Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI
Ufficio federale della sanità pubblica UFSP
Divisione Trasformazione digitale

Aiuto dell'Ufficio federale della sanità pubblica (UFSP)

Allegato 8 OCIP-DFI[1] – Precisazione della procedura per il processo di certificazione secondo la LCIP[2]:

- calcolo del numero di campioni
- audit presso le autorità di registrazione locali

Edizione 1.0 del 16 febbraio 2022

Contatto:

Lorena Kegel
Sezione Sanità digitale
Ufficio federale della sanità pubblica
lorena.kegel@bag.admin.ch

[1] Ordinanza del DFI sulla cartella informatizzata del paziente (RS 816.111).
[2] Legge federale sulla cartella informatizzata del paziente (RS 816.1).

1 Situazione iniziale

Nel processo di certificazione l'Identity Provider (IdP) definisce il campo di applicazione della certificazione secondo la LCIP. Nel campo di applicazione rientrano anche le terze parti incaricate dall'IdP, le cosiddette autorità di registrazione locali (Local Registration Authorities; LRA), le quali provvedono a verificare l'identità al momento dell'emissione degli strumenti d'identificazione (SID). Vi rientrano anche Local Registration Officers mobili (LRAO mobili), che non effettuano la verifica dell'identità al momento dell'emissione dei SID presso un'unica sede, bensì sul posto presso i clienti (p. es. in una struttura sanitaria). Una volta completata con successo la certificazione iniziale potranno essere incluse nel campo di applicazione ulteriori LRA.

Le LRA e i relativi LRAO mobili devono soddisfare i seguenti requisiti:

- le LRA a cui appartengono gli LRAO mobili rappresentano una chiara struttura giuridica;
- deve essere possibile rendere disponibile all'organismo di certificazione (OC) l'estratto del registro di commercio della LRA a cui appartengono gli LRAO mobili;
- l'LRAO mobile deve poter svolgere la sua attività da un LRA Office certificato o essere impiegato presso LRA Office. Non sono accettate persone singole che rappresentano una ditta individuale.

Esempio fittizio di un LRAO mobile: un impiegato postale che lavora in un ufficio postale già certificato secondo l'allegato 8 OCIP-DFI esegue in modalità mobile la verifica dell'identità al momento dell'emissione dei SID.

Il numero di campioni delle LRA da sottoporre ad audit è calcolato in conformità con la normativa **IAF MD-1:2018 (MD1)**. L'attuazione della selezione del campione secondo l'MD1 è un requisito minimo obbligatorio. Nel quadro di tale normativa, quale titolare dello schema di certificazione («schema owner») l'UFSP ha precisato l'attuazione per ridurre il numero di campioni sulla base del rischio. L'obiettivo delle precisazioni è assicurare che tutti gli OC attuino la selezione del campione applicando le stesse norme in tutta la Svizzera e, di conseguenza, tutti gli IdP vengano esaminati allo stesso modo.

2 Calcolo del numero di campioni

2.1 Osservazioni generali

In linea di principio, tutte le LRA rientrano nel campo di applicazione della certificazione e vengono perciò considerate per il calcolo del numero di campioni (si veda il punto 2.2). Anche gli LRAO mobili fanno parte del campione e non sono contati separatamente. Un prerequisito essenziale per la certificazione è la formazione delle LRA per l'emissione di SID. La struttura territoriale e organizzativa dei corsi di formazione deve essere presa in considerazione nel calcolo del numero di campioni (si veda il punto 2.3). Ai sensi dell'approccio basato sul rischio, le LRA vengono inoltre ponderate in modo differenziato in base al settore, permettendo così una riduzione mirata e ragionevole del numero di campioni in funzione del potenziale di rischio (si vedano i punti 2.4 e 2.5).

2.2 Formula / Coefficiente

Le dimensioni del campione y corrispondono alla radice quadrata del numero di sedi secondo la formula $y=\sqrt{x}$, dove x è il numero totale di sedi.

Al momento delle certificazioni iniziali, degli audit di revisione annuali e delle ricertificazioni (se il certificato è scaduto) la formula y=√x viene adeguata moltiplicando il risultato dell'estrazione della radice quadrata per i seguenti coefficienti:

	Coefficiente	**Formula**
Certificazione iniziale	1	y=1,0√x
1° audit di revisione	0,6	y=0,6√x
2° audit di revisione	0,6	y=0,6√x
Ricertificazione	0,8	y=0,8√x

2.3 Approccio basato sul rischio

In sede di selezione del campione l'OC prende in considerazione la struttura territoriale e organizzativa dei corsi di formazione LRA da parte di un IdP. Di conseguenza, l'OC procede con un approccio 1:n all'inizio degli audit, vale a dire che tutte le LRA nel campo di applicazione sono sottoposte ad audit fino a quando non si raggiunge una valutazione soddisfacente dei risultati degli audit. Se un IdP esegue il roll out dei suoi corsi di formazione LRA nello stesso modo in tutta la Svizzera (p. es. per tutti gli uffici postali) e lo documenta per scritto in un'autodichiarazione, si può presumere che la qualità al momento dell'emissione di un SID sia uniforme e si può proseguire passando direttamente al punto 2.5 «Ponderazione per settore».

2.4 Determinazione del settore della LRA

La formula di cui al punto 2.2 è applicata separatamente per le LRA operanti in settori diversi. La classificazione delle LRA avviene in base alla nomenclatura generale delle attività economiche dell'Ufficio federale di statistica (NOGA 2008; https://www.kubb-tool.bfs.admin.ch/it). Ciò significa che le LRA che operano nel commercio (p. es. nel commercio al dettaglio) o che erogano servizi finanziari (p. es. le banche), nonché le LRA attive nella consulenza legale, nell'amministrazione pubblica o nella sanità sono raggruppate per settore e utilizzate come campione per l'audit.
Il calcolo e l'approvazione degli audit per un settore sono da valutare per ciascun IdP; ciò significa che il calcolo è eseguito per ciascun IdP e che i controlli delegati dall'IdP alle LRA sono assegnati per lo specifico campo di applicazione.

2.5 Ponderazione per settore

Settore secondo il punto 2.3	**Fattore***
Commercio al dettaglio in generale (p. es. punti vendita Migros o Coop)	1
Strutture sanitarie: farmacie e studi medici	0,60
Strutture sanitarie: ospedali e case per anziani e di cura	0,60
Servizi postali (p. es. uffici postali)	0,50
Amministrazione pubblica (p. es. Comuni)	0,33
Consulenza legale (p. es. studi legali e notarili)	0,33
Servizi finanziari (p. es. banche)	0,33

*L'UFSP si riserva espressamente il diritto di procedere a un adeguamento o ampliamento dei settori e dei fattori.

2.6 Attuazione / Pianificazione

D'intesa con l'OC, l'IdP comunica periodicamente (raccomandazione dell'UFSP: ogni tre mesi), sulla base di un modello di immissione e a una data di riferimento, il numero delle LRA per settore secondo il punto 2.5

a. che operano già come emittenti di SID,
b. che nel frattempo non operano più come emittenti di SID e
c. che prevedono di emettere SID nel periodo di pianificazione.

Il calcolo del numero di campioni (LRA) da esaminare per settore si basa sempre sul numero totale di LRA che in quel momento operano in ciascun settore. Anche negli anni degli audit di revisione il campione è sempre dimensionato sulla base del numero totale di LRA che in quel momento operano in ciascun settore.

Procedura di calcolo

1. Rilevare il numero di LRA per settore che rientrano nel campo di applicazione.
2. Moltiplicare il totale di ciascun settore per il fattore di ponderazione di cui al punto 2.5.
3. Estrarre la radice quadrata di questo risultato intermedio e moltiplicarla per il coefficiente di cui al punto 2.2.
4. Arrotondare per eccesso all'unità superiore il numero di campioni per settore. Si ottiene il numero totale di campioni per settore.
5. L'OC deve assicurare che il campione contenga almeno una LRA per settore.

Esempio di calcolo fittizio: nel campo di applicazione del primo audit di revisione di un IdP vi sono 1000 LRA operanti nel settore dei servizi postali. La dimensione del campione è calcolata come segue:

1. numero di LRA nel campo di applicazione per settore = 1000
2. 1000 x 0,5 = 500
3. 0,6 x $\sqrt{500} \approx 13{,}42$
4. dimensione del campione = 14
5. tutte le 14 LRA in questo settore devono soddisfare i requisiti di controllo, altrimenti tutti i Local Registration Offices con non conformità (NC) saranno sospesi.

Se un campione di LRA di un settore è stato sottoposto ad audit, tale settore è considerato auditato. Altre LRA dello stesso settore che si aggiungono nel corso dell'anno dopo l'avvenuta certificazione iniziale non sono sottoposte a un audit aggiuntivo.

Al momento del go-live della LRA devono essere soddisfatte le seguenti condizioni:

- tutti i dipendenti rilevanti per la LRA sono formati;
- l'attestato di formazione dei dipendenti rilevanti per la LRA è stato inoltrato per verifica all'OC;
- i controlli delegati dall'IdP alle LRA devono essere tassativamente garantiti dall'IdP per ogni organizzazione, a prescindere dal fatto che abbia avuto luogo un audit da parte dell'OC;
- la persona responsabile della formazione e la persona responsabile della sicurezza delle informazioni hanno confermato per scritto all'OC l'esito positivo dell'attuazione della formazione;
- le non conformità individuate dall'OC devono essere corrette ed eliminate dagli LRA Offices dopo ogni controllo obbligatorio;
- l'OC decide in merito all'approvazione dei LRA Offices dopo la stesura del rapporto di audit, nel quale sono documentate per scritto le NC riscontrate, le NC da correggere tassativamente e le NC da correggere nel prossimo futuro.

2.7 Glossario

Identity Provider (IdP)	Emittente di strumenti d'identificazione per la cartella informatizzata del paziente
Local Registration Authority (LRA)	Parti terze incaricate dall'IdP di emettere strumenti d'identificazione
Local Registration Authority Office (LRA Office)	Una di più sedi possibili di una LRA
Local Registration Officer mobile (LRAO mobile)	Persona dipendente di una LRA che può essere impiegata da quest'ultima in qualsiasi luogo, fermo restando che la LRA deve rappresentare una chiara struttura giuridica ed essere in grado di presentare un estratto del registro di commercio
Organismo di certificazione (OC)	Organismo di certificazione accreditato secondo la LCIP che esegue gli audit
Settore	= comparto; può essere costituito da una o più organizzazioni; si vedano anche i punti 2.4 e 2.5 per la determinazione e la ponderazione