHIAVE COMPARATIVA • PREDISPOSIZIONE DI RAPPORTI PREVISIONALI • SU MINACCIA, VULNERABILITA' E TECNICHE E INIZIATIVE CRIMINALI	RISPOSTA OPERATIVA AL VERIFICARSI DI UN EVENTO CRIMINALE IN DANNO DELLE I.C.	• GESTIONE DELL'INFRASTUTTURA DEL C.N.A.I.P.I.C. • GESTIONE DELLE RISORSE STRUMENTALI • PIANIFICAZIONE FORMAZIONE DEL PERSONALE

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
C.N.A.I.P.I.C.

I servizi di protezione informatica sono erogati sulla base di **apposite convenzioni**, previste dalla stessa legge istitutiva, stipulate **tra il Dipartimento della Pubblica Sicurezza e le singole infrastrutture critiche**, con le quali si realizza in tale particolare settore **un rapporto di partnership pubblico-privato**. Tale attività è stata recentemente incrementata, con il contributo degli Uffici territoriali di Specialità, fornendo assistenza a favore delle Aziende riconosciute sensibili, per la natura del servizio fornito sul territorio nazionale

CYBERSICUREZZA E DATI SENSIBILI

Roma, 8-11 novembre 2018

ITALIAN CHAPTER

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
C.N.A.I.P.I.C. CONVENZIONI

CNAIPIC

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
C.N.A.I.P.I.C.

ATTIVITA' ANNO 2016		ATTIVITA' ANNO 2017	
844	ATTACCHI RILEVATI	ATTACCHI RILEVATI	1032
6721	ALERT DIRAMATI	ALERT DIRAMATI	31524
70	FILONI DI INDAGINE AVVIATI	FILONI DI INDAGINE AVVIATI	72
85	RICHIESTE DI COOPERAZIONE HIGH TECH CRIME NETWORK	RICHIESTE DI COOPERAZIONE HIGH TECH CRIME NETWORK	83

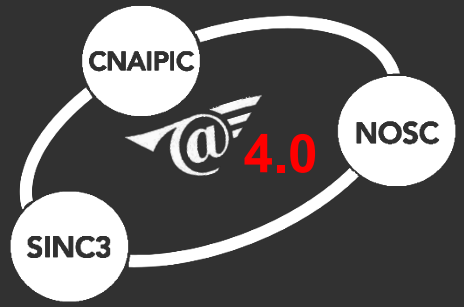
CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
D.L. 18 MAGGIO 2018 N.65

Nel mese di maggio il Consiglio dei Ministri ha approvato il citato Decreto Legislativo per attuare in Italia la Direttiva NIS. **I settori che rientrano nell'ambito di applicazione del decreto attuativo sono quelli già espressamente previsti dalla Direttiva** (ossia energia, trasporti, banche, mercati finanziari, **sanità**, fornitura e distribuzione di acqua potabile e infrastrutture digitali; nonché motori di ricerca, servizi cloud e piattaforme di commercio elettronico).

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
L'INIZIATIVA SINC3



Realizzare un Sistema Nazionale Anticrimine Informatico (valorizzazione dell'esperienza CNAIPIC)

- **Partenariato pubblico-privato**
- **Costruire un modello di diagnosi e prevenzione delle minacce cyber esteso alle PMI (Piccole e Medie Imprese) ed alle PAL (Pubbliche Amministrazioni Locali)**
- **Veicolare in tempo reale preziose informazioni di sicurezza (prevenzione)**
- **Formare squadre per il pronto intervento presso le realtà colpite da attacchi cyber (contrasto – attività di PG)**

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
COMMISSARIATO DI P.S. ONLINE

Commissariato di P.S. online
Sportello per la sicurezza degli utenti del web

Prima esperienza in Europa, il portale del **Commissariato di P.S. on-line** (www.commissariatodips.it), inserito all'interno del Servizio della Polizia Postale e delle Comunicazioni, è nato con lo scopo di **rendere sempre più fruibile e semplice la possibilità per il cittadino di interagire con la Polizia**, senza la necessità di uscire di casa. Con i suoi innovativi sistemi di interattività con l'utente della Rete, attraverso apposite "finestre dialogo", e direttamente collegato con il mondo dei social network, vede, tra i suoi interlocutori privilegiati i più giovani, nonché utenti che versano in condizioni di emarginazione e vulnerabilità.

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
C.N.C.P.O.

Il **Centro Nazionale per il Contrasto alla Pedopornografia On line** (C.N.C.P.O), istituito con la legge 6 febbraio 2006 n. 38 nell'ambito del Servizio Polizia Postale e delle Comunicazioni, **svolge attività di coordinamento nell'ambito del contrasto e della prevenzione della pedopornografia in Rete** e delle connesse forme di devianza e di rischio per i minorenni.

CYBERSICUREZZA E DATI SENSIBILI

LA POLIZIA POSTALE E DELLE COMUNICAZIONI
PIATTAFORMA OF2CEN

OF2CEN
ONLINE FRAUDS CYBER CENTRE AND EXPERT NETWORK

La piattaforma «OF2CEN» è una risorsa condivisa con le banche che raccoglie, attraverso connessioni cifrate, le segnalazioni degli utenti vittime di frodi informatiche creando una black list di tutti i rapporti bancari utilizzati per perfezionare le frodi e utili sotto il profilo investigativo

- Promozione e cura dell'attività info-investigativa tra i vari Compartimenti, al fine di coordinare le indagini tra i vari uffici periferici, evitando inutili duplicazioni e sovrapposizioni delle attività
- Studio dei nuovi sistemi di pagamento (e-payment, mobile payment) e delle cd. cryptovalute

CYBERSICUREZZA E DATI SENSIBILI

MARCO VALERIO CERVELLINI

Responsabile delle Relazioni Esterne e Comunicazioni
Servizio Polizia Postale e delle Comunicazioni

Aspetti legali dell'uso delle nuove tecnologie nella professione medica

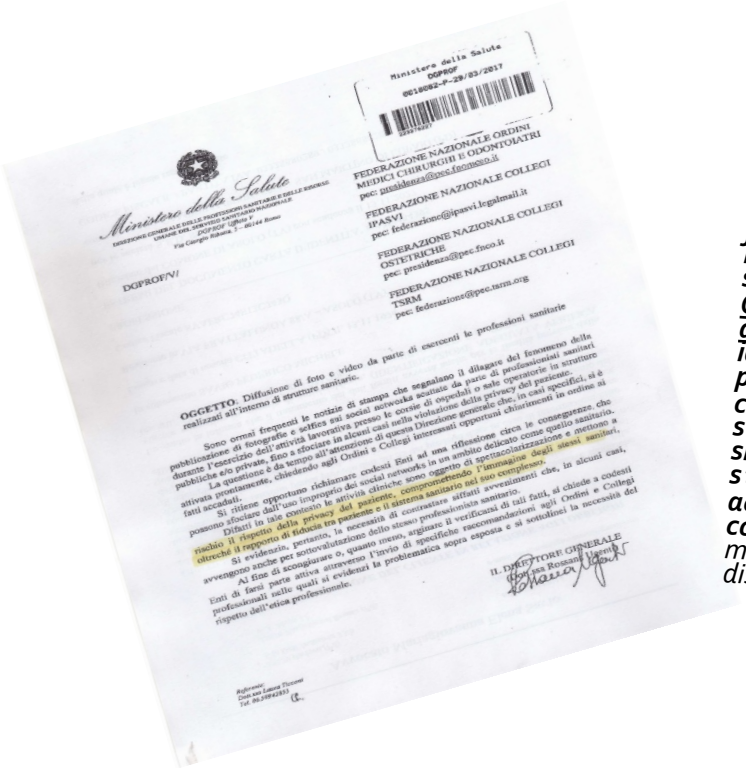
avv. Mariagiovanna Savio
Impresa, privacy e nuove tecnologie

@ info@mariagiovannasavio.it
3479440014
Padova V.le dell'Industria 23/b
www.mariagiovannasavio.it

NON C'E' DISTINZIONE TRA VITA PRIVATA E VITA PROFESSIONALE

- Codice di Deontologia
- Giuramento Professionale
- Nota del Ministero della Salute
- Ordine dei Medici di Milano

Aspetti legali dell'uso delle nuove tecnologie nella professione medica



Ministero della Salute

DGPROF

0018082-P-29/03/2017

FEDERAZIONE NAZIONALE ORDINI MEDICI CHIRURGHI E ODONTOIATRI
pec: presidenza@pec.fnomceo.it

FEDERAZIONE NAZIONALE COLLEGI IPASVI
pec: federazione@ipasvi.legalmail.it

FEDERAZIONE NAZIONALE COLLEGI OSTETRICHE
pec: presidenza@pec.fnco.it

FEDERAZIONE NAZIONALE COLLEGI TSRM
pec: federazione@pec.tsrm.org

DGPROF/VI

OGGETTO. Diffusione di foto e video da parte di esercenti le professioni sanitarie realizzati all'interno di strutture sanitarie.

Sono ormai frequenti le notizie di stampa che segnalano il dilagare del fenomeno della pubblicazione di fotografie e selfies nei social networks scattate da parte di professionisti sanitari durante l'esercizio dell'attività lavorativa presso le cosiddette strutture di ospitalità o sale operatorie in strutture pubbliche e/o private, fino a sfociare in alcuni casi nella violazione della privacy dei pazienti.

La questione è da tempo all'attenzione di questa Direzione generale che, in casi specifici, si è attivata prontamente, chiedendo agli Ordini e Collegi interessati opportuni chiarimenti in ordine ai fatti accaduti.

Si ritiene opportuno richiamare codesti Enti ad una riflessione circa le conseguenze che possono sfociare dall'uso improprio dei social networks in un ambito delicato come quello sanitario, oltreché il rispetto della privacy del paziente, componente di spettacolarizzazione e mettono a rischio il rapporto di fiducia tra paziente e il sistema sanitario nel suo complesso.

Difatti in tale contesto le attività cliniche sono oggetto di spettacolarizzazione degli stessi sanitari, avvengono anche per sottovalutazione dello stesso professionista sanitario che, in alcuni casi, Si evidenzia, pertanto, la necessità di contrastare siffatti avvenimenti che, in alcuni casi, Al fine di sconsigliare attraverso l'invio di specifiche raccomandazioni agli Ordini e Collegi Enti di farsi parte attiva di evidenziare la problematica sopra esposta e si sottolinei la necessità del professionali nelle quali si evidenzi la problematica sopra esposta e si sottolinei la necessità del rispetto dell'etica professionale.

IL DIRETTORE GENERALE

Referente:
Dott.ssa Laura Tironi
Tel. 06.5994283

"...nella generalità dei casi, infatti, **il soggetto che svolge una professione per cui sia richiesta l'iscrizione ad un albo, nonché l'osservanza ad un codice deontologico, non riesce facilmente a scindere la propria individualità dal lavoro che svolge.**

Ciò in particolare dinnanzi all'altro. Il professionista è identificato direttamente con la persona, e per questo motivo i comportamenti tenuti dallo stesso sono più facilmente sindacabili e discutibili. Con la stessa facilità con cui si acquisisce stima e fama presso i consociati, così la si perde o ci si macchia di disapprovazione e disprezzo."

Milano

Milano, richiamo dell'Ordine ai medici: state attenti a come usate i social

L'IMPATTO DELLE NUOVE TECNOLOGIE SULLA PROFESSIONE MEDICA

RAPPORTO CON I PAZIENTI

ORGANIZZAZIONE DEL LAVORO

L'ORGANIZZAZIONE DEL LAVORO

BACK OFFICE: *strumenti per la gestione del lavoro (fascicolo sanitario elettronico, smartphone, tablet, pc, software, server, email, pec, firma digitale, fatture elettroniche, cloud, gestionali di studio, strumenti di diagnosi, dispositivi di cura, open data, personale impiegato e collaboratori esterni, fornitori, amministratori di sistema, ecc.…).*

DISPOSIZIONI NORMATIVE

- TRATTAMENTO DEI DATI PERSONALI E SICUREZZA INFORMATICA
- FATTURAZIONE ELETTRONICA
- POSTA ELETTRONICA CERTIFICATA
- FIRME ELETRONICHE

- DOCUMENTO ELETTRONICO
- CONSERVAZIONE ELETTRONICA
- DIRITTO D'AUTORE
- CODICE CIVILE E CODICE PENALE

L' ORGANIZZAZIONE DEL LAVORO

richiede un'analisi preventiva che tenga conto della normativa applicabile in materia

OGNI STRUMENTO ELETTTRONICO HA UN PROPRIO ASPETTO GIURIDICO

NEL RAPPORTO CON I PAZIENTI

FRONT OFFICE: *strumenti per offrire e rendere la prestazione professionale (email, pec, social network, blog, sito internet, strumenti di diagnosi, dispositivi di cura, robotica, intelligenza artificiale, ecc.)*

DISPOSIZIONI NORMATIVE

- TRATTAMENTO DEI DATI PERSONALI E SICUREZZA INFORMATICA
- DOCUMENTO ELETTRONICO (validità e trasmissione)
- CODICE CIVILE E PENALE

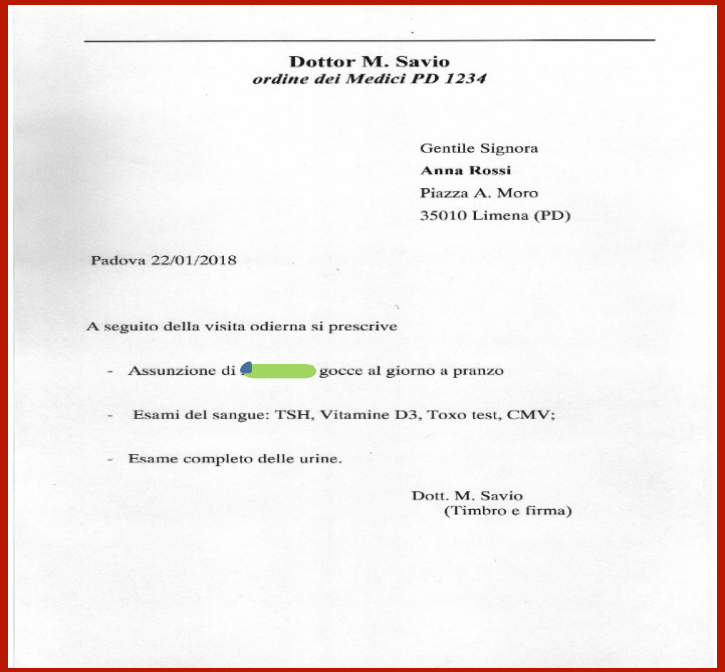
- COMMERCIO ELETTRONICO
- CODICE DEL CONSUMO
- DIRITTO D'AUTORE
- …..

IL DOCUMENTO ELETRONICO

***

LA POSTA ELETTRONICA CERTIFICATA

IL DOCUMENTO ELETTRONICO



Dottor M. Savio
ordine dei Medici PD 1234

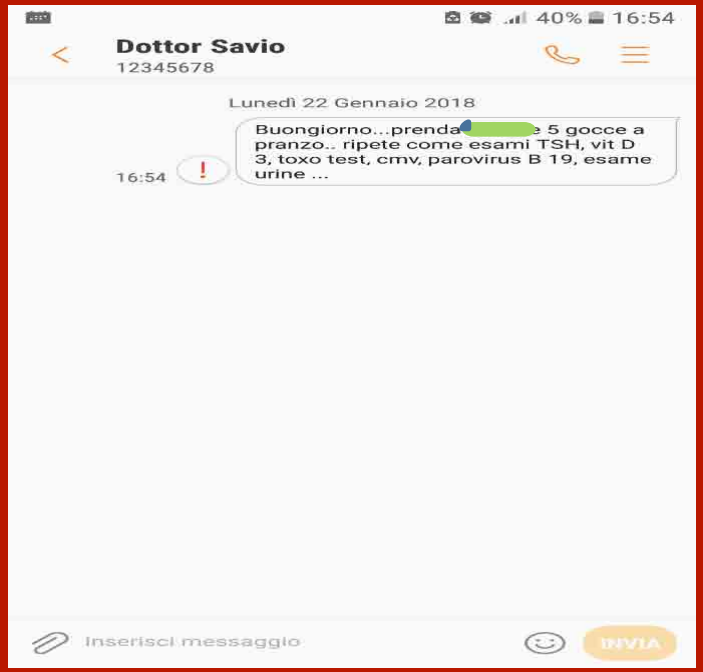
Gentile Signora
Anna Rossi
Piazza A. Moro
35010 Limena (PD)

Padova 22/01/2018

A seguito della visita odierna si prescrive

- Assunzione di [redacted] gocce al giorno a pranzo
- Esami del sangue: TSH, Vitamine D3, Toxo test, CMV;
- Esame completo delle urine.

Dott. M. Savio
(Timbro e firma)



EIDAS

- *Articolo 46 Effetti giuridici dei documenti elettronici*

  A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

@

- *Cass. civ. Sez. VI - 2 Ord., 14/05/2018, n. 11606 «In tema di efficacia probatoria dei documenti informatici, il messaggio di posta elettronica (cd.* ***e-mail) costituisce un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»***

LA POSTA ELETTRONICA CERTIFICATA

- ✓PATERNITA'
- ✓INTEGRITA'
- ✓ORA DELL'INVIO
- ✓ORA DELLA CONSEGNA

T.A.R. Umbria Perugia Sez. I, 09/05/2018, n. 300

«Il servizio di posta elettronica certificata presenta delle caratteristiche peculiari tali da garantire agli utenti ***certezza e valore legale dell'invio e della consegna o della mancata consegna del messaggio al destinatario****. Detto sistema…….garantire* ***la certezza del documento, non rendendo possibili modifiche al messaggio,*** *…… la pec* ***garantisce l'opponibilità a terzi*** *del messaggio, dal momento che la ricevuta rilasciata al mittente del gestore costituisce* ***prova legale dell'avvenuta spedizione*** *…. certificando che il messaggio che è stato spedito, è stato consegnato e non è stato alterato in fase di trasmissione,* ***con l'attestazione di data ed ora di ciascuna delle operazioni descritte*** *…in modo che* ***non possano esserci dubbi sullo stato della spedizione di un messaggio****.*

NEL RAPPORTO CON I PAZIENTI

L'uso di strumenti informatici non muta il contenuto della prestazione professionale e le responsabilità da essa derivanti

IL DOCUMENTO ELETTRONICO HA PIENO VALORE DI LEGGE

Aspetti legali dell'uso delle nuove tecnologie nella professione medica

avv. Mariagiovanna Savio
Impresa, privacy e nuove tecnologie

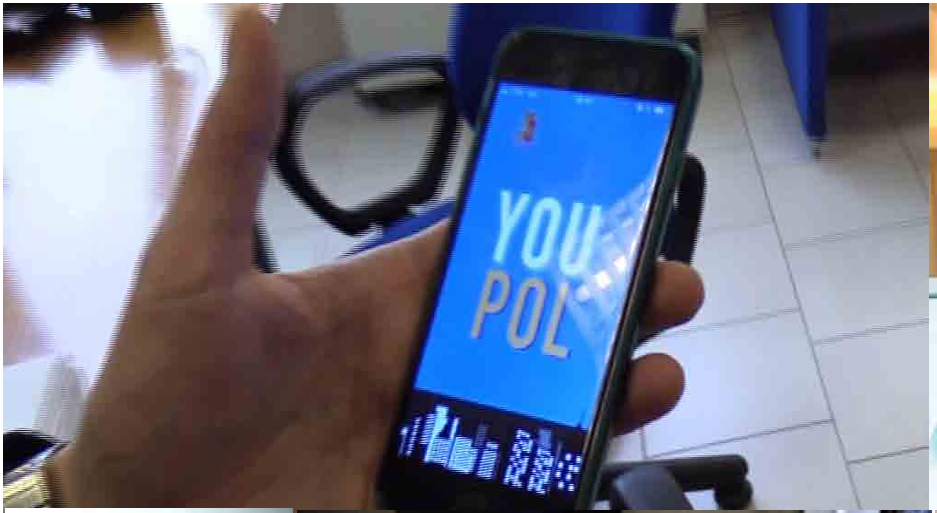
@ info@mariagiovannasavio.it
3479440014
Padova V.le dell'Industria 23/b
www.mariagiovannasavio.it

Quesiti ai relatori

Marco Valerio Cervellini

1. A chi possiamo rivolgerci in caso di necessità?
2. Come possiamo proteggere i nostri dati?
3. Come riconoscere la presenza di un virus o malware nel nostro sistema informatico?

A chi possiamo rivolgerci ?



Come possiamo proteggere i nostri dati?

Roma, 8-11 novembre 2018

ITALIAN CHAPTER

Come riconoscere un virus o malware ?

Roma, 8-11 novembre 2018

ITALIAN CHAPTER

Giuseppe Bernieri

1. Come prevenire eventuali problematiche relative ad attacchi di tipo social engineering ed in generale di cyber security?

2. In riferimento al quadro normativo vigente, quali sono gli aspetti pratici che un medico deve tenere in considerazione rispetto alla tematica cyber security?

3. Come avviene la notifica di un incidente di cyber security da parte di un operatore di servizi essenziali?

Security prevention

For ***individuals***:

- do not provide personal information
- always be suspicious
- use multi factor authentication when possible
- understand what information you share on social media

For ***companies***:

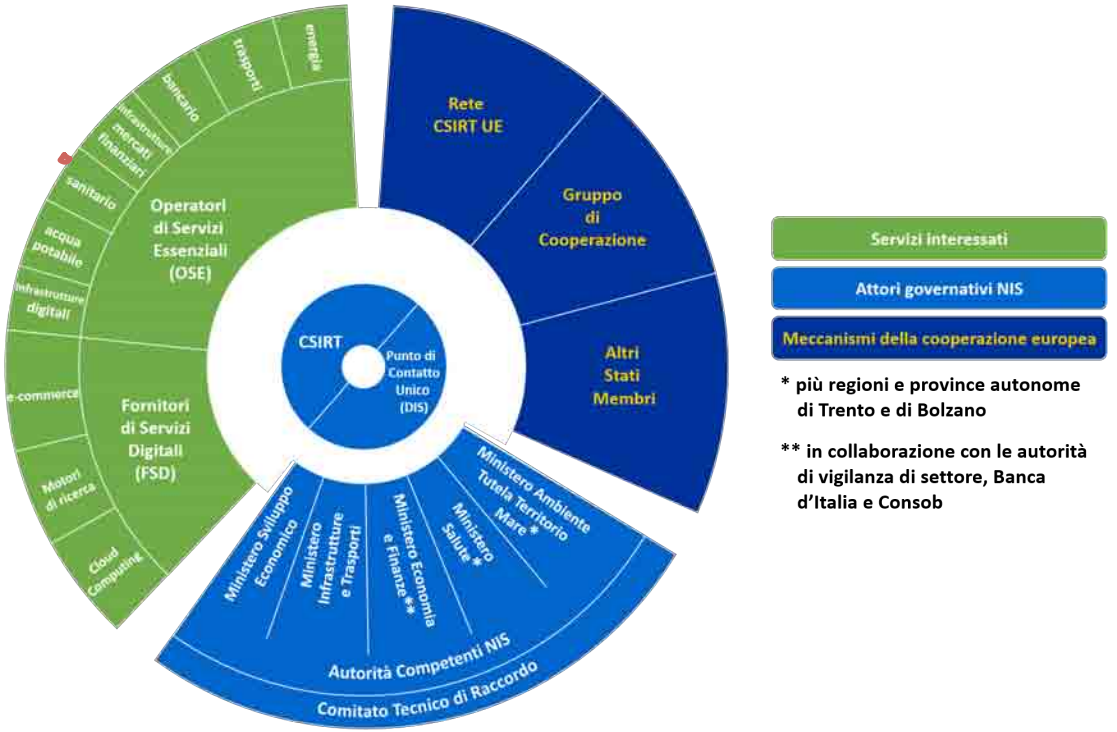
- 3rd party tests (***pentesting***)
- use internal policies for strong authentication
- training / user awareness
- limit public information

Direttiva NIS

Con il **Decreto Legislativo 18 maggio 2018, n.65**, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cd. **Direttiva NIS**, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli **Operatori di Servizi Essenziali (OSE)** e ai **Fornitori di Servizi Digitali (FSD).**

Quadro normativo

Gli **OSE** sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori **sanitario**, dell'**energia**, dei **trasporti**, **bancario**, delle **infrastrutture dei mercati finanziari**, della **fornitura e distribuzione di acqua potabile** e delle **infrastrutture digitali.**



Fonte: https://www.csirt-ita.it/nis.html

Quadro normativo

Gli Operatori di Servizi Essenziali (OSE):

- sono chiamati ad adottare **misure tecniche e organizzative adeguate e proporzionate** alla **gestione dei rischi** e a **prevenire** e **minimizzare l'impatto degli incidenti** a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio.

- hanno l'**obbligo di notificare, senza ingiustificato ritardo**, gli **incidenti** che hanno un **impatto rilevante**, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.

Fonte: https://www.csirt-ita.it/nis.html

Quadro normativo

Le **Autorità competenti NIS**, quali responsabili dell'attuazione del decreto:

- individuano le soglie in ragione delle quali un incidente è da considerarsi pregiudizievole per la sicurezza dei sistemi informativi
- se un evento implica anche violazione di dati personali, operano in stretta cooperazione con il Garante per la protezione dei dati personali per soddisfare il regolamento europeo per la protezione dei dati personali (**GDPR**).

MODELLO DI NOTIFICA INCIDENTE

TIPOLOGIA DI NOTIFICA ○ Obbligatoria ○ Volontaria - ex art. 18 D.lgs. 65/2018

Sezione A: Soggetto che effettua la notifica

Nome e cognome

Ruolo e funzione rivestiti

Indirizzo PEC e/o e-mail

Recapito telefonico

Ulteriori informazioni utili

Sezione B: Dettagli dell'operatore/fornitore

Denominazione ente/azienda e ragione sociale

Indirizzo sede legale (indicare anche il nominativo del rappresentante legale dell'azienda in Italia)

La notifica dell'incidente deve essere effettuata utilizzando il modulo disponibile nella sezione "modulistica" del sito del CSIRT Italia.

Il modulo deve essere firmato digitalmente e inviato in forma cifrata all'indirizzo email: **notifica.nis@csirt-ita.it**.

Fonte: https://www.csirt-ita.it/nis.html

Mariagiovanna Savio

1. Come comportarsi innanzi ad una richiesta di parere medico tramite «social»?
2. Devo monitorare la mia casella PEC?
3. Quali sono le implicazioni dell'uso del cloud nella mia professione?

Come comportarsi innanzi ad una richiesta di parere medico tramite «social»?

Devo monitorare la mia casella PEC?

Quali sono le implicazioni dell'uso del cloud nella mia professione?

Domande da parte dei partecipanti

Associazione Medici Endocrinologi
Per la qualità clinica in Endocrinologia

Take Home Messages

- La categoria **«Healthcare» è una tra le più esposte**
- **Anche realtà**, come ad esempio uno **studio medico o il proprio ambulatorio**, sono soggette ad **elevati rischi** (personal computer, smartphone, ecc.)
- **Non fornite informazioni personali**, siate sempre sospettosi ed attenzione a quali informazioni condividete sui social media (siate sempre prudenti)
- **Il messaggio di posta elettronica** (cd. e-mail) costituisce un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
- **L'uso di strumenti informatici** non muta il contenuto della prestazione professionale e le responsabilità da essa derivanti ed il **documento elettronico ha pieno valore di legge**
- **La polizia postale** e delle comunicazioni ha un ruolo importante per la nostra difesa

Grazie a tutti per l'attenzione!