Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la santé publique OFSP
Division Transformation numérique

Aide de l'Office fédéral de la santé publique (OFSP)

Annexe 8 de l'ODEP-DFI[1] – Précision de la procédure dans le cadre de la certification selon la LDEP[2] :

- Relevé du nombre d'échantillonnages
- Audits sur place des Local Registration Authorities

Édition 1.0 du 16 février 2022

Contact :

Lorena Kegel
Section Santé numérique
Office fédéral de la santé publique
lorena.kegel@bag.admin.ch

[1] Ordonnance du DFI sur le dossier électronique du patient (RS 816.111)
[2] Loi fédérale sur le dossier électronique du patient (RS 816.1).

1 Contexte

Dans le cadre de la certification, l'Identity Provider (IdP) définit le champ d'application de la certification selon la LDEP. Ce dernier s'étend aux tiers mandatés par l'IdP, désignés sous le nom de Local Registration Authorities (LRA), qui procèdent à la vérification de l'identité lors de la délivrance des moyens d'identification. Il inclut également les LRA Officer mobiles (LRAO mobiles), qui effectuent la vérification de l'identité lors de la délivrance des moyens d'identification sur place, chez les clients (p. ex. dans un établissement de santé). Après une première certification réussie, d'autres LRA peuvent être incluses dans le champ d'application.

Les LRA et leurs LRAO mobiles doivent répondre aux exigences suivantes :

- Les LRA auxquelles les LRAO mobiles sont rattachés constituent une structure juridique claire.
- L'extrait du registre du commerce des LRA auxquelles les LRAO mobiles sont rattachés doit pouvoir être mis à disposition de l'organisme de certification (OC).
- Le LRAO mobile doit pouvoir exercer son activité depuis un LRA Office certifié ou être employé par le LRA Office. Les personnes représentant une entreprise en particulier ne sont pas acceptées.

Exemple de LRAO mobile : un employé de la Poste qui travaille dans un bureau de poste déjà certifié selon l'annexe 8 de l'ODEP-DFI effectue la vérification de l'identité de manière mobile lors de la délivrance des moyens d'identification.

Le nombre d'échantillonnages des LRA à auditer est relevé conformément à la norme **IAF MD-1:2018 (MD1)**. Il est impératif, à titre d'exigence minimale, de sélectionner les échantillonnages selon la norme MD1. Dans le cadre de cette norme, l'OFSP, en sa qualité de propriétaire du schéma, a défini des précisions au niveau de la mise en œuvre, lesquelles adaptent le nombre d'échantillonnages en fonction des risques. Ces précisions visent à garantir que tous les OC de Suisse se conforment aux mêmes règles de mise en œuvre et qu'ainsi, tous les IdP soient contrôlés de la même manière.

2 Calcul du nombre d'échantillonnages

2.1 Remarques générales

De manière générale, toutes les LRA sont incluses dans le champ d'application de la certification et, par conséquent, toutes sont prises en compte dans le calcul du nombre d'échantillonnages (cf. 2.2). Les LRAO mobiles font également partie de l'échantillonnage et ne sont pas comptés à part. La formation des LRA à la délivrance des moyens d'identification est une condition essentielle de la certification. La structure territoriale et organisationnelle des formations doit être prise en compte dans le calcul du nombre d'échantillonnages (cf. 2.3). De plus, conformément à l'approche fondée sur les risques, les LRA sont pondérées différemment en fonction du secteur concerné. Les échantillonnages s'en trouvent ainsi réduits à un nombre raisonnable, de manière ciblée et en fonction du potentiel de risques (cf. 2.4 et 2.5).

2.2 Formule / coefficient

La taille de l'échantillonnage y doit être la racine carrée du nombre de sites : $y=\sqrt{x}$, où x représente le nombre total de sites.

S’agissant de premières certifications, d’audits de renouvellement annuels et de re-certifications (= après échéance de la validité du certificat), le résultat de la formule $y=\sqrt{x}$ est multiplié par les coefficients suivants :

	Coefficient	**Formule**
Première certification	1	$y=1.0\sqrt{x}$
1er audit de renouvellement	0.6	$y=0.6\sqrt{x}$
2e audit de renouvellement	0.6	$y=0.6\sqrt{x}$
Re-certification	0.8	$y=0.8\sqrt{x}$

2.3 Approche fondée sur les risques

La structure territoriale et organisationnelle des formations des LRA dispensées par un IdP est prise en compte par l’OC lors de la sélection des échantillonnages. Au début des audits, l’OC adopte par conséquent une approche 1:n, ce qui signifie que toutes les LRA du champ d’application sont contrôlées jusqu’à obtention d’une évaluation satisfaisante des résultats des audits. Lorsqu’un IdP dispense ses cours de formation destinés aux LRA de la même manière dans toute la Suisse (p. ex. pour tous les bureaux de poste) et consigne cela dans une autodéclaration, on considère qu’il y a qualité uniforme dans la délivrance des moyens d’identification, et il est possible de passer directement au ch. 2.5 Pondération par secteur.

2.4 Détermination du secteur des LRA

La formule énoncée au ch. 2.2 est appliquée séparément aux LRA de différents secteurs. La classification des LRA est fondée sur la nomenclature générale des activités économiques de l’Office fédéral de la statistique (NOGA 2008 ; https://www.kubb-tool.bfs.admin.ch/fr). Cela signifie que les LRA qui sont actives dans le commerce (p. ex. le commerce de détail) ou offrent des services financiers (p. ex. les banques) et les LRA actives dans le conseil juridique, l’administration publique ou la santé sont regroupées par secteur et utilisées comme échantillon pour le contrôle.
Le calcul et la validation des audits pour un secteur doivent être évalués séparément pour chaque IdP. Autrement dit, le calcul est effectué par IdP et les contrôles délégués par l’IdP aux LRA sont attribués au champ d’application spécifique.

2.5 Pondération par secteur

Secteur selon le ch. 2.3	**Facteur***
Commerce de détail en général (p. ex. points de vente Migros ou Coop)	1
Structures de santé : pharmacies et cabinets médicaux	0.60
Établissements de santé : hôpitaux et établissements médico-sociaux	0.60
Services postaux (p. ex. bureaux de poste)	0.50
Administration publique (p. ex. communes)	0.33
Conseil juridique (p. ex. cabinets d’avocats, notaires)	0.33
Services financiers (p. ex. banques)	0.33

* L’OFSP se réserve expressément la possibilité d’adapter ou d’étendre les secteurs et les facteurs.

2.6 Mise en œuvre / planification

Après entente avec l'OC, l'IdP communique périodiquement sur la base d'un modèle de saisie (recommandation de l'OFSP : tous les trimestres) à une date de référence le nombre de LRA par secteur (conformément au ch. 2.5) :

a. qui délivrent déjà des moyens d'identification,
b. qui ne délivrent plus de moyens d'identification, et
c. qui prévoient de délivrer des moyens d'identification pendant la période de planification.

Le nombre d'échantillonnages à contrôler (LRA) par secteur se calcule toujours sur la base du nombre actuel total de LRA par secteur. Cette règle s'applique également les années où ont lieu les audits de renouvellement.

Marche à suivre pour le calcul :

1. Relever le nombre de LRA du champ d'application par secteur.
2. Multiplier le total de chaque secteur par la pondération conformément au ch. 2.5.
3. Déterminer la racine carrée de ce résultat intermédiaire et la multiplier par le coefficient indiqué au ch. 2.2.
4. Arrondir le nombre d'échantillonnages par secteur au nombre entier supérieur. On obtient ainsi le nombre total d'échantillonnages par secteur.
5. L'OC doit s'assurer qu'au moins une LRA par secteur est incluse dans l'échantillonnage.

Exemple de calcul : le champ d'application du premier audit de renouvellement d'un IdP comprend 1000 LRA dans le secteur des services postaux. La taille des échantillonnages est calculée de la manière suivante :

1. Nombre de LRA dans le champ d'application par secteur = 1000
2. 1000 x 0.5 = 500
3. 0.6 x $\sqrt{500} \approx 13.42$
4. Taille des échantillonnages = 14
5. Les 14 LRA de ce secteur doivent satisfaire aux exigences du contrôle, faute de quoi tous les LRA Offices présentant des non-conformités (NC) sont suspendus.

Si une LRA constituant l'échantillonnage d'un secteur a été audité, ce secteur est considéré comme audité. Les autres LRA qui rejoignent le même secteur en cours d'année après avoir obtenu leur première certification ne sont pas soumises à un audit supplémentaire.

Les conditions suivantes doivent être remplies au moment du lancement de la LRA :

- Tous les collaborateurs effectuant des tâches relevant de la LRA sont formés.
- L'attestation de formation de ces collaborateurs a été envoyée à l'OC pour vérification.
- Les contrôles délégués par l'IdP aux LRA doivent impérativement être garantis par l'IdP auprès de chaque organisation, indépendamment du fait qu'un audit ait été effectué par l'OC.
- La personne responsable de la formation et celle responsable de la sécurité des informations ont confirmé par écrit à l'OC que la formation avait été réalisée avec succès.
- Les NC identifiées par l'OC doivent être améliorées et les améliorations implémentées par les LRA Offices pour tous les contrôles impératifs.
- L'OC décide de la validation des LRA Offices après l'établissement du rapport d'audit, dans lequel sont consignés par écrit les NC constatées, les améliorations des NC à implémenter impérativement et celles à prévoir dans un avenir proche.

2.7 Glossaire

Identity Provider (IdP)	Délivreur de moyens d'identification pour le dossier électronique du patient.
Local Registration Authority (LRA)	Tiers mandatés par l'IdP en vue de la délivrance de moyens d'identification.
Local Registration Authority Office (LRA Office)	L'un des sites possibles d'une LRA.
Mobile Local Registration Officer (mobile LRAO)	Personne effectuant des interventions en dehors d'un lieu fixe pour le compte de la LRA, celle-ci présentant une structure juridique claire et pouvant fournir un extrait du registre du commerce.
Organisme de certification (OC)	Organisme de certification reconnu au sens de la LDEP, qui effectue les audits.
Secteur	= branche ; un secteur peut être constitué d'une ou de plusieurs organisations ; voir aussi les ch. 2.4 et 2.5 pour la détermination et la pondération.