

Part 11 Compliance Questionnaire

Published date: July 29, 2026

Last updated: August 29, 2026

Policy owner: Anatoly Geyfman

Version: 1.1

Classification: Confidential

This checklist is completed during Validation Execution for any system that handles electronic records or applies electronic signatures. Each item is answered Yes / No / N/A, with the evidence reference (test case ID, screenshot, configuration item) and a comment.

#	Topic	Question	Reference	Deviceflow Position
1	System validation	Has the system itself been validated for its intended use?	Part 11 §11.10(a); Annex 11 §4	Yes, see validation website
2	Record retrieval	Can records be accurately and readily retrieved throughout the retention period, in human-readable and electronic form?	Part 11 §11.10(b); Annex 11 §7	Yes, see URS-034
3	Record protection	Are records protected from unauthorized alteration or deletion?	Part 11 §11.10(c)	Yes

4	Access control	Is system access limited to authorized individuals, with unique accounts?	Part 11 §11.10(d), (g); Annex 11 §12	Yes, see URS-001
5	Audit trail	Is a secure, computer-generated, time-stamped audit trail enabled, retained, and reviewable?	Part 11 §11.10(e); Annex 11 §9	Yes, see URS-003
6	Operational checks	Are operational checks in place to enforce sequencing of steps and events?	Part 11 §11.10(f)	Yes, see URS-010
7	Authority checks	Are authority checks in place to ensure only authorized individuals can use the system, sign records, or alter records?	Part 11 §11.10(g)	Yes, see URS-002, URS-005, URS-008, URS-055. A signing code can only be requested, verified, or spent by the rep the certification is actually assigned to – mirroring the gate on completion itself.
8	Device checks	Are device checks in place to ensure validity of the	Part 11 §11.10(h)	Yes, see URS-021

		source of data input or operational instructions?		
9	Training and qualification	Are persons developing, maintaining, or using the system qualified and trained?	Part 11 §11.10(i); Annex 11 §2	Yes, see SDLC and Vendor Questionnaire for more info
10	E-signature uniqueness	Is each electronic signature unique to one individual and not reused or reassigned?	Part 11 §11.200; Annex 11 §14	Yes, see URS-001 . The one-time signing code is single-use per (rep, certification, etc) — requesting a new code supersedes any prior live one, and a consumed code can never authorize a second signature.
11	E-signature components	Does the e-signature include at least two distinct identification components (e.g., user ID + password)?	Part 11 §11.200	Yes, see URS-001 . Beyond the login session (first component), certification signing now requires a one-time code — delivered by email and, where

				available, SMS — verified immediately before the completion signature is recorded (second component). This satisfies §11.200(a)(1) at the point of signature execution, not only at session login.
12	E-signature binding	Are electronic signatures permanently linked to their respective records?	Part 11 §11.70	Yes, see URS-003. A cryptographic payload (Signatures.signedPayloadSha256) is computed from a canonical serialization of the signature's key fields (certification, version, executed-at, form submission, meaning, record id, signer, drawn-mark hash) before the record row exists, so the signature

				and its record re-verify from stored data alone.
13	Session management	Does the system enforce session timeout / lockout after inactivity?	Annex 11 §12	Yes, after 7 days of inactivity
14	Backup & recovery	Are backup, restoration, and disaster-recovery procedures defined and periodically tested?	Annex 11 §7.2	Yes, see vendor questionnaire
15	Time-stamp integrity	Is the system clock synchronized to a reliable time source, and are time-stamps tamper-resistant?	Annex 11 §9	Yes

Attestation

I attest that the information provided in this document is accurate and complete to the best of my knowledge.

Field	Value
Name	Anatoly Geyfman
Title	CEO

Signature	
Date	08/29/2026

Document revision history

Version	Date	Author	Description
1.0	July 29, 2026	Anatoly Geyfman	Initial version
1.1	August 29, 2026	Anatoly Geyfman	Updated Part 11 signature requirements to match current capabilities