



Prot. 123/SN

8 febbraio 2024

Al Ministero dell'Interno  
Dipartimento della Pubblica Sicurezza  
Direzione Centrale di Sanità

R O M A

Al Ministero dell'Interno  
Dipartimento della Pubblica Sicurezza  
Segreteria del Dipartimento  
Ufficio V per le Relazioni Sindacali

R O M A

**Oggetto: Gestione dati sensibili e posta elettronica certificata**

La gestione dei dati sensibili in formato elettronico è una delle problematiche ancora non ben recepite, specialmente quella inerente alla certificazione medica del dipendente in MIPG Web.

Sebbene la disposizione della Direzione Centrale della Sanità del 13.09.2022, prot. 16006/2022, abbia specificatamente indicato il MIPG come “un sistema informativo valido e quanto prezioso, che consente di abbattere gli oneri amministrativi favorendo nel contempo la gestione informatica dei documenti”, la seconda parte della circolare definisce il flusso documentale dei certificati non ragionevolmente funzionale, andando in parte contro l’attuale normativa CAD.

Tra le tante difficoltà vi è quella relativa all’amministrazione materiale del certificato medico cartaceo da consegnare in ufficio anche quando, come specifica la circolare, il certificato può essere anche sottoscritto con firma digitale che, una volta stampato, perde qualsiasi certificazione digitale senza possibilità di riscontro di autenticità.

La Circolare in questione, a nostro avviso, è da aggiornare, sopra tutto in forza delle nuove funzionalità del sistema MIPG, che permette al medico di interagire su differenti Aree Organizzative Omogenee, evitando così la trasmissione via PEC del certificato che, ad ogni passaggio, viene duplicato rendendo lo stesso documento difforme l’uno dall’altro.

Inoltre, se intendiamo raggiungere una vera semplificazione di questa materia, questa OS auspica di intraprendere un percorso che porti, anche per i dipendenti della Polizia di Stato, alla certificazione medica esclusivamente elettronica.



In attesa di un eventuale processo completamente elettronico, la gestione dell'attuale certificato cartaceo potrebbe ottimizzarsi solo con uno studio del flusso documentale a cura di esperti, sul piano della vera e propria materia sanitaria, legislativa e conoscenza tecnica delle funzionalità dell'applicativo MIPG. Tale ottimizzazione porterebbe, oltre alla riduzione l'impiego di persone e uffici impegnati alla trattazione del dato sensibile, alla tempestiva visione del certificato del dipendente al medico di competenza. Cosa che, allo stato attuale, il sanitario è l'ultimo a leggere il documento.

Per evitare, inoltre, il duplicarsi del lavoro, anche in questo caso è auspicabile una cooperazione applicativa tra MIPG e GUS-N, così da evitare di alimentare due sistemi informatici con la stessa informazione, con il concreto rischio di difformità.

A tal riguardo la scrivente O.S. ritiene che sarebbe quanto mai necessario ribadire i passaggi, gli strumenti e il personale deputato alla trattazione e visione dei citati certificati medici.

È bene ribadire che i certificati medici, come da richiamata circolare, possono e devono essere gestiti con lo strumento MIPG Web, anche in forza alla obbligatoria protocollazione in entrata elettronica.

Inoltre, con la funzione obbligatoria di criptazione MIPG del file, il sistema garantisce un'ulteriore sicurezza anche quando, per un prevedibile errore, viene collocato in un'area "pubblica". Anche in tale ipotesi l'utente che potrà aprire il file sarà solo colui accreditato con profilo di trattazione dato sensibile, mentre agli altri sarà impossibile consultare il documento (situazione questa che è bene ribadire). Pertanto la riservatezza del dato NON è certamente garantita dalla posizione del file, ma soprattutto dal profilo MIPG dell'utente.

Altra problematica che influisce gravemente sulla riservatezza della documentazione, è quella relativa alla diminuzione degli indirizzi PEC degli uffici. Allo stato attuale, infatti, mancano caselle di Posta elettronica certificata per gli Uffici Affari Generali che, di sovente, si trovano a gestire documentazione sensibile e soggetta a riservatezza.

Con l'utilizzo sempre più massivo del sistema MIPG, si impone, alla gran parte dei dipendenti, di dover provvedere a spedire la documentazione prodotta e/o lavorata. Pertanto, molti, se non tutti, sono accreditati sullo stesso indirizzo PEC e, non potendo differenziare l'accesso tra la visione di posta in entrata e posta in uscita, tutti possano consultare i documenti contenuti, compresi quelli sensibili e soggetti a riservatezza.

Ci si interroga poi, su chi debba rispondere, in caso di contestazione di violazione della privacy, laddove siano stati eliminati canali riservati alla trasmissione di documenti sensibili e riservati esterni alla AOO.



Pertanto, chiediamo di fornire, quanto prima, caselle specifiche di posta elettronica certificata a tutti quegli uffici che devono trattare dati sensibili, quali ufficio sanitario, Ufficio Affari Generali ecc. che solitamente trattano materie inerenti al personale dipendente.

Si chiede altresì la possibilità di valutare la creazione di una casella PEC specifica per le sale operative delle questure e delle specialità che, nelle piccole e medie realtà, sono gli unici uffici funzionanti H24 al fine di poter ottimizzare le comunicazioni urgenti in orari particolari, così da ottemperare agli obblighi di protocollazione, anche quando non è presente personale addetto.

Per quanto esposto questa OS rimane a disposizione per qualsiasi ulteriore chiarimento in merito, sempre in un'ottica di costruttiva collaborazione

IL SEGRETARIO GENERALE FSP  
Valter Mazzetti