Firenze, 07/05/2020
Prot. n. 38374

A tutti i dipendenti
Azienda USL Toscana Centro

Oggetto: Linee guida per la trasmissione telematica dei dati personali: modalità e condizioni di conformità al Regolamento UE 2016/679 (GDPR).

Nell'ambito delle misure adottate dal Governo per il contenimento e la gestione dell'emergenza epidemiologica da COVID-19 (coronavirus), sono stati emanati una serie di decreti di urgenza, in particolare il D.L. 9/03/2020 n. 14 ove all'art. 14 dispone in merito al trattamento dei dati nel contesto emergenziale.

Al di fuori degli ambiti puntualmente individuati e normati dalla citata decretazione di emergenza, è integralmente confermata l'applicabilità del previgente quadro normativo in materia di protezione dei dati personali, segnatamente anche per quanto concerne lo specifico tema dell'utilizzo della posta elettronica per la trasmissione informatica dei dati particolari (*in primis* dati relativi alla salute, art 9 GDPR) e dei dati relativi a condanne penali e reati (art. 10 GDPR) da parte degli attori del servizio sanitario.

Le linee guida allegate, predisposte dal tavolo regionale privacy coordinato dalla regione Toscana, confermano, pertanto, in riferimento a distinti ambiti di operatività, le modalità di utilizzo della posta elettronica in conformità alle specifiche disposizioni vigenti e con le adeguate misure che questa Azienda deve garantire a tutela del livello di sicurezza del trattamento dei dati ai sensi dell'art.32 del GDPR.

A tali linee guida il personale si deve attenere e in caso di dubbi o necessità di maggiori chiarimenti potete rivolgervi all'Avv. Michele Morriello via email responsabileprotezionedati@uslcentro.toscana.it.

Il Titolare del Trattamento dati
per l'Azienda USL Toscana Centro
Il Direttore Generale
(Dr. Paolo Morello Marchese)

Allegato: Linee guida utilizzo della posta elettronica per la trasmissione di dati personali particolari/relativi a condanne penali e reati:modalità e condizioni di conformità al Regolamento UE 2016/679 – GDPR.

Azienda USL Toscana centro

SST Azienda USL Toscana centro
Servizio Sanitario della Toscana

Il Direttore Generale
Azienda USL Toscana Centro
Dr. Paolo Morello Marchese

50122 Firenze
Piazza S. Maria Nuova,1
Telefono:
055 693.9222; 9219; 8389
Fax: 055 693.9223
e-mail:
direttoregenerale@uslcentro.toscana.it

Il Responsabile Protezione Dati
Avv Michele Morriello

e.mail::
responsabileprotezionedati@uslcentro.toscana.it

UTILIZZO DELLA POSTA ELETTRONICA PER LA TRASMISSIONE DI DATI PERSONALI PARTICOLARI/RELATIVI A CONDANNE PENALI E REATI: MODALITA' E CONDIZIONI DI CONFORMITA' AL REGOLAMENTO UE 2016/679 - RGPD

CONTESTO E INTRODUZIONE

In relazione al periodo di durata dello stato di emergenza deliberato dal Consiglio dei ministri in data 31 gennaio 2020 e relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili,il decreto legge 9 marzo 2020, n. 14, recante "Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19, all'art. 14, rubricato "Disposizioni sul trattamento dei dati personali nel contesto emergenziale"":

- regola (comma 1) l'interscambio di dati, anche sanitari, legittimando i soggetti ivi individuati,(tra i quali le Aziende sanitarie) a effettuare trattamenti, inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del Regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19
- prevede(comma 2) che la comunicazione a soggetti pubblici e privati, diversi da quelli del comma 1, nonché la diffusione dei dati personali diversi da quelli di cui agli artt. 9 e 10 del regolamento (UE) 2016/679 possa essere effettuata nei casi in cui risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto
- fa espressamente salvi (comma 3) in riferimento ai trattamenti di cui ai commi precedenti, il rispetto dei principi di cui all'art. 5 RGPD e l'adozione di misure appropriate a tutela dei diritti e delle libertà degli interessati (l'art. 5 citato declina i principi del trattamento dei dati, liceità,correttezza, integrità e riservatezza etc., che ogni titolare deve dimostrare di rispettare)..

Lo stesso art. 14 ai commi 4 e 5, sempre limitatamente al contesto emergenziale,introduce semplificazioni per taluni adempimenti formali (modalità di individuazione dei soggetti autorizzati al trattamento e rilascio dell'informativa).

Preme evidenziare che al di fuori degli ambiti puntualmente individuati e normati dalla sopra citata decretazione di emergenza, è integralmente confermata l'applicabilità del previgente quadro normativo in materia di protezione dei dati personali, segnatamente anche per quanto concerne lo specifico tema di cui all'oggetto, l'utilizzo della posta elettronica per la trasmissione informatica dei dati particolari (*in primis* dati relativi alla salute, art 9 RGPD) e dei dati relativi a condanne penali e reati (art. 10 RGPD) da parte degli attori del servizio sanitario regionale. Pertanto, di seguito e in riferimento a distinti ambiti di operatività, un quadro riassuntivo delle modalità di utilizzo di questo strumento in conformità alle specifiche disposizioni vigenti e con le adeguate misure che ogni titolare deve garantire a tutela del livello di sicurezza del trattamento ai sensi dell'art. 32 RGPD.

1.1 Modalità utilizzo posta elettronica all'interno dell'organizzazione del titolare

All'interno dell'organizzazione del titolare, la trasmissione/accessibilità informatica di dati particolari/relativi a condanne penali e reati riconducibili alla persona (dato nominale o associato a codici riconducibili alla persona) da parte di personale autorizzato al trattamento, si realizza ordinariamente attraverso strumenti/soluzioni informatiche dedicate

(utilizzo dello stesso applicativo verticale, applicativi verticali diversi e operanti in collaborazione applicativa, dossier, piattaforme /spazi digitali condivisi etc..) con l'obiettivo di contenere l'informazione all'interno di un ambito predefinito e strettamente monitorabile attraverso i log di procedura.

L'utilizzo del sistema di posta elettronica tradizionale del titolare (e-mail) è da considerarsi soluzione residuale da porre in essere solo ove risulti indispensabile e con l'obbligo di attenersi alle seguenti modalità:

- divieto di riportare in chiaro nel corpo della mail contenuti riferibili a informazioni personali cd sensibili (dati particolari/relativi a condanne penali e reati)
- spedire il documento contenente i dati personali in forma di allegato al messaggio e non come testo del messaggio
- l'allegato deve essere criptato e protetto da password (ad. es. file compresso zip e protetto da password) e la password deve essere comunicata al destinatario con canale diverso dalla mail (telefono, sms,fax etc.).

Su zippatura e policy password si rimanda all'allegato alla presente nota.

1.2 Modalità utilizzo posta elettronica verso/da soggetti terzi rispetto all'organizzazione del titolare

La comunicazione/trasmissione dei dati verso/da soggetti terzi rispetto all'organizzazione del titolare può avvenire, in presenza di idonea base giuridica, nei seguenti casi:

a. <u>verso/da altro soggetto pubblico</u> (altra azienda sanitaria, ente pubblico etc..)
In caso di comunicazione con altri soggetti istituzionali, posto che è preferibile attivare canali specifici di comunicazione mediante strumenti quali accesso via web e accesso in modalità di collaborazione applicativa, per comunicazioni la cui periodicità è limitata e la quantità dei dati è contenuta, utilizzare lo strumento di Posta Elettronica Certificata con l'obbligo di attenersi alle seguenti modalità

- le informazioni devono essere inviate in forma di allegato al messaggio e non come testo compreso nella body part del messaggio
- allegato contenente le informazioni zippato e protetto da password
- password comunicata mediante un canale diverso da quello utilizzato per trasmettere i dati (ad es. invio per posta elettronica ordinaria, fax, sms, telefono).
- apposita procedura per interrompere l'invio per PEC a un destinatario che abbia comunicato il furto o lo smarrimento delle credenziali di autenticazione per l'accesso al proprio sistema di PEC o altre condizioni di possibile rischio per la riservatezza dei dati.

b.<u>verso/da soggetto privato</u> (MMG/PLS, struttura accreditata, fornitore etc)
In tali casi si individua, quale modalità ordinaria e corrente lo strumento di Posta Elettronica Certificata con l'obbligo di attenersi alle modalità di cui al precedente punto a.
In subordine e in via straordinaria (limitatamente al periodo di durata dell'emergenza stante le correlate limitazioni negli spostamenti e nell'operatività dei singoli) si individua la seguente modalità:

- invio da posta elettronica ordinaria a posta elettronica ordinaria
- convalida dell'indirizzo mail esterno con procedura di verifica apposita in modo da impedire che il documento anche se criptato sia recapitato a soggetto diverso dal destinatario

- le informazioni devono essere inviate in forma di allegato al messaggio e non come testo compreso nella body part del messaggio
- allegato contenente le informazioni zippato e protetto da password
- password comunicata mediante un canale diverso da quello utilizzato per trasmettere i dati (ad es. fax, sms, telefono).

Su procedura di convalida indirizzo mail, zippatura e policy password si rimanda all'allegato alla presente nota.

1.3 Modalità utilizzo posta elettronica verso il paziente

In presenza di idonea base giuridica, lo strumento di posta elettronica è utilizzabile per l'invio al paziente del referto/altra documentazione sanitaria o comunque recante informazioni direttamente /indirettamente riferite al suo stato di salute nel rispetto delle seguenti modalità:

a. invio tramite posta elettronica ordinaria

- convalida dell'indirizzo mail esterno con procedura di verifica apposita in modo da impedire che il documento anche se criptato sia recapitato a soggetto diverso dall'interessato
- referto/documentazione spediti in forma di allegato a un messaggio e non come testo compreso nel corpo del messaggio
- allegato protetto con tecniche di cifratura e accessibili tramite una password per l'apertura del file consegnata separatamente all'interessato
- possibilità per il paziente di confermare l'indirizzo di posta elettronica cui ricevere l'invio in occasione di successivi accertamenti clinici.

b. invio tramite Posta Elettronica Certificata

- referto/documentazione spediti in forma di allegato a un messaggio e non come testo compreso nel corpo del messaggio.

La necessità di assicurare una consulenza appropriata nell'effettuazione di alcuni test genetici fa ritenere possibili servizi di tele refertazione solo nel caso in cui l'interessato si sottoponga a tali indagini cliniche nell'ambito di un complessivo servizio di tele consulenza; in tal caso occorre seguire il *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101* del 5 giugno 2019, ovvero:

- utilizzo della Posta Elettronica Certificata
- trasmissione dei dati in forma di allegato e non come testo compreso nel corpo del messaggio
- cifratura dei dati avendo cura di rendere nota al destinatario la chiave crittografica tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati.

E' vietato l'utilizzo della posta elettronica/Posta Elettronica Certificata per l'invio al paziente nei casi di accertamenti sull'HIV.

Su procedura di convalida indirizzo mail, zippatura e policy password si rimanda all'allegato alla presente nota.

Normativa di riferimento

- Provvedimento Autorità Garante n. 36 del 19 novembre 2009 *". Linee guida in tema di referti on-line"*
- D.P.C.M 8 agosto 2013 *"Modalità di consegna, da parte delle Aziende sanitarie,dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento online delle prestazioni erogate, ai sensi dell'articolo 6, comma 2, lettera d) , numeri 1) e 2) del decreto-legge 13 maggio 2011, n.70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, recante «Semestre europeo – prime disposizioni urgenti per l'economia».*
- Provvedimento Autorità Garante n. 393 del 2 luglio 2015 *"Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche "*
- Provvedimento Autorità Garante n. 146 del 5 giugno 2019 "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"*
- Parere Autorità Garante al Ministero della Salute su un documento recante "*Modalità tecniche per lo scambio dei dati relativi alla situazione vaccinale degli iscritti tra le istituzioni scolastiche/educative e formative e l'Azienda sanitaria locale competente*" - 22 febbraio 2018
- Parere Autorità Garante sulle modalità di consegna della ricetta medica elettronica - 19 marzo 2020

ALLEGATI

Allegato 1. "*Procedura di convalida indirizzo mail, zippatura e policy password: istruzioni operative"*

ALLEGATO 1

Procedura di convalida indirizzo mail, zippatura e policy password: istruzioni operative.

La convalida dell'indirizzo mail è una operazione necessaria per avere la certezza che la comunicazione avvenga con il soggetto effettivamente destinatario della missiva.
L'indirizzo mail sarà quindi rilevato nel contatto con l'utente in presenza, per esempio nella fase della prenotazione, oppure della visita, o anche nel contatto telefonico.

Altre modalità che forniscono certezza sono relative a procedure che consentono il riconoscimento sicuro dell'utente, per esempio su servizi o app in cui l'identificazione avvenga tramite CNS (quale la Tessera sanitaria): sarebbe quindi da considerarsi verificato per esempio il numero di telefono inserito nel Fascicolo Sanitario da parte dell'utente nei "numeri utili" della sezione "Il mio taccuino", in quanto compilabile solo dall'interessato.

L'indirizzo mail potrà essere verificato, con ragionevole affidabilità mediante l'incrocio con altro strumento di contatto dell'utente, per esempio inviandogli un codice via sms sul numero di cellulare fornito come proprio e chiedendo di rispondere alla mail inviata all'indirizzo dichiarato, riportando quel codice.

La criptazione del documento allegato serve a mantenere riservato il contenuto della comunicazione anche dopo che la mail è stata ricevuta dal destinatario, rimandando alla esclusiva responsabilità di quest'ultimo la eventualità che il documento rimanga in chiaro sulla postazione di lavoro dopo che è stata effettuata l'operazione di decriptazione.
Per sicurezza, chi riceve e decripta l'allegato, può mantenere sullo strumento in uso (e che collega in internet) solo la copia criptata dell'allegato, o effettuare una successiva criptazione della stessa con propria password; oppure può scaricare il documento in chiaro su supporto fuori linea (chiavetta usb, hd esterno) per la sua conservazione condifenziale.

La comunicazione di un documento criptato necessita di due requisiti:

1) la password di criptazione utilizzata dall'inviante deve essere conosciuta dal soggetto che riceve il documento (procedura simmetrica)
2) lo strumento (software) utilizzato per effettuare la criptazione deve essere disponibile anche al soggetto che vuole decriptare.

In questo caso avere la disponibilità di un software liberamente scaricabile dal web rappresenta una ottima opportunità.
La procedura seguente illustra come procedere per l'invio di documenti compressi e crittografati utilizzando il prodotto 7-Zip scaricabile liberamente dal sito www.7-zip.org.
La procedura che segue illustra l'utilizzo di questo prodotto per la criptazione.
La procedura è da intendersi esemplificativa dei parametri e delle fasi operative che devono essere normalmente eseguite.
Nella scelta del prodotto è da preferirsi la semplicità di acquisizione (e la gratuità) da parte del ricevente; la disponibilità del prodotto multipiattaforma (Windows, Linux, MAC, IOS, Android, ecc.) la semplicità dello svolgimento della fase di criptazione/decriptazione.
In particolare il prodotto utilizzato in queste istruzioni da una parte offre l'opportunità di poter essere decriptato anche mediante altre app o software (winzip, winrar, ecc.), ma potrebbe non essere garantito il funzionamento in alcune piattaforme MAC).

Per utilizzare il software occorre scaricarlo installarlo sul proprio pc (se non si posseggono i diritti di amministratore del pc, rivolgersi all'help desk per il supporto).

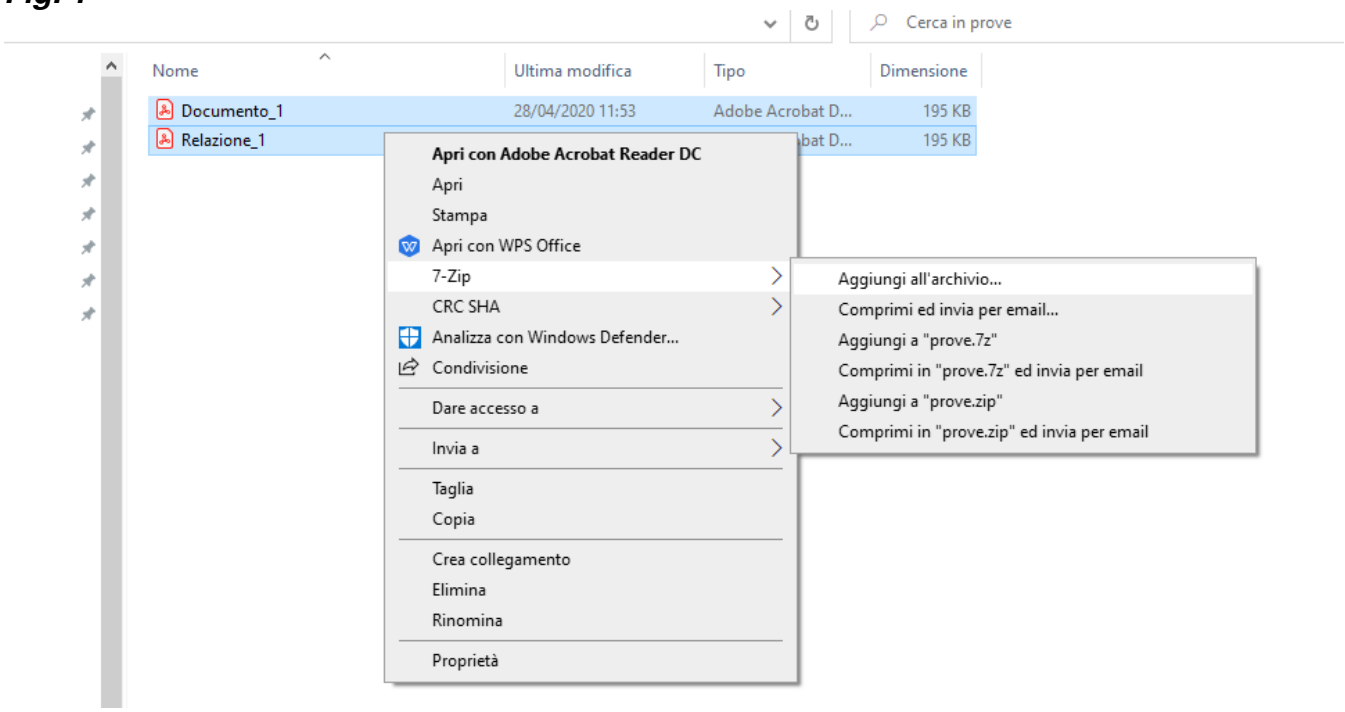
Per effettuare la cifratura procedere come segue:

1) scrivere su un proprio documento la password che si utilizzerà per la criptazione, in modo da poterla riportare correttamente in fase di criptazione del documento e essere sicuri di comunicarla in modo corretto al destinatario.

   Questo consente di costruire la password della complessità desiderata che si raccomanda avere le seguenti caratteristiche minime:
   - lunghezza almeno 10 caratteri
   - la password deve contenere numeri, caratteri sia maiuscoli che minuscoli, e simboli, combinati fra loro: almeno uno per ogni insieme, quindi almeno un carattere maiuscolo, almeno un carattere minuscolo, almeno un numero, almeno un carattere speciale fra quelli ammessi, esempio: "@nTr0poL0g1a";
   - non deve avere più di tre caratteri consecutivi che si ripetono;
   - non deve riportare facilmente ad analogie sull'utente (es. combinazione di caratteri del nome e numeri della data di nascita);

2) **Fig. 1**. Selezionare il/i file da proteggere (es. dall'interfaccia di windows tenendo premuto <ctrl> +tasto sx del mouse su ciascun file); cliccare quindi con il tasto dx del mouse, selezionare 7-Zip e quindi "Aggiungi all'archivio"

Fig. 1

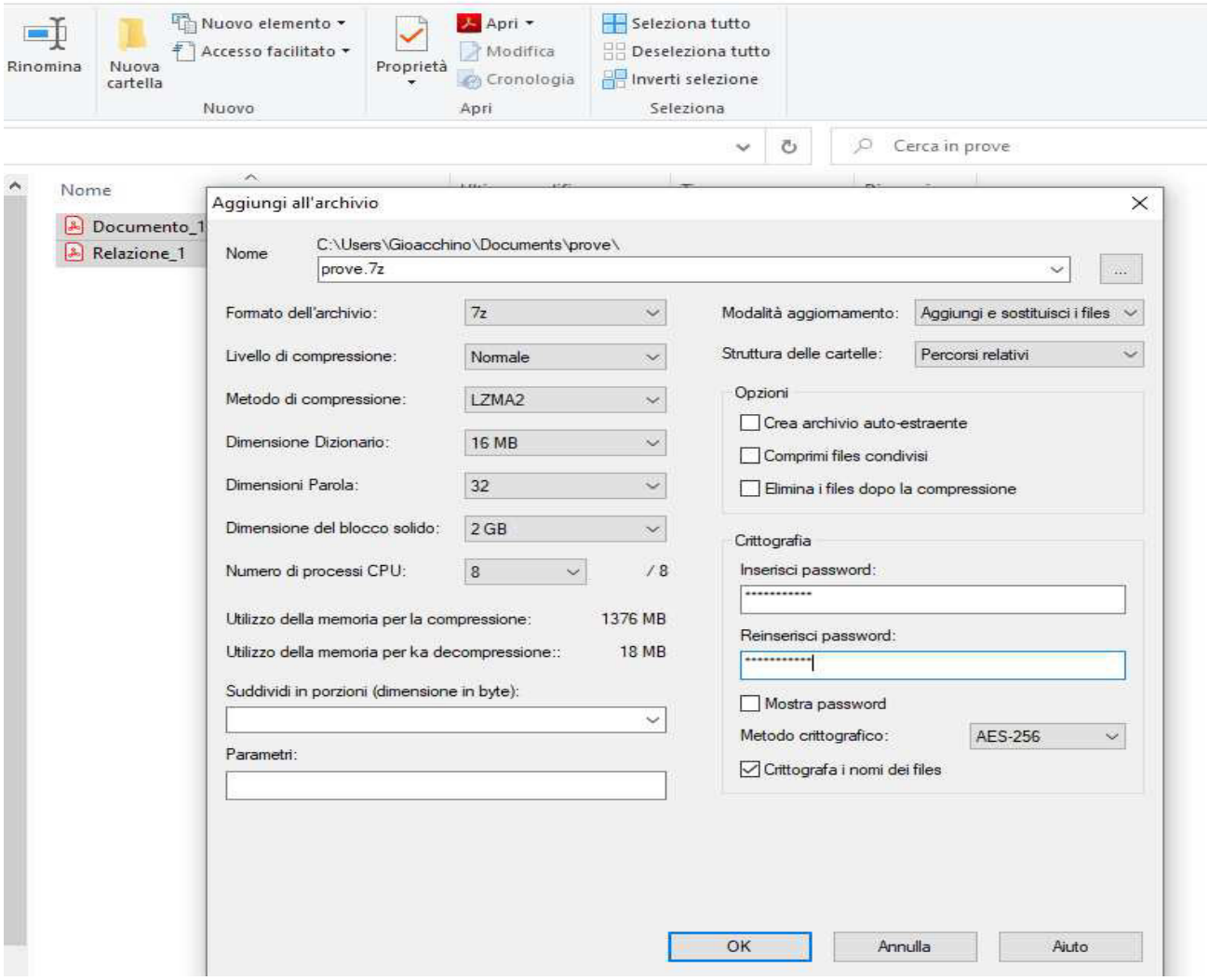


3) **Fig. 2**. Sulla videata che si apre:
   - Selezionare <Formato Archivio>: 7z
   - Assegnare un nome al file criptato (es. prove.7z)
   - Selezionare <Metodo Crittografico>: AES-256
   - Inserire la password scelta nelle due posizioni indicate (o copia/incolla dal

documento su cui si è trascritta al punto 1

- Mettere il check su <Crittografa i nomi dei file> (impedisce anche la visualizzazione prima della decriptazione del nome dei file contenuti).

Fig. 2



4) Inviare tramite mail il file criptato ottenuto;

5) Comunicare per altro canale la password di criptazione/decriptazione, per esempio tramite telefono, o tramite sms o strumenti social quali whatsapp, o Telegram

Con 7-Zip si possono produrre anche degli allegati con criptazione più debole ma sempre protetti da password, con estensione ".zip" da selezionare nel "Formato dell'archivio" e "Metodo crittografico" selezionato come ZipChripto (disponibile per l'estensione .zip).

Documenti zippati con l'estensione ".zip" possono essere prodotti anche con altri strumenti free o a pagamento (winzip, winrar) con procedure pressochè identiche a quelle illustrate per 7-Zip, veicolando archivi che possono essere sicuramente decriptati con i prodotti disponibili nelle varie piattaforme.