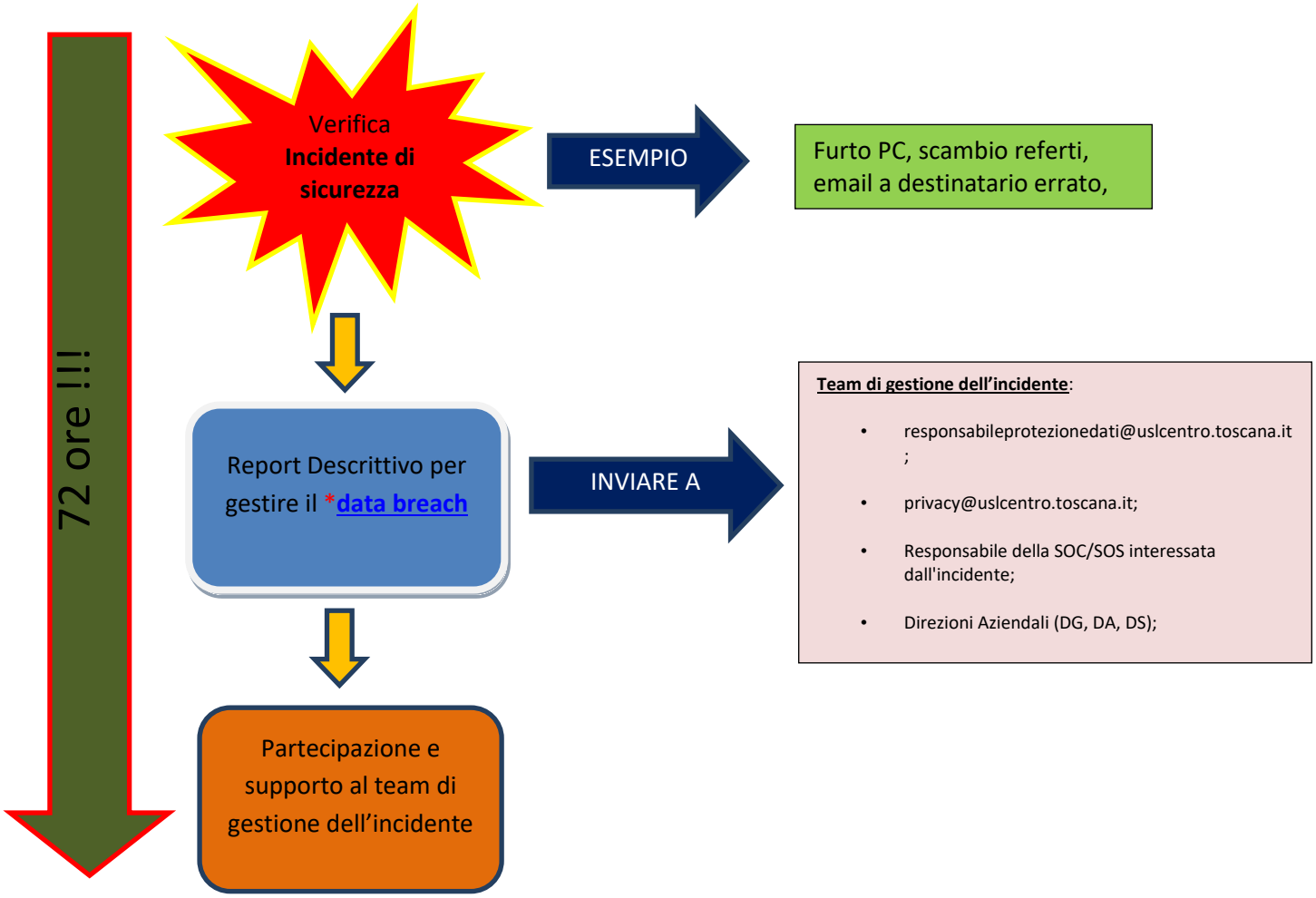
MEMO PRIVACY

Caro Collega,
per mettere in sicurezza i dati personali che trattiamo, che nella maggioranza dei casi appartengono alle categorie particolari come i dati sulla salute, **ti ricordiamo alcune regole fondamentali per evitare comportamenti non corretti che espongono le persone (i nostri assistiti = interessati) a subire danni quali, a titolo esemplificativo**, la discriminazione, il furto o l'usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, la perdita di riservatezza di dati coperti da segreto professionale.
In presenza di un INCIDENTE DI SICUREZZA che ha comportato o rischia di comportare la perdita di riservatezza, integrità o disponibilità dei dati, dobbiamo essere in grado di riconoscere un episodio critico e rispondere prontamente per contenere e, auspicabilmente, eliminare le conseguenze negative.
Tra i più comuni esempi di incidenti possiamo ricordare:

- ✓ Furto di PC o di altri dispositivi rimovibili (hard-disk, USB);
- ✓ Invio email a destinatari sbagliati (senza password di protezione dei documenti allegati);
- ✓ Consegna di cartella clinica a persona errata e/o scambio di referti;
- ✓ Pubblicazione di atto all'albo on line contenente dati coperti dalla riservatezza.

Proprio per tutelare i nostri Assistiti, l'Azienda ha implementato una serie di importanti misure di sicurezza e adottato una specifica procedura aziendale di gestione degli incidenti e violazione dei dati personali (c.d. data breach) *delibera 250/2020 del 28.02.2020. In molti casi, infatti, intervenire tempestivamente per contrastare un incidente di sicurezza consente di contenere al minimo l'impatto negativo per gli interessati.

Cosa devi fare?



Ti ricordiamo, inoltre, che alcune misure minime di sicurezza **DEVONO** essere sempre presenti.

Ogni dispositivo utilizzato:

✓ deve essere protetto da *PASSWORD e le regole per costruire una buona PW sono inserite nella *scheda ICT del cruscotto privacy; utilizza PW diverse per ogni dispositivo/applicativo e per ogni account, la PW è personale e deve essere conservata con cura evitando di scriverla su fogli che poi tieni sotto la tastiera o nelle vicinanze, di scriverle su file non protetti; non utilizzare mai la possibilità di salvare la PW, quindi devi sempre inserire la PW per accedere ai dispositivi, agli applicativi; non usare la PW del collega per entrare negli applicativi;

✓ Il dispositivo che l'azienda ti ha assegnato o che tu utilizzi deve essere custodito con cura e diligenza; non devono essere lasciate aperte le sessioni di lavoro, se ti devi allontanare dalla postazione, anche se hai inserito lo screensaver, devi chiudere la sessione prima di assentarti;

✓ Nel caso di utilizzo di uno stesso dispositivo da parte di più utenti devi creare una cartella protetta da password dove inserire la documentazione al fine di non renderla accessibile ad altri; la cartella non deve essere collocata nel desktop ma salvata sul disco (percorso documenti).

Quando scrivi una **email** ricorda che non deve essere mai inserito il dato "sensibile" nel corpo della email ma deve essere allegato al messaggio e il documento deve essere protetto con password. *Le indicazioni per come criptare le trovi sul cruscotto privacy insieme alle *Linee guida per la trasmissione telematica dei dati.

Ricorda il principio di minimizzazione nel trattare i dati: tratta, cioè, solo i dati che sono indispensabili e necessari per assolvere alle finalità per le quali sono raccolti, es. il foglio o il file di programmazione dei turni che si porta a conoscenza dei colleghi per la programmazione delle attività non deve mai contenere la causa dell'assenza perché è sufficiente inserire la "A" di assenza.

Ti sei registrato sul portale privacy sezione atti di nomina, come disposto con la *nota del DG prot. n. 129293/19 del 5/12/2019, sottoscrivendo l'atto che ti designa incaricato del trattamento o referente del trattamento se direttore di struttura aziendale? Se ancora non l'hai fatto clicca sul link *portale privacy e trovi le indicazioni per procedere e se hai bisogno di supporto scrivi a privacy@uslcentro.toscana.it L'autorizzazione al trattamento dei dati è condizione essenziale per poter svolgere la propria attività istituzionale.

Ti ricordiamo di partecipare al corso obbligatorio FAD "La protezione dei dati personali in sanità" che deve essere concluso entro il 31/12/2021. Se non ti fosse arrivata la email di convocazione scrivi a sergio2.biagini@uslcentro.toscana.it in qualità di referente dell'evento formativo.

Ti ricordiamo che il non rispetto delle disposizioni impartite in materia di protezione dei dati è fonte di responsabilità disciplinare, amministrativa, erariale e in caso di sanzioni amministrative l'azienda è obbligata a relazionare alla Corte dei Conti sulla sanzione comminata e a procedere all'azione di rivalsa nei confronti del dipendente ritenuto responsabile dell'evento che ha generato la violazione dei dati.

Contatti

Per qualsiasi chiarimento puoi contattare il RPD e l'ufficio privacy

responsabileprotezionedati@uslcentro.toscana.it

privacy@uslcentro.toscana.it

0573/352867

*** la documentazione citata (indicazioni, linee guida, procedure) è direttamente consultabile cliccando sulla parola in blu e sottolineata, inoltre è consultabile sul portale privacy sezione *cruscotto**