Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Abteilung Digitale Transformation

Hilfestellung des Bundesamtes für Gesundheit (BAG)

Anhang 8 EPDV-EDI[1] – Präzisierung des Vorgehens im Zertifizierungsprozess nach EPDG[2]:

- Erhebung der Anzahl Stichproben
- Audits bei local registration authorities vor Ort

Ausgabe 1.0 vom 16. Februar 2022

Kontakt:

Lorena Kegel
Sektion Digitale Gesundheit
Bundesamt für Gesundheit
lorena.kegel@bag.admin.ch

[1] Verordnung des EDI über das elektronische Patientendossier (SR 816.111).
[2] Bundesgesetz über das elektronische Patientendossier (SR 816.1).

1 Ausgangslage

Im Zertifizierungsprozess definiert der Identity Provider (IdP) den Geltungsbereich der Zertifizierung nach EPDG. Im Geltungsbereich sind ebenfalls vom IdP beauftragte Dritte, sogenannte local registration authorities (LRA), die die Prüfung der Identität bei der Herausgabe der Identifikationsmittel (IDM) vornehmen. Dazu gehören auch mobile LRA Officer (mobile LRAO), die die Prüfung der Identität bei Herausgabe der IDM nicht an einem einzelnen Standort durchführen, sondern bei den Kunden vor Ort (bspw. in einer Gesundheitseinrichtung). Nach erfolgreicher Erstzertifizierung können weitere LRA in den Geltungsbereich aufgenommen werden.

LRA und deren mobile LRAO müssen folgende Anforderungen erfüllen:

- Die LRA, denen die mobilen LRAO angehören, stellen eine klare Rechtsstruktur dar.
- Der Handelsregisterauszug der LRA, denen die mobilen LRAO angehören, muss der Zertifizierungsstelle (ZS) zur Verfügung gestellt werden können.
- Der mobile LRAO muss seine Tätigkeit ausgehend von einem zertifizierten LRA Office ausführen können respektive eine Anstellung beim LRA Office haben. Einzelpersonen, die eine Einzelfirma darstellen, werden nicht akzeptiert.

Fiktives Beispiel für einen mobilen LRAO: Ein Postangestellter, der in einer Poststelle arbeitet, die bereits nach Anhang 8 EPDV-EDI zertifiziert ist, führt die Prüfung der Identität bei Herausgabe der IDM mobil durch.

Die Anzahl Stichproben der zu auditierenden LRA werden gemäss der Norm **IAF MD-1:2018 (MD1)** erhoben. Die Umsetzung der Stichprobenauswahl nach MD1 ist als Mindestanforderung zwingend. Im Rahmen dieser Norm hat das BAG als Schemaowner Präzisierungen in der Umsetzung definiert, welche die Anzahl Stichproben risikobasiert anpasst. Die Präzisierungen sollen sicherstellen, dass die Umsetzung gesamtschweizerisch durch alle ZS nach gleicher Vorgabe erfolgt und somit alle IdP gleich geprüft werden.

2 Berechnung der Anzahl Stichproben

2.1 Allgemein

Grundsätzlich sind alle LRA im Geltungsbereich der Zertifizierung und damit werden alle LRA für die Berechnung der Anzahl Stichproben herangezogen (siehe 2.2). Auch die mobilen LRAO sind Teil der Stichprobe und werden nicht separat gezählt. Eine wesentliche Voraussetzung für die Zertifizierung ist die Schulung der LRA zur Herausgabe von IDM. Die territoriale und organisatorische Struktur der Schulungen muss bei der Berechnung der Anzahl Stichproben einbezogen werden (siehe 2.3). Im Sinne des risikobasierten Ansatzes werden die LRA zudem nach Sektor unterschiedlich gewichtet und damit wird die Anzahl Stichproben gezielt entlang dem Risikopotenzial auf ein sinnvolles Mass reduziert (siehe 2.4 und 2.5).

2.2 Formel / Koeffizient

Der Umfang der Stichprobe y muss die Quadratwurzel der Anzahl Standorte sein: $y=\sqrt{x}$
x ist die Gesamtanzahl an Standorten.

Bei Erstzertifizierungen, jährlichen Wiederholungsaudits und Re-Zertifizierungen (= nach Ablauf der Gültigkeit des Zertifikats) wird das Ergebnis der Formel $y=\sqrt{x}$ mit folgendem Koeffizienten multipliziert:

	Koeffizient	**Formel**
Erstzertifizierung	1	$y=1.0\sqrt{x}$
1. Wiederholungsaudit	0.6	$y=0.6\sqrt{x}$
2. Wiederholungsaudit	0.6	$y=0.6\sqrt{x}$
Re-Zertifizierung	0.8	$y=0.8\sqrt{x}$

2.3 Risikoansatz

Die territoriale und organisatorische Struktur der LRA-Schulungen durch einen IdP wird von der ZS bei der Stichprobenauswahl berücksichtigt. Entsprechend verfährt die ZS zu Beginn der Audits mit einem 1:n-Ansatz, d.h. alle LRA im Geltungsbereich werden geprüft bis eine zufriedenstellende Beurteilung der Resultate aus den Audits erreicht wird. Wenn ein IdP seine LRA-Schulungen gesamtschweizerisch deckungsgleich ausrollt (z.B. für alle Poststellen) und dies in einer Selbstdeklaration festhält, kann von einer einheitlichen Qualität bei der Herausgabe eines IDM ausgegangen werden und direkt mit Ziffer 2.5 Gewichtung pro Sektor fortgefahren werden.

2.4 Herleitung des Sektors der LRA

Die Formel unter 2.2 wird separat für LRA in verschiedenen Sektoren angewendet. Die Einteilung der LRA erfolgt in Anlehnung an die allgemeine Systematik der Wirtschaftszweige des Bundesamtes für Statistik (NOGA 2008; https://www.kubb-tool.bfs.admin.ch/de). D.h. LRA, die im Handel tätig sind (z.B. Detailhandel) oder die Finanzdienstleistungen erbringen (z.B. Banken) sowie LRA in der Rechtsberatung, in der öffentlichen Verwaltung oder im Gesundheitswesen werden pro Sektor zusammengefasst und als Stichprobe zur Prüfung herangezogen.
Die Berechnung und Freigabe der Audits für einen Sektor sind pro IdP zu beurteilen, d.h. die Berechnung wird pro IdP berechnet und die vom IdP an den LRA delegierten Kontrollen für den spezifischen Geltungsbereich zugeordnet.

2.5 Gewichtung pro Sektor

Sektor gemäss Ziffer 2.3	**Faktor***
Detailhandel allgemein (z.B. Verkaufsstellen der Migros oder Coop)	1
Gesundheitseinrichtungen: Apotheken und Arztpraxen	0.60
Gesundheitseinrichtungen: Spitäler sowie Alters- und Pflegeheime	0.60
Postdienstleistungen (z.B. Poststellen)	0.50
Öffentliche Verwaltung (z.B. Gemeinden)	0.33
Rechtsberatung (z.B. Anwaltskanzleien, Notare)	0.33
Finanzdienstleistungen (z.B. Banken)	0.33

*Das BAG behält sich ausdrücklich vor, eine Anpassung respektive Erweiterung der Sektoren und Faktoren vorzunehmen.

2.6 Umsetzung / Planung

Der IdP meldet in Absprache mit der ZS auf Basis eines Eingabe-Templates periodisch (Empfehlung BAG: quartalsweise) an einem Stichtag die Anzahl LRA pro Sektor gemäss Ziffer 2.5, welche
a. bereits als Herausgeber von IDM tätig sind,
b. unterdessen nicht mehr als Herausgeber von IDM tätig sind und
c. die Herausgabe von IDM in der Planungsperiode vorsehen.

Die Berechnung der zu prüfenden Stichprobenmenge (LRA) pro Sektor erfolgt immer auf der aktuellen Gesamtanzahl LRA pro Sektor. Auch in den Jahren der Wiederholungsaudits wird immer die Bemessung auf die aktuelle Gesamtzahl LRA pro Sektor angesetzt.

Vorgehen für die Berechnung:
1. Die Anzahl LRA im Geltungsbereich wird pro Sektor erhoben.
2. Das Total pro Sektor wird mit der Gewichtung gemäss Ziffer 2.5 multipliziert.
3. Von diesem Zwischenergebnis wird die Wurzel gezogen und mit dem Koeffizienten nach Ziffer 2.2 multipliziert.
4. Die Anzahl Stichproben werden pro Sektor auf die nächsthöhere ganze Anzahl aufgerundet. Dies ergibt die Gesamtzahl Stichproben pro Sektor.
5. Es ist durch die ZS sicherzustellen, dass jeweils mindestens 1 LRA pro Sektor in der Stichprobe enthalten ist.

Fiktives Rechenbeispiel: Im Geltungsbereich für den 1. Wiederholungsaudit eines IdP befinden sich 1000 LRAs im Sektor Postdienstleistungen. Die Stichprobengrösse wird wie folgt berechnet:
1. Anzahl LRA im Geltungsbereich pro Sektor = 1000
2. 1000 x 0.5 = 500
3. 0.6 x $\sqrt{500} \approx 13.42$
4. Stichprobengrösse = 14
5. Alle 14 LRA in diesem Sektor müssen die Kontrollanforderungen erfüllen, ansonsten werden alle LRA Offices mit Nicht-Konformitäten (NC) suspendiert.

Wurde eine LRA Stichprobe aus einem Sektor auditiert, gilt dieser Sektor als geprüft. Weitere LRA, die unterjährig in demselben Sektor nach erfolgter Erstzertifizierung dazu stossen, werden nicht zusätzlich auditiert.

Zum Zeitpunkt des Go-Live der LRA müssen folgende Bedingungen erfüllt sein:
- Alle LRA-relevanten Mitarbeitenden sind geschult.
- Der Ausbildungsnachweis der LRA-relevanten Mitarbeitenden wurde an die ZS zur Prüfung eingereicht.
- Die vom IdP an den LRA delegierten Kontrollen sind bei jeder Organisation durch den IdP zwingend sicherzustellen, unabhängig ob ein Audit durch die ZS stattgefunden hat.
- Die ausbildungsverantwortliche Person und die Person, welche für die Informationssicherheit verantwortlich ist, haben der ZS schriftlich die erfolgreiche Umsetzung der Schulung bestätigt.
- Von der ZS gesichtete Nicht-Konformitäten müssen von den LRA Offices über alle zwingend geforderten Kontrollen verbessert und umgesetzt sein.
- Die ZS entscheidet über die Freigabe der LRA Offices nach der Erstellung des Audit-Berichtes, in dem schriftlich festgehalten wird, welche NC es gibt, welche NC zwingend umzusetzen sind und welche NC für die nahe Zukunft terminiert werden können.

2.7 Glossar

Identity Provider (IdP)	Herausgeber von Identifikationsmitteln für das elektronische Patientendossier
Local Registration Authority (LRA)	Vom IdP beauftragte Dritte zur Herausgabe von Identifikationsmitteln
Local Registration Authority Office (LRA Office)	Einer von mehreren möglichen Standorten eines LRA
Mobile Local Registration Officer (mobile LRAO)	Ortsunabhängig einsetzbare Person, die mit der LRA in einem Angestelltenverhältnis steht, wobei die LRA eine klare Rechtsstruktur darstellen und einen Handelsregisterauszug vorlegen können
Sektor	= Branche; kann aus einer oder mehreren Organisationen bestehen; siehe auch Ziffer 2.4 und 2.5 für die Herleitung und Gewichtung
Zertifizierungsstelle (ZS)	Nach EPDG akkreditierte Zertifizierungsstelle, die die Audits durchführt