

Telemedicine Standards — Full Guidance

Complete criterion-by-criterion guidance: worked examples, first steps, common mistakes, implementation plans, and Monitor verification methods for all 45 criteria.

8 standards · 45 criteria · Version 3.0

ASF STANDARDS · TELEMEDICINE · STANDARD 6

Standard 6 — Data Privacy & Patient Confidentiality

5 criteria · 5 non-negotiable · 0 core · Version 3.0

CRITERIA IN THIS STANDARD

6.1 — The Patient's Session Environment Is Actively Addressed

6.2 — A Third Party Present But Unseen Is Genuinely Disclosed and Consented To

6.3 — Session Recording Follows a Clear, Specific Policy

6.4 — The Provider's Own Home Office Meets the Same Privacy Standard

6.5 — Substance Use Disorder Records Follow the Heightened, Distinct Confidentiality Standard

6.1 The Patient's Session Environment Is Actively Addressed

NON-NEGOTIABLE

The patient's session environment is genuinely, actively addressed at the start of care — specific guidance on finding a private location, practical suggestions when home isn't quiet or private — not simply assumed private because the patient is participating from their own device.

In plain terms: At the start of care, the patient is told how to make their session private — a room with a door, headphones, no one listening — and the provider checks each time.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

The patient joins from the kitchen with children present. From the car park at work. From a shared bedroom. A mental health session, a discussion of an STI, a domestic violence disclosure — none can happen safely in those settings. The service must give guidance at intake (a private room, a closed door, headphones, a signal if someone enters) and the provider must check at each session ('Are you somewhere private? Can anyone hear?'). If not, the session is deferred or limited to non-sensitive content. Privacy is the patient's right and the provider's responsibility to protect.

WHAT GOOD LOOKS LIKE

- Patients are genuinely, proactively guided on finding a private location.
- Concrete alternatives are offered when home isn't private or quiet.
- Attention to environment is genuinely calibrated to visit sensitivity.

COMMON FAILURE MODES

- Environment privacy is assumed adequate without any active guidance.
- No alternatives are offered for patients without a private home space.
- Environment receives the same minimal attention regardless of topic sensitivity.

WORKED EXAMPLE

IN PRACTICE

A telemedicine mental health service.

BEFORE

No guidance was given. Providers noticed background voices, children, and open-plan settings but proceeded. A patient disclosed abuse in a session her abuser overheard from the next room.

ACTION

Intake materials now include a one-page privacy guide: a private room with a closed door, headphones, a 'do not disturb' arrangement, a hand signal if privacy is lost. Every session begins with 'Are you somewhere private? Can anyone hear or see?' and the answer is recorded. If not private, the provider offers to reschedule or limits the session. Alternative private locations (a car, a community centre room, the service's partner sites) are suggested for patients without one.

AFTER

The Monitor reviewed the intake guide, 40 session notes with privacy confirmation, and 5 sessions rescheduled for privacy. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Write a one-page privacy guide for patients.
2. Script the check: 'Are you somewhere private?'
3. Record the answer every session.
4. Reschedule if not private.

The most common mistake: Noticing the patient is not in private and proceeding anyway.

SELF-ASSESSMENT QUESTIONS

1. Is the patient genuinely, proactively guided on finding a private location for their session, not left to figure this out alone? — *Real, active guidance, not an assumption the patient will independently find privacy.*

Evidence: Patient environment guidance materials

2. Are practical alternatives offered when a patient's home genuinely isn't private or quiet? — *Real, concrete alternative suggestions, not guidance limited to an assumed-available private home space.*

Evidence: N/A — tested directly

3. Is environment addressed specifically for sensitive topics, not treated as equally important for every visit type? — *Genuine, calibrated attention reflecting the real sensitivity of what will actually be*

discussed.

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **Guidance exists in intake materials but isn't reinforced verbally at the start of an actual session.** — Real, active reinforcement at the point of use is more reliable than guidance provided once and easily forgotten.
- **Alternatives are suggested generally but not tailored to what's realistically available to a specific patient's circumstances.** — Genuine, practical guidance should reflect what's actually feasible for the individual patient, not a generic list.
- **Environment is addressed for new patients but not consistently revisited for established, ongoing patients.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current patient environment guidance for genuine specificity and practicality.
Week 2	Build concrete alternative suggestions for patients without a private home space.
Week 3	Reinforce environment guidance verbally at the start of sessions, not intake materials alone.
Ongoing	Revisit environment guidance periodically for established patients.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Guidance materials review	Reviews actual patient-facing materials for genuine, specific environment guidance.
OBSERVE	Session opening observation	Observes whether environment is genuinely addressed at the start of an actual session.
DOCUMENT	Sensitivity calibration review	Reviews whether environment attention is genuinely calibrated to the sensitivity of the visit.

SUPERVISOR TIPS

- **Ask a patient whether they were given any specific guidance on finding a private location.** — A specific, real answer reveals genuine practice, not an assumption of adequate guidance.
- **Observe an actual session opening for genuine environment discussion.** — Direct observation reveals whether this happens in practice, not just in intake documentation.

EVIDENCE BASE

[26] Official telehealth guidance specifically advises patients to find a private location for their session and provides concrete suggestions — a quiet room at home, a private space in a community setting, a parked car — reflecting that session environment privacy requires active guidance, not assumed adequacy from platform security alone.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

6.2 **A Third Party Present But Unseen Is Genuinely Disclosed and Consented To**

NON-NEGOTIABLE

When someone other than the patient is present during a session — visible or not — this is genuinely disclosed, and specific consent is obtained before discussing sensitive information, particularly when the patient is in a public location where the conversation could be overheard.

In plain terms: If anyone other than the patient is in the room — visible or not — the provider knows, the patient has agreed, and it is recorded. No hidden listeners.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

A family member sitting off-camera, a partner in the next room, a carer 'just helping' — each is a third party to a confidential consultation. The patient may not feel free to speak; the provider may not know who is listening; consent is compromised. The rule: the provider asks who is present at the start of every session; anyone present is named and the patient confirms consent to their presence; the presence and consent are recorded; the patient can ask them to leave at any point. For sensitive topics, the provider may ask to speak to the patient alone. A hidden listener is a breach the patient did not agree to.

WHAT GOOD LOOKS LIKE

- Providers genuinely, actively ask whether anyone else is present.
- Specific, documented consent is genuinely obtained when a third party is present.
- Public location risk is genuinely, actively addressed before continuing.

COMMON FAILURE MODES

- Providers assume the patient is alone based only on what's visible on screen.
- Consent for third-party presence isn't genuinely obtained or documented.
- A patient's apparently public location isn't addressed before continuing with sensitive topics.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service where third-party presence was not addressed.

BEFORE

Providers sometimes heard other voices or saw movement off-camera. They did not ask. A patient discussing a psychiatric medication was later found to have had her employer's HR representative present at her request — but the provider had not known and had not confirmed it was her choice.

ACTION

Every session begins with: 'Is anyone else in the room or able to hear us? Do you want them to be present?' Anyone present is named in the session note with the patient's consent recorded.

Providers are trained to ask for a private word with the patient at any point. Patients are told at intake that they can have a support person present but must say so.

AFTER

The Monitor reviewed 40 session notes with third-party disclosure recorded (8 with named support persons and consent). Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Add 'Who else is present?' to the session opening script.
2. Record every third party and the patient's consent.
3. Train providers to ask for a private word when needed.
4. Tell patients the rule at intake.

The most common mistake: Hearing another voice and not asking who it is.

SELF-ASSESSMENT QUESTIONS

1. Are providers genuinely trained to actively ask whether anyone else is present, not assuming the patient is alone? — *Real, active inquiry, not an assumption based on who's visible on screen.*

Evidence: Provider training on third-party presence inquiry

2. Is specific consent genuinely obtained and documented before discussing sensitive information with a third party present? — *Real, documented consent, not proceeding without confirming the patient is comfortable being overheard.*

Evidence: Third-party presence consent documentation

3. When a patient is in a public location, does the provider genuinely address this before continuing with sensitive topics? — *Real, active address of the public-location risk, not proceeding as though the setting were private.*

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **Inquiry happens for new patients but isn't consistently repeated for established, ongoing patients.** — An established patient's actual circumstances at a given session can genuinely differ from prior visits.

- **Consent is obtained verbally but not consistently documented in a genuinely retrievable way.** — Documented consent provides more reliable, real evidence than a verbal exchange alone.
- **Public location risk is addressed when obviously apparent but not consistently for more ambiguous settings.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current practice for genuine inquiry about third-party presence at session start.
Week 2	Train providers to actively ask and document consent when a third party is present.
Week 3	Build specific guidance for addressing apparently public patient locations.
Ongoing	Extend genuine, repeated inquiry to established, ongoing patients.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
OBSERVE	Third-party inquiry observation	Observes an actual session opening for genuine, active inquiry about anyone else present.
DOCUMENT	Consent documentation review	Reviews records for genuine, documented consent when a third party is present.
OBSERVE	Public location handling observation	Observes how a provider genuinely addresses a patient joining from an apparently public location.

SUPERVISOR TIPS

- **Observe an actual session opening for genuine inquiry about who else might be present.** — Direct observation reveals whether this genuinely happens, not an assumption based on stated policy.
- **Ask to see documented consent for a real case where a third party was present.** — A real, specific record reveals genuine practice, not policy language alone.

EVIDENCE BASE

[27] Established health privacy guidance specifically requires recorded consent before continuing a consultation when a translator, caregiver, or family member is present, or when the patient is in a public location where the conversation may be overheard, reflecting the genuine risk of an unseen third party during a telehealth session.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

6.3 Session Recording Follows a Clear, Specific Policy

NON-NEGOTIABLE

Session recording follows a clear, specific, documented policy — whether recording ever occurs, under what circumstances, where recordings are stored, and how long they're retained — not left ambiguous, given real, documented gaps in this area leave both providers and patients genuinely uncertain and uncomfortable.

In plain terms: There is a written policy on whether sessions are ever recorded, when, by whom, with what consent, how stored, and who can access — and it is followed. Patients are told.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

A recorded consultation is a permanent record of the most private conversation a person may have. Recording without consent is illegal in many jurisdictions and unethical everywhere. Recording with consent creates obligations: secure storage, defined retention, controlled access, and the patient's right to a copy or deletion. The policy may be 'never'; that is legitimate and simple. If recording is permitted for any purpose — quality, training, clinical — every element

must be specified, consent must be explicit and revocable, and the platform's own recording settings must match the policy. Patients must also be told that they may not record without consent.

WHAT GOOD LOOKS LIKE

- A clear, specific, documented recording policy genuinely exists.
- The policy specifically addresses storage location and retention duration.
- Patients are genuinely, specifically informed about recording before it happens.

COMMON FAILURE MODES

- No clear policy exists; practice is left to individual provider discretion.
- The policy is silent on storage location or retention duration.
- Recording occurs without the patient's genuine, prior knowledge.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service whose video platform had recording enabled by default.

BEFORE

Sessions were being recorded automatically to the vendor's cloud. Nobody had decided this; it was the default setting. Patients did not know. Nobody knew who could access the recordings or how long they were kept.

ACTION

The service decided: no routine recording. The platform's recording was disabled at the admin level. A written policy states recording occurs only for defined clinical purposes with the patient's explicit written consent per recording, stored in the encrypted record system, retained per the records policy, accessible to the treating clinician only. Patients are told at intake that sessions are not recorded and that they may not record. Historical recordings were deleted with documentation.

AFTER

The Monitor reviewed the policy, the platform's admin settings (recording disabled), intake

materials, and the deletion record. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Check your platform's recording settings right now.
2. Decide: never, or under what exact conditions?
3. Write the policy and configure the platform to match.
4. Tell patients.

The most common mistake: Not knowing whether the platform is recording — check the default.

SELF-ASSESSMENT QUESTIONS

1. Does the service have a clear, specific, documented policy on whether and when sessions are recorded? — *A real, specific written policy, not ambiguity left for individual providers to navigate independently.*

Evidence: Session recording policy documentation

2. Does this policy genuinely address storage location and retention duration for any recordings that are made? — *Real, specific storage and retention detail, not a policy silent on what happens to a recording after the session.*

Evidence: N/A — tested directly

3. Are patients genuinely, specifically informed whether their session is being recorded, before it happens? — *Real, prior, specific notification, not recording occurring without the patient's genuine knowledge.*

Evidence: Patient recording notification record

COMMON REASONS FOR A PARTIAL ANSWER

- **A policy exists for standard consultations but isn't specifically addressed for group or family sessions.** — Every session type deserves the same genuine policy clarity, not standard consultations alone.
- **Storage location is specified but retention duration isn't clearly, specifically defined.** — Both elements genuinely matter to a patient's real understanding of what happens to their recorded information.
- **Notification happens but isn't consistently documented as genuinely occurring before recording begins.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current recording practice for genuine, specific policy clarity.
Week 2	Build a clear, documented policy addressing whether, when, storage, and retention.
Week 3	Establish consistent, documented patient notification before any recording.
Ongoing	Extend policy clarity to all session types, not standard consultations alone.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Policy documentation review	Reviews the actual, specific, documented recording policy.
DOCUMENT	Storage and retention review	Reviews whether the policy specifically addresses storage location and retention duration.
OBSERVE	Patient notification observation	Observes whether patients are genuinely, specifically informed about recording before it occurs.

SUPERVISOR TIPS

- **Ask to see the actual, written recording policy, not a general assurance recording is handled appropriately.** — A specific, real document reveals genuine clarity, not assumed adequacy.
- **Ask a provider directly what the specific retention period is for a session recording.** — A specific, confident answer reveals genuine, clear policy, not individual discretion.

EVIDENCE BASE

[28] Practitioners often lack clear guidance on whether and how to record telehealth sessions, creating genuine ambiguity and discomfort for both provider and patient, establishing a clear, specific, documented recording policy as necessary to close this documented gap.

[ASF training courses on GMJ Academy →](#)

6.4 The Provider's Own Home Office Meets the Same Privacy Standard

NON-NEGOTIABLE

A provider conducting sessions from a home office genuinely meets the same privacy and security standard as a clinical setting would — device encryption, a secure network, genuine physical privacy from others in the household — not treated as a lower-scrutiny environment simply because it's the provider's own home.

In plain terms: A provider working from home has a private room, a secure device, a secure network, no one who can overhear, and the same data protection as an office — verified, not assumed.

Facility category	Crisis	Transition	Small	Standard
Applicability	Adapted	Full	Full	Full

WHY THIS MATTERS

The provider joins from the kitchen table while family passes through. Their laptop is shared with a teenager. The Wi-Fi is the neighbour's. Papers with patient names are on the desk. The home office is the weakest link in telemedicine security and the least examined. The standard is the same as a clinical office: a private room with a closed door; a work-only device with encryption and MFA; a secure network (not public Wi-Fi, ideally VPN); no patient information visible or audible to others; a clean desk; a screen lock. The service verifies this — by attestation at minimum, by inspection where practical — and provides what the provider needs.

WHAT GOOD LOOKS LIKE

- Provider devices are genuinely, verifiably encrypted.

COMMON FAILURE MODES

- Device encryption is assumed adequate without genuine verification.

- Home network security is genuinely, specifically verified.
- Providers genuinely have real physical privacy during sessions.

- Home network security is unexamined, not specifically verified.
- Physical privacy is assumed from a designated space without genuine confirmation.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service with 12 providers all working from home.

BEFORE	Providers used their own laptops, some shared with family. Two worked from shared living spaces. One used a cafe's Wi-Fi occasionally. No standard existed; no verification was done. A provider's child appeared on camera during a session and could be heard commenting.
ACTION	A home office standard was written with the same requirements as the clinical office. The service issued managed work devices with encryption, MFA, and remote wipe. A VPN is mandatory. Each provider completed a home office self-assessment and a video walkthrough with the compliance lead. Non-compliant setups were remediated (a door lock, a privacy screen, a headset). Annual re-attestation.
AFTER	The Monitor reviewed the standard, 12 completed self-assessments with walkthrough sign-off, the device management record, and the VPN enforcement configuration. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Ask each provider: private room? Work-only device? Secure network? Anyone who can overhear?
2. Write the home office standard.
3. Issue managed devices and require VPN.
4. Verify each setup by video walkthrough.

The most common mistake: Assuming the provider's home is as secure as the office because the provider is a professional.

SELF-ASSESSMENT QUESTIONS

1. Is the provider's device for conducting sessions genuinely encrypted, not assumed adequate without verification? — *Real, verified device encryption, not an assumption based on the device being personally owned and trusted.*

Evidence: Provider device encryption verification

2. Is the provider's home network genuinely secure, specifically verified, not assumed adequate? — *Real, verified network security, not an unexamined assumption about home network safety.*

Evidence: Home network security verification

3. Does the provider genuinely have physical privacy from others in the household during a session? — *Real, verified physical privacy, not an assumption based on having a designated home office space.*

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **Device encryption is verified for provider-issued equipment but not for personally owned devices also used for sessions.** — Every device genuinely used to access patient information deserves the same verification, regardless of ownership.
- **Network security is addressed at initial setup but not periodically reconfirmed as home network configurations can change.** — A home network's real security can change over time, and periodic reconfirmation reflects this reality.
- **Physical privacy is generally adequate but hasn't been specifically confirmed for providers sharing a household with others working or studying at home.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current home office privacy and security for genuine verification versus assumed adequacy.
Week 2	Verify encryption for every device genuinely used to conduct sessions, regardless of ownership.
Week 3	Confirm home network security and genuine physical privacy for every provider.

When	What
Ongoing	Periodically reconfirm home office security as configurations may change.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Device encryption review	Reviews evidence of genuine, verified encryption for devices used to conduct sessions.
DOCUMENT	Network security review	Reviews evidence of genuine, verified home network security.
ASK	Physical privacy interview	Asks a provider to describe their actual physical privacy setup during sessions.

SUPERVISOR TIPS

- **Ask a provider to describe their actual home office setup, including device and network security.** — A specific, confident answer reveals genuine attention, not an assumption of adequacy.
- **Ask specifically about physical privacy for a provider sharing a household with others.** — This reveals whether genuine privacy has been confirmed, not assumed from a general home office description.

EVIDENCE BASE

[29] Many clinicians continue conducting sessions from home offices with unencrypted devices and storing session recordings in personal cloud storage, having never completed the compliance transition required since temporary pandemic-era enforcement discretion ended, establishing the provider's home office as a genuine, distinct privacy compliance layer separate from platform security.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

6.5 Substance Use Disorder Records Follow the Heightened, Distinct Confidentiality Standard

NON-NEGOTIABLE

Records related to substance use disorder treatment genuinely follow the specific, heightened confidentiality standard that applies to them — requiring the patient's own written consent for disclosure — not treated identically to general health information under standard confidentiality practice.

In plain terms: Records of substance use disorder treatment follow the separate, stricter confidentiality rules that apply to them — separate consent, restricted sharing, no disclosure without specific authorisation.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Adapted	Full

WHY THIS MATTERS

In many jurisdictions, substance use disorder treatment records have a higher confidentiality standard than general health records (42 CFR Part 2 in the US, equivalents elsewhere): they cannot be shared even with other treating providers without specific written consent; they cannot be used in legal proceedings without a court order; they must be segregated or flagged; breaches carry distinct penalties. A telemedicine service that stores SUD records alongside general records with the same access and sharing rules is violating the higher standard. The service must know the rule, identify SUD records, and apply the stricter regime.

WHAT GOOD LOOKS LIKE

- Substance use disorder records genuinely follow the specific, heightened standard.
- Disclosure is genuinely based on the patient's own specific written consent.
- Staff are specifically trained on this distinct standard, not assuming general practice suffices.

COMMON FAILURE MODES

- These records are treated identically to general health information.
- Disclosure relies on a general release, not specific written consent for this category.
- Staff aren't specifically trained; general health privacy knowledge is assumed sufficient.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service providing addiction treatment alongside general mental health.

BEFORE	SUD treatment records were in the same system with the same access as all records. Records had been shared with primary care providers under the general consent. Staff were unaware of the distinct standard.
ACTION	The compliance lead identified the applicable SUD confidentiality regulation. SUD records were flagged in the system with restricted access to the treating team. A separate SUD-specific consent form was introduced for any disclosure, naming the recipient and purpose. Disclosures without it are blocked. Staff completed training on the distinct standard. Historical disclosures were reviewed and patients notified where required.
AFTER	The Monitor reviewed the flagged record configuration, the SUD-specific consent form, training records, and the disclosure log with specific consents. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Find the SUD confidentiality regulation for your jurisdiction.
2. Identify and flag every SUD treatment record.
3. Introduce a separate SUD disclosure consent.
4. Train staff on the difference.

The most common mistake: Sharing SUD records under the general health consent — SUD records need their own.

SELF-ASSESSMENT QUESTIONS

1. Do substance use disorder records genuinely follow this distinct, heightened confidentiality standard? — *Real adherence to this distinct*

standard, not treated identically to general health information.

Evidence: SUD-specific confidentiality protocol documentation

2. Is disclosure genuinely based on the patient's own specific written consent, not a general release? — *Real, specific written consent for this category, not a general release assumed sufficient.*

Evidence: Patient written consent for SUD record disclosure

3. Are staff specifically trained on this distinct standard, not assuming general health privacy training suffices? — *Real, specific training, not an assumption of general confidentiality knowledge.*

Evidence: Staff training on substance use disorder confidentiality standard

COMMON REASONS FOR A PARTIAL ANSWER

- **The distinct standard is understood by clinical staff but not consistently by administrative staff who may handle these records.** — Every staff member with access to these specific records deserves the same genuine understanding of this heightened standard.
- **Written consent is obtained but doesn't specifically distinguish this category from general information release consent.** — Genuine compliance requires consent language specifically reflecting this distinct, heightened requirement.
- **The standard is applied for direct SUD treatment records but not consistently for related information in a broader clinical note.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current handling of substance use disorder records for genuine adherence to the distinct standard.
Week 2	Establish specific written consent language distinguishing this category from general release.
Week 3	Train all staff with potential record access, not clinical staff alone, on this heightened standard.
Ongoing	Audit handling of related information within broader clinical notes for consistent application.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	SUD protocol review	Reviews evidence that substance use disorder records genuinely follow the distinct, heightened standard.
DOCUMENT	Written consent review	Reviews documentation confirming disclosure is based on genuine, specific patient written consent.
DOCUMENT	Staff training review	Reviews training records confirming staff are specifically educated on this distinct standard.

SUPERVISOR TIPS

- **Ask an administrative staff member whether they're aware of the distinct standard for these specific records.** — This reveals whether genuine understanding extends beyond clinical staff alone.
- **Ask to see the actual, specific written consent language used for this category of disclosure.** — A real, specific document reveals genuine compliance, not an assumption general consent suffices.

EVIDENCE BASE

[30] Multiple countries' health privacy frameworks specifically establish heightened confidentiality protections for substance use disorder or addiction treatment records, distinct from general health information privacy practice, often requiring the patient's own specific consent for disclosure.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

← **Telemedicine Standards**
— all standards

Self-assess against these criteria →

← **Standard 5 — Prescribing & Controlled Substance Management**



Standard 7 — Governance & Provider Credentialing →

© 2026 Accréditation Sans Frontières · PHIG · Sheni Network

ASF STANDARDS · TELEMEDICINE · STANDARD 7

Standard 7 — Governance & Provider Credentialing

5 criteria · 3 non-negotiable · 2 core · Version 3.0

CRITERIA IN THIS STANDARD

- 7.1 — Malpractice Insurance Explicitly Covers Telemedicine
- 7.2 — Malpractice Coverage Genuinely Follows the Patient's State
- 7.3 — Technology-Driven Operational Failures Are Specifically Covered
- 7.4 — Provider Credentials Are Verified Directly, Not Accepted on Self-Report
- 7.5 — A Genuine Coverage Plan Exists for a Solo Provider's Absence

7.1 Malpractice Insurance Explicitly Covers Telemedicine

NON-NEGOTIABLE

Every provider's malpractice insurance explicitly, affirmatively states coverage for telemedicine practice — not assumed included in a standard policy that predates telemedicine becoming mainstream, given many such older policies contain explicit exclusions for virtual care absent a specific endorsement.

In plain terms: Every provider's malpractice insurance policy explicitly says it covers telemedicine — in writing, not assumed from a general policy.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

Many malpractice policies were written for in-person practice. Some exclude telemedicine; some cover it only in the provider's home jurisdiction; some are silent, which means a dispute at the worst possible time. A provider without confirmed telemedicine coverage is practising uninsured — and a claim would fall on them personally, and potentially on the service. The service must obtain, for each provider, written confirmation from the insurer that telemedicine practice is covered, and must file it and renew it.

WHAT GOOD LOOKS LIKE

- Every policy explicitly, affirmatively states telemedicine coverage.
- Coverage is genuinely confirmed in writing with the carrier.
- Verification is genuinely reconfirmed at every renewal or policy change.

COMMON FAILURE MODES

- Telemedicine coverage is assumed from a standard policy's silence on the matter.
- Confirmation, if any, is verbal, not documented in writing.
- Coverage was verified once and never reconfirmed at renewal.

WORKED EXAMPLE

IN PRACTICE	
A 14-clinician telemedicine service.	
BEFORE	Providers had malpractice insurance. Nobody had checked whether it covered telemedicine. When the compliance lead asked insurers, three policies excluded telemedicine entirely and four covered it only in the provider's home state.
ACTION	Each provider obtained written confirmation from their insurer of telemedicine coverage, or a rider

adding it, or a new policy. The confirmations are filed with expiry dates. The service's own entity policy was reviewed and amended to explicitly cover telemedicine operations. Annual re-confirmation is required.

AFTER

The Monitor reviewed 14 written coverage confirmations and the entity policy with telemedicine endorsement. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Ask each provider's insurer, in writing: 'Does this policy cover telemedicine?'
2. File the written answer.
3. Fix every 'no' or 'unclear' before the provider's next session.
4. Re-confirm annually.

The most common mistake: Assuming a malpractice policy covers telemedicine because it covers medicine.

SELF-ASSESSMENT QUESTIONS

1. Does every provider's malpractice policy explicitly, affirmatively state coverage for telemedicine practice? — *Real, affirmative confirmation in the policy itself, not an assumption based on a standard policy's silence.*

Evidence: Malpractice policy telemedicine endorsement documentation

2. Has this coverage been genuinely confirmed in writing with the insurance carrier, not assumed from a verbal assurance? — *Real, written confirmation, not a verbal representation alone.*

Evidence: Written carrier confirmation

3. Is this verification genuinely reconfirmed when a provider's policy renews or changes, not treated as a one-time check? — *Real, periodic reconfirmation, not verification assumed to remain valid indefinitely.*

Evidence: Renewal reconfirmation record

COMMON REASONS FOR A PARTIAL ANSWER

- **Coverage is confirmed for the primary provider but not specifically verified for covering or contracted providers. —**

Every provider delivering care under this service carries the same real requirement for confirmed coverage.

- **Written confirmation exists but doesn't specifically reference telemedicine by name, leaving genuine ambiguity.** — Specific, explicit language addressing telemedicine directly is what actually resolves the real ambiguity this criterion exists to prevent.
- **Verification happened at initial policy purchase but hasn't been reconfirmed through a subsequent renewal cycle.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current malpractice policies for genuine, explicit telemedicine coverage language.
Week 2	Obtain written confirmation from the carrier for any policy lacking explicit telemedicine language.
Week 3	Extend verification to all providers, including covering or contracted staff.
Ongoing	Reconfirm coverage at every policy renewal or change.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Policy endorsement review	Reviews the actual policy documentation for genuine, affirmative telemedicine coverage.
DOCUMENT	Written confirmation review	Reviews evidence of genuine, written carrier confirmation, not verbal assurance alone.
DOCUMENT	Renewal reconfirmation review	Reviews whether coverage is genuinely reconfirmed at each policy renewal or change.

SUPERVISOR TIPS

- **Ask to see the actual written confirmation of telemedicine coverage, not a general assurance of adequate insurance.** — A real, specific document reveals genuine verification, not an assumption of coverage.
- **Ask when telemedicine coverage was last reconfirmed with the carrier.** — A specific, real answer reveals genuine, ongoing practice, not a one-time historical check.

EVIDENCE BASE

[31] Many older malpractice insurance policies were drafted before telemedicine became mainstream and contain explicit exclusions for virtual care unless a formal endorsement is added, with coverage needing to be affirmatively stated in policy declarations or endorsements, since silence is not protection.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

7.2 Malpractice Coverage Genuinely Follows the Patient's State

NON-NEGOTIABLE

Malpractice coverage genuinely, explicitly extends to every state where a patient is actually located during care — not assumed sufficient because a provider is licensed there through an interstate compact, given compact licensure and malpractice insurance are genuinely separate, unlinked requirements.

In plain terms: Malpractice coverage explicitly extends to every jurisdiction where a patient is located during care — not just the provider's home jurisdiction.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

A policy that covers telemedicine 'in the state where the provider is licensed and located' does not cover the patient across the border. If the patient is harmed and sues in their jurisdiction, the policy may not respond. Coverage must follow the patient: every jurisdiction in the licensure matrix (2.1) must be a jurisdiction where the policy applies. The insurer confirms this in writing; the service reconciles the licensure matrix against the coverage territory; any gap is closed by endorsement or by not serving that jurisdiction.

WHAT GOOD LOOKS LIKE

- Coverage genuinely, explicitly extends to every state where patients are actually located.
- Coverage is genuinely verified separately from licensure compliance.
- A proactive process confirms coverage before seeing a patient in a new state.

COMMON FAILURE MODES

- Coverage is assumed sufficient based on compact licensure alone.
- Insurance verification is conflated with licensure compliance, not separately confirmed.
- Coverage gaps are discovered only after care has already been delivered in a new state.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service with providers licensed across multiple jurisdictions.

BEFORE

Malpractice coverage was confirmed for telemedicine (7.1) but the territory was not checked. Several policies covered only the provider's home state. Providers were seeing patients in states where they were licensed but not insured.

ACTION

For each provider, the insurer confirmed the coverage territory in writing. The licensure matrix was reconciled against it. Gaps were closed by policy endorsement extending territory, or by removing the uninsured jurisdictions from the provider's scheduling eligibility. The reconciliation is repeated annually and when licensure changes.

AFTER

The Monitor reviewed the territory confirmations, the reconciled matrix, and the scheduling configuration matching insured territory. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. For each provider, ask the insurer: 'Which jurisdictions does this cover?'

2. Compare to where they are licensed and see patients.
3. Close every gap.
4. Reconcile annually.

The most common mistake: Licensed in five states, insured in one.

SELF-ASSESSMENT QUESTIONS

1. Does malpractice coverage genuinely, explicitly extend to every state where patients are actually located? — *Real, specific, state-by-state confirmed coverage, not assumed from compact licensure alone.*
Evidence: State-specific coverage confirmation

2. Is coverage genuinely verified separately from licensure, not treated as automatically bundled together? — *Real, distinct verification of insurance coverage, not conflated with licensure compliance.*
Evidence: N/A — tested directly

3. Is there a specific process for confirming coverage before a provider sees a patient in a genuinely new state? — *A real, proactive verification process, not discovering a coverage gap only after care has already been delivered.*
Evidence: New-state coverage verification process

COMMON REASONS FOR A PARTIAL ANSWER

- **Coverage is confirmed for the provider's most common patient states but not for less frequent ones.** — Every state where a patient is genuinely located carries the same real coverage requirement, regardless of frequency.
- **Staff understand the general principle but haven't specifically verified it applies correctly to their own current coverage.** — General understanding needs to translate into genuine, specific verification of the provider's own actual policy.
- **A new-state verification process exists but isn't consistently followed under scheduling pressure.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current coverage for genuine, explicit extension to every state where patients are actually located.
Week 2	Establish a proactive verification process before seeing a patient in a genuinely new state.
Week 3	Train staff on the genuine, distinct separation between licensure and insurance coverage.
Ongoing	Audit coverage against actual patient location patterns.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	State-specific coverage review	Reviews evidence that malpractice coverage explicitly extends to every state where patients are actually located.
ASK	Licensure-insurance distinction interview	Asks staff whether they understand licensure and insurance coverage as genuinely separate requirements.
DOCUMENT	New-state verification process review	Reviews the process for confirming coverage before a provider sees a patient in a new state.

SUPERVISOR TIPS

- **Ask how the service would confirm malpractice coverage before a provider sees a patient in a state they haven't seen patients in before.** — A specific, confident answer reveals a genuine, proactive process, not an assumption of automatic coverage.
- **Ask a provider directly whether they understand licensure and malpractice coverage as separate requirements.** — A specific, accurate answer reveals genuine understanding, not conflation of the two.

EVIDENCE BASE

[32] Interstate licensure compacts such as the Interstate Medical Licensure Compact facilitate multi-state licensure but do not inherently standardize

malpractice insurance requirements, meaning providers must separately confirm their coverage explicitly extends to every state where they actually deliver care.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

7.3

**Technology-Driven Operational Failures
Are Specifically Covered**

CORE

Insurance coverage specifically addresses technology-driven operational failures — a failed video platform, corrupted data transmission, an algorithmic triage tool error contributing to patient harm — not assumed included within standard clinical malpractice coverage, given traditional malpractice policies often don't cover this genuinely distinct category of exposure.

In plain terms: The service's insurance specifically covers technology failures — a platform outage, a data breach, a failed connection during an emergency — not just clinical negligence.

Facility category	Crisis	Transition	Small	Standard
Applicability	N/A	Full	Adapted	Full

WHY THIS MATTERS

Telemedicine has failure modes that in-person care does not: the platform goes down for a day and 200 appointments are missed; a data breach exposes thousands of records; the connection drops during an emergency and the patient is harmed by the delay. General and malpractice insurance may not cover these. Cyber liability, business interruption, and technology errors-and-omissions coverage address them. The service should review its policies against a list of technology failure scenarios and confirm coverage for each in writing.

WHAT GOOD LOOKS
LIKE

COMMON FAILURE
MODES

- Coverage for technology-driven operational failures is specifically confirmed, not assumed.
- This coverage question was genuinely raised and directly confirmed with the carrier.
- The service understands the specific scope of what this coverage addresses.

- Technology failure coverage is assumed included within standard clinical malpractice.
- This specific question was never raised with the carrier; silence is treated as inclusion.
- The service has no specific understanding of what technology-related coverage actually includes.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service with malpractice and general liability insurance only.

BEFORE

No cyber liability, no business interruption, no technology E&O. When the video platform suffered an outage that cancelled a day of appointments, the loss was uninsured. When the service considered a data breach scenario, it realised it had no coverage for notification costs or regulatory penalties.

ACTION

An insurance broker reviewed the service against a technology failure scenario list: platform outage, data breach, ransomware, connection failure causing harm, vendor failure. Cyber liability and technology E&O policies were added. Business interruption was extended to platform outage. The coverage map is documented and reviewed annually.

AFTER

The Monitor reviewed the coverage map with policies matched to scenarios, and the new cyber and technology E&O policies. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. List your technology failure scenarios: outage, breach, connection failure, vendor failure.
2. Ask your broker which are covered.
3. Add cyber liability and technology E&O if missing.
4. Document the coverage map.

The most common mistake: Assuming malpractice insurance covers a data breach — it does not.

SELF-ASSESSMENT QUESTIONS

1. Does insurance coverage specifically address technology-driven operational failures? — *Real, specific confirmation, not an assumption it's automatically included.*

Evidence: Technology failure coverage confirmation

2. Has this coverage question been genuinely raised and confirmed with the carrier? — *Real, direct confirmation, not silence interpreted as inclusion.*

Evidence: N/A — tested directly

3. Does the service understand which technology failure scenarios this coverage would and would not address? — *Real, specific understanding, not an assumption of broad protection.*

Evidence: Coverage scope understanding documentation

COMMON REASONS FOR A PARTIAL ANSWER

- **Coverage was discussed generally with the carrier but the specific scenarios named in this criterion weren't individually addressed.** — Genuine confirmation should specifically address concrete scenarios, not remain at a general, unspecific level.
- **Coverage exists for platform failures but hasn't been specifically confirmed for algorithmic or automated triage tool errors.** — Every genuinely distinct technology exposure deserves the same specific confirmation, not only the most obvious one.
- **Understanding of coverage scope exists at a leadership level but isn't communicated to providers who might need it in an actual claim.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current malpractice coverage for genuine confirmation of technology-driven failure protection.
Week 2	Raise this specific coverage question directly with the insurance carrier, addressing concrete scenarios.
Week 3	Document the service's specific understanding of coverage scope.
Ongoing	Communicate this understanding to providers, not leadership alone.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Technology coverage confirmation review	Reviews evidence that technology-driven failure coverage was specifically confirmed, not assumed.
ASK	Carrier confirmation interview	Asks staff whether this specific coverage question was genuinely raised with the insurance carrier.
DOCUMENT	Scope understanding review	Reviews the service's documented understanding of what this coverage does and doesn't address.

SUPERVISOR TIPS

- **Ask whether the specific question of technology failure coverage was ever directly raised with the carrier.** — A specific, real answer reveals genuine confirmation, not an assumption based on general policy language.
- **Ask a provider whether they understand what would happen, insurance-wise, if a platform failure contributed to a patient harm event.** — A specific, thoughtful answer reveals genuine, communicated understanding, not knowledge confined to leadership alone.

EVIDENCE BASE

[33] When care delivery depends on digital platforms, software malfunctions including failed video platforms, corrupted data transmission, or algorithmic triage tool errors can contribute to patient harm, with

traditional malpractice policies often not covering these technology-driven operational failures.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

7.4 **Provider Credentials Are Verified Directly, Not Accepted on Self-Report**

NON-NEGOTIABLE

Every remote provider's credentials — licensure, board certification, education — are verified directly with the issuing authority, not accepted based on the provider's own self-reported documentation, given the absence of a physical site visit that might otherwise surface an inconsistency makes this direct verification genuinely more important, not less. Every provider completes structured orientation to the platform and its protocols before independent practice, and performance and competency are formally evaluated on a defined schedule.

In plain terms: Every remote provider's licence, board certification, and education are verified directly with the issuing bodies — not accepted from their CV or a scanned certificate.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

A remote provider may never be met in person. Their credentials are documents on a screen. Fraud is easier and detection harder. Primary source verification — contacting the licensing board, the certification body, the medical school — is the only way to know the provider is who they say they are and qualified as they claim. It is done before the

first session, documented, and repeated at licence renewal. The service that accepts a scanned certificate has verified that a scan exists.

WHAT GOOD LOOKS LIKE

- Every provider's credentials are genuinely, directly verified with issuing authorities.
- Verification genuinely covers licensure, certification, and education together.
- Verification is genuinely, periodically reconfirmed, not a one-time check.

COMMON FAILURE MODES

- Credentials are accepted based on provider self-report without direct verification.
- Verification covers licensure alone, missing certification or education.
- Verification happened once at hire and was never reconfirmed.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service that had recruited 16 providers remotely.

BEFORE

Credentials were accepted from CVs and scanned certificates. Nobody had contacted a licensing board. An audit with primary source verification found one provider's board certification had lapsed and another's claimed fellowship did not exist.

ACTION

Primary source verification was completed for every provider: licence with each licensing board; board certification with the certifying body; education with the institution; work history with two prior employers. Findings were documented; the two discrepancies were addressed. Verification is repeated at each licence renewal and annually for certification. A credentials file exists for every provider.

AFTER

The Monitor reviewed 16 credentials files with primary source verification evidence and dates. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. For each provider, contact the licensing board and verify the licence.
2. Contact the certifying body and verify certification.
3. Contact the medical school and verify the degree.
4. File the evidence.

The most common mistake: Verifying that a certificate exists rather than that it is genuine.

SELF-ASSESSMENT QUESTIONS

1. Are every provider's credentials genuinely verified directly with the issuing authority, not accepted on self-report? — *Real, direct verification, not trust in documentation the provider submitted themselves.*

Evidence: Direct credential verification record

2. Does this verification genuinely cover licensure, board certification, and education, not licensure alone? — *Complete, genuine verification across every relevant credential type, not a partial check.*

Evidence: N/A — tested directly

3. Is verification genuinely reconfirmed periodically, not treated as a one-time check at initial hire? — *Real, periodic reconfirmation, not verification assumed to remain valid indefinitely.*

Evidence: Periodic reconfirmation schedule

4. Does every provider complete structured orientation to the platform, protocols, and escalation pathways before seeing patients independently? — *Real, structured orientation specific to remote practice, not an assumption that in-person competence transfers automatically.*

Evidence: Orientation completion record

5. Is provider performance and competency formally evaluated on a defined schedule, documented and shared with them? — *A real, periodic, documented evaluation, distinct from credential checking alone.*

Evidence: Performance evaluation record

COMMON REASONS FOR A PARTIAL ANSWER

- **Direct verification happens for licensure but board certification is accepted from self-submitted documentation.** — Every credential category carries the same real importance and deserves the same direct verification.
- **Verification is thorough at initial onboarding but isn't reconfirmed as licenses and certifications approach renewal.** — A credential's real, current validity depends on genuine reconfirmation, not a historical check alone.
- **Verification happens for full-time providers but is less rigorous for occasional or covering providers.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current credential verification for genuine, direct confirmation versus self-report acceptance.
Week 2	Establish direct verification with issuing authorities for licensure, certification, and education.
Week 3	Build a periodic reconfirmation schedule extending to all providers, including occasional staff.
Ongoing	Audit verification records for continued currency.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Direct verification review	Reviews evidence of genuine, direct verification with issuing authorities for every provider.
DOCUMENT	Credential completeness review	Reviews whether verification genuinely covers licensure, certification, and education together.
DOCUMENT	Reconfirmation schedule review	Reviews whether verification is genuinely, periodically reconfirmed.

SUPERVISOR TIPS

- **Ask how the service would directly verify a specific provider's board certification, not licensure alone.** — A specific, confident answer reveals genuine, complete verification, not licensure-only checking.

- **Ask when a specific provider's credentials were last reconfirmed.** — A specific, real answer reveals genuine, ongoing practice, not a one-time historical check.

EVIDENCE BASE

[34] Direct verification of provider credentials with the issuing licensing authority, distinct from acceptance of self-reported documentation, is established as necessary practice, carrying particular importance for remote-only practice arrangements that lack the informal verification opportunities a physical site provides.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

7.5

A Genuine Coverage Plan Exists for a Solo Provider's Absence

CORE

For a service staffed by a single provider, a genuine, defined coverage arrangement exists for when that provider is unavailable — illness, leave, emergency — with a real, named alternative for patients needing care in that gap, not an assumption that patients will simply wait or seek care elsewhere on their own. The service has a named person with documented accountability for clinical governance and a separate accountability for financial decisions, a brief, genuine statement of mission and values, and every policy in use is authorised by a named person and reviewed on a defined schedule.

In plain terms: If the service has one provider, there is a written arrangement for who covers when they are ill or away — and patients know how to reach care.

Facility category	Crisis	Transition	Small	Standard
Applicability	Adapted	Full	Full	Full

WHY THIS MATTERS

This is the telemedicine version of PHC 7.1: a solo provider's absence is a service closure unless there is cover. Patients with ongoing care, prescriptions, and crises need someone. Coverage means a named provider or service who will see the patients, access to records, a message to patients about how to reach cover, and a test of the arrangement before it is needed.

WHAT GOOD LOOKS LIKE

- A genuine, defined coverage arrangement exists and is real, not theoretical.
- A specific, named alternative provider is identified for coverage gaps.
- Patients are genuinely, proactively aware of the coverage plan.

COMMON FAILURE MODES

- No defined coverage arrangement exists beyond an assumption patients will manage.
- No specific alternative is identified; patients are vaguely told to seek care elsewhere.
- Patients only learn about coverage gaps when they actually encounter one.

WORKED EXAMPLE

IN PRACTICE

A single-provider telemedicine psychiatry service with 300 patients.

BEFORE

When the provider was hospitalised for two weeks, the service stopped. Patients could not reach anyone. Prescriptions expired. One patient in crisis contacted the service's email and received no reply.

ACTION

A reciprocal coverage agreement was signed with another solo telemedicine psychiatrist: each covers the other's urgent needs, prescription renewals, and crisis contacts during absence. Records access was arranged with patient consent. An absence protocol names who activates cover, the message patients receive, and how the covering provider is reached. It was tested with a planned absence.

AFTER

The Monitor reviewed the signed agreement, the absence protocol, the records access arrangement, and the test record. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Find another solo provider and propose reciprocal cover.
2. Write the absence protocol.
3. Arrange records access with patient consent.
4. Test it.

The most common mistake: A solo provider with no cover — the service does not exist when they are ill.

SELF-ASSESSMENT QUESTIONS

1. Does a genuine, defined coverage arrangement exist for when a solo provider is unavailable? — *A real, specific arrangement, not an assumption that patients will manage without care.*

Evidence: Coverage arrangement documentation

2. Is there a real, named alternative provider or service patients can be directed to during a coverage gap? — *A specific, real alternative, not a vague suggestion to seek care elsewhere.*

Evidence: Named alternative provider documentation

3. Are patients genuinely informed of the coverage plan, not left to discover it only when they need it? — *Real, proactive patient awareness, not information they only encounter during an actual gap.*

Evidence: N/A — tested directly

4. Is there a named person with documented accountability for clinical governance, and a separate named accountability for financial decisions? — *Real, named accountability for each, even at a solo-provider service.*

Evidence: Governance role documentation

5. Does the service have a brief, genuine written statement of its mission and values? — *A real, specific statement, not an absence of one on the assumption a small service doesn't need it.*

Evidence: Mission/values statement

6. Is every policy in use authorised by a named person and reviewed on a defined schedule? — A real, if lightweight, authorisation and review process.

Evidence: Document authorisation/review record

COMMON REASONS FOR A PARTIAL ANSWER

- **A coverage plan exists for planned absences but not genuinely for sudden, unplanned unavailability.** — A genuine emergency doesn't announce itself in advance, and the plan needs to cover this reality too.
- **An alternative provider is named but the relationship hasn't been recently reconfirmed as still active.** — A coverage relationship needs to remain genuinely active, not just historically established.
- **The plan exists but patient awareness relies on them happening to ask, not proactive communication.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current coverage arrangements for genuine readiness, including sudden, unplanned absence.
Week 2	Establish or reconfirm a specific, named alternative provider relationship.
Week 3	Build proactive patient communication about the coverage plan.
Ongoing	Periodically reconfirm the coverage relationship remains genuinely active.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Coverage plan review	Reviews the actual, defined coverage arrangement for when the sole provider is unavailable.
DOCUMENT	Alternative provider review	Reviews the specific, named alternative provider or service patients would be directed to.
ASK	Patient awareness interview	Asks a patient whether they know what to do if the service's provider were unavailable.

SUPERVISOR TIPS

- **Ask what specifically would happen if the provider became suddenly, unexpectedly unavailable today.** — A specific, confident answer reveals a genuine plan, not an assumption it would work out.
- **Ask a patient directly whether they know what to do if the provider were unavailable.** — This tests genuine, proactive awareness, not an assumption patients would figure it out.

EVIDENCE BASE

[35] Defined coverage arrangements for a solo provider's unavailability, distinct from an assumed continuation of care without one, are established as necessary practice for genuine continuity in any single-provider care model, telemedicine included.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

← **Telemedicine Standards**
— all standards

Self-assess against these criteria →

← **Standard 6 — Data
Privacy & Patient
Confidentiality**

**Standard 8 — Health &
Migration →**

© 2026 Accréditation Sans Frontières · PHIG · Sheni Network

Standard 8 — Health & Migration

10 criteria · 7 non-negotiable · 3 core · Version 3.0

CRITERIA IN THIS STANDARD

- 8.1 — People-Centred Care Adapted to Migration and Displacement Experience
 - 8.2 — Digital Literacy and Device Access Barriers Are Actively Addressed
 - 8.3 — Language and Communication Aids — Interpreters and Cultural Mediators
 - 8.4 — Genuine Agency Is Respected, Not Treated as a Passive Technology Recipient
 - 8.5 — Continuity Across Mobility Is Actively Supported Through Portable Records
 - 8.6 — Evidence-Informed Care for Refugee and Migrant Populations
 - 8.7 — Staff Reflective Practice, Bias Awareness, and Self-Care in Migration Contexts
 - 8.8 — Digital Privacy Concerns Specific to Displaced Populations Are Genuinely Addressed
 - 8.9 — Legal Status Diversity Recognition
 - 8.10 — Care Is Documented and Provided Regardless of Immigration or Legal Status
-

8.1 People-Centred Care Adapted to Migration and Displacement Experience

Care is genuinely adapted to a patient's migration and displacement experience — including trauma-informed practice and awareness of legal-status barriers to access — not delivered identically regardless of that history, whether the visit occurs in a stable setting or through the far more variable circumstances telemedicine allows a displaced patient to connect from.

In plain terms: Care is genuinely adapted for refugee and migrant patients — recognising trauma, legal-status fears, and the barriers they face — not just delivered the same way as for everyone else.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

A refugee who has crossed a border on foot, lost family, and now fears deportation does not arrive at the telemedicine service as an ordinary patient. They may not disclose symptoms that could mark them as a burden. They may not return for follow-up because they moved or because the last clinic reported them. They may react to a physical examination with terror rooted in what was done to them before. Trauma-informed care means staff understand this, explain before touching, ask permission, avoid triggering procedures where possible, and never threaten legal consequences. It means the telemedicine service has decided that a person's migration status does not change their right to care — and staff know it.

WHAT GOOD LOOKS LIKE

- Care is genuinely, visibly adapted to migration and displacement history.
- Trauma-informed practice is actually applied, not just referenced.
- Providers demonstrate specific awareness of

COMMON FAILURE MODES

- Care is delivered identically regardless of migration history.
- Trauma-informed practice exists only as a stated principle, not applied practice.

legal-status access barriers.

- Providers show no specific awareness of legal-status barriers.

WORKED EXAMPLE

IN PRACTICE

A 17-clinician telemedicine service in a city with a large refugee population.

BEFORE

Refugee patients were treated identically to others. Staff had no training on trauma or migration. The Coordinator observed a nurse insisting a woman remove her headscarf for a routine examination, and a receptionist asking for immigration documents at registration. Refugee patients reported avoiding the telemedicine service because 'they ask questions.'

ACTION

A half-day trauma-informed care module was delivered to all patient-facing staff, developed with a refugee support NGO. A written policy stated that immigration status is not asked and does not affect care. Registration was simplified to name, date of birth, and contact. Examination consent scripts were adapted. A refugee liaison worker was engaged part-time through the NGO.

AFTER

The Monitor reviewed the policy, training records (94% of staff), and interviewed the liaison worker and two refugee patients who described feeling safe. Observed a consultation where the clinician explained each step before touching. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Ask refugee-serving organisations in your area what their clients say about your telemedicine service.
2. Write one sentence: 'We do not ask immigration status and it does not affect care.' Post it.
3. Arrange trauma-informed care training with an NGO that knows the population.

4. Remove immigration document requests from registration.

The most common mistake: Believing that treating everyone 'the same' is equity — for a traumatised patient, the same treatment is a different experience.

SELF-ASSESSMENT QUESTIONS

1. Is care genuinely adapted to a patient's migration and displacement experience, not delivered identically regardless of history? — *Genuine adaptation, not a generic cultural-awareness statement.*

Evidence: Training record on migration-adapted care

2. Is trauma-informed practice genuinely applied, not just referenced as a principle? — *Actual practice adaptation, not an assumption of general sensitivity.*

Evidence: N/A — tested directly

3. Are providers aware of legal-status barriers to access that may affect this specific patient? — *Specific awareness, not a general sense that barriers can exist.*

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **Adaptation happens for patients who disclose their history but isn't proactively considered otherwise.** — Not every patient will volunteer this history unprompted, even when it is clinically relevant.
- **Providers are aware of the principle but haven't received specific training on applying it remotely.** — General awareness doesn't reliably translate into genuine practice adaptation without specific training.
- **Adaptation is strong for the first consultation but isn't sustained across ongoing remote follow-up.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current practice for genuine adaptation to migration and displacement history.
Week 2	Train providers specifically on trauma-informed, migration-adapted practice.

When	What
Week 3	Build awareness of legal-status access barriers into standard practice.
Ongoing	Revisit adaptation as the ongoing patient relationship develops.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
ASK	Migration-adapted care interview	Asks providers how they adapt practice specifically for a patient's migration and displacement history.
OBSERVE	Trauma-informed practice observation	Observes an actual consultation for genuine trauma-informed practice, not generic sensitivity.
DOCUMENT	Training content review	Reviews training materials for specific coverage of migration-adapted, trauma-informed care.

SUPERVISOR TIPS

- **Ask a provider to describe a specific example of adapting care for a patient's migration history.** — A real, specific example reveals genuine practice, not familiarity with the principle.
- **Ask about continuity of care support specifically for patients without stable documentation.** — This is where genuine adaptation is most tested.

EVIDENCE BASE

[36] WHO Competency Standard 1 (Refugee and Migrant Health: Global Competency Standards for Health Workers, 2021) requires health workers to adapt practice to migration and displacement experiences, address trauma-informed care and psychosocial needs, and support continuity of care regardless of legal status.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.2 Digital Literacy and Device Access Barriers Are Actively Addressed

NON-NEGOTIABLE

Barriers to telemedicine access specific to displaced and migrant populations — limited device access, unreliable connectivity, lower digital literacy — are genuinely, actively addressed, not assumed absent simply because a patient has managed to connect for this particular visit.

In plain terms: The service actively removes the barriers refugees and migrants face in using telemedicine — no smartphone, no data, no quiet place, no digital experience — with loaner devices, data support, partner sites, and hands-on help.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Adapted	Full

WHY THIS MATTERS

Telemedicine assumes a smartphone, a data plan, a private space, and the skill to use an app. A refugee in a shelter, a migrant worker in shared housing, an elderly person who has never used video — each lacks one or more. 'Telemedicine is accessible' is true only for people who already have the means. Addressing barriers means: loaner devices; data credits or Wi-Fi access; partner sites (community centres, NGOs) with private rooms and equipment; a tech assistant who sets up the first call; phone-only options; and materials in the patient's language. The service that does not do this has excluded the people who most need it.

WHAT GOOD LOOKS LIKE

- Device and connectivity barriers are genuinely, actively assessed.
- Digital literacy support is genuinely offered where needed.

COMMON FAILURE MODES

- Barriers are assumed absent because a patient managed to connect for this visit.
- No digital literacy support is offered; independent navigation is assumed.

- A real alternative access method exists for unreliable technology access.

- No alternative exists for patients with unreliable technology access.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service contracted to serve a refugee population.

BEFORE

Consultations required a smartphone app. Uptake among refugees was 15%. Interviews found: no smartphone (30%), no data (40%), no private space (50%), could not use the app (35%). The service had assumed the platform was accessible.

ACTION

Partnerships with three community organisations provided private rooms with tablets and Wi-Fi. A loaner device programme with data credits was set up. A bilingual tech assistant does a set-up call with every new patient. A phone-only pathway was created. Materials were translated into six languages with pictorial guides. Uptake rose to 68%.

AFTER

The Monitor reviewed the partner site agreements, the loaner device register (45 devices), the tech assistant's set-up log, the phone pathway, and uptake data. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Ask ten refugee patients what stopped them using the service.
2. Partner with a community organisation for private rooms and devices.
3. Assign someone to set up the first call with every new patient.
4. Offer a phone-only option.

The most common mistake: Declaring the service accessible because the app is free.

SELF-ASSESSMENT QUESTIONS

1. Are device and connectivity barriers specific to this population genuinely, actively assessed, not assumed absent? — *Real, active assessment, not an assumption a successful connection today means reliable access generally.*

Evidence: Access barrier assessment process

2. Is digital literacy support genuinely offered where needed, not assumed unnecessary? — *Real, offered support, not an assumption every patient can navigate the platform independently.*

Evidence: Digital literacy support materials

3. Is there a genuine alternative access method for a patient whose connectivity or device access is unreliable? — *A real, practical alternative, not care limited to those with reliable technology access.*

Evidence: Alternative access method documentation

COMMON REASONS FOR A PARTIAL ANSWER

- **Assessment happens at intake but isn't revisited as a patient's actual circumstances may change.** — A patient's access reliability can genuinely change, particularly for a population with real mobility.
- **Digital literacy support exists in the dominant local language but not in the patient's own language.** — Genuine support needs to be usable in the language the patient actually understands.
- **An alternative access method exists but isn't proactively offered, relying on the patient to request it.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current practice for genuine assessment of device and connectivity barriers.
Week 2	Build digital literacy support materials in relevant languages.
Week 3	Establish and proactively offer a genuine alternative access method.
Ongoing	Revisit access barrier assessment as patient circumstances change.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Barrier assessment review	Reviews the process for genuinely assessing device and connectivity barriers for this population.
DOCUMENT	Digital literacy support review	Reviews materials or processes genuinely supporting patients with lower digital literacy.
DOCUMENT	Alternative access review	Reviews the genuine alternative access method available for patients with unreliable technology access.

SUPERVISOR TIPS

- **Ask how the service would identify a patient struggling with the platform who hasn't said so directly.** — A specific, thoughtful answer reveals genuine, proactive attention, not reliance on the patient to report difficulty.
- **Ask what alternative exists for a patient whose smartphone or data access is genuinely unreliable.** — A specific, real answer reveals a genuine alternative, not an assumption everyone has adequate access.

EVIDENCE BASE

[37] Systematic review of telemedicine for refugee populations identifies limited access to technology, unreliable internet connectivity, and insufficient digital literacy as key barriers hindering effective telemedicine use, requiring active strategies including affordable connectivity, digital literacy support, and multilingual platforms.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.3 Language and Communication Aids — Interpreters and Cultural Mediators

NON-NEGOTIABLE

Trained interpreters or cultural mediators are engaged for language-discordant remote consultations — never minor children, and only family members when genuinely no other option exists and the situation is not high-risk.

In plain terms: Trained interpreters or cultural mediators are used for language-discordant consultations — never children, and family members only when there is truly no alternative.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Adapted	Full

WHY THIS MATTERS

This is the refugee-specific counterpart of 8.3, and the stakes are higher. Refugee patients may be discussing torture, sexual violence, or mental illness — topics a family member cannot interpret and should not hear. A cultural mediator adds what an interpreter cannot: understanding of why a patient from a particular background may refuse a male examiner, may not disclose a symptom, or may interpret a question as a threat. Children must never interpret for parents: it exposes them to adult content, it distorts the information, and it places the child in an impossible position. Where the telemedicine service serves a refugee population, interpreter and mediator access is a core service, not an extra.

WHAT GOOD LOOKS LIKE

- Trained interpreters or cultural mediators are the default for language-discordant consultations.
- Providers confirm, without hesitation, that minors are never used to interpret.
- Family-member interpretation, when it happens, is reserved for genuinely low-risk situations only.

COMMON FAILURE MODES

- Ad hoc bilingual staff or family members are the default, with trained interpreters rarely engaged.
- A minor has been used to interpret, even occasionally.
- Family members interpret for high-risk situations like informed consent or bad news.

WORKED EXAMPLE

IN PRACTICE

A 16-clinician telemedicine service serving a refugee settlement of 30,000 people.

BEFORE

Interpretation was by family members or other patients from the same language group. A ten-year-old was observed interpreting her mother's gynaecological consultation. A man was asked to interpret for a woman describing sexual violence. There was no interpreter budget and no mediator role.

ACTION

With NGO support, four cultural mediators from the main refugee language groups were recruited and trained. A phone interpretation service covered other languages. A written rule prohibited children interpreting and required same-gender interpreters for sensitive consultations. Interpreter and mediator use was documented. Staff were briefed on why family interpretation is unsafe.

AFTER

The Monitor reviewed 20 refugee patient records: interpreter or mediator documented in all language-discordant consultations. Observed a mediator-supported consultation. Interviewed a mediator who described the same-gender rule in practice. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Ask how the last ten refugee consultations were interpreted.
Count how many used a child or a family member.
2. Write the rule today: no children; family only as a last resort and never for sensitive topics.
3. Recruit mediators from the main language groups — NGOs can help.
4. Contract a phone service for other languages.

The most common mistake: Using the patient's child to interpret because they speak the language best — the child is harmed and

the information is distorted.

SELF-ASSESSMENT QUESTIONS

1. Are trained interpreters or cultural mediators engaged for language-discordant remote consultations? — *Not ad hoc bilingual staff or family members as the default.*

Evidence: Interpreter engagement record

2. Is a minor ever used to facilitate interpretation for a family member? — *This should never happen — a specific, absolute rule, not a judgement call.*

Evidence: N/A — tested directly

3. When a family member interprets due to genuine unavailability of a trained interpreter, is this reserved for low-risk situations only? — *Not used for informed consent, complex diagnoses, or bad news — situations requiring professional language support.*

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **Trained interpreters are engaged for scheduled consultations but not for urgent or same-day remote visits.** — Risk doesn't scale down proportionally with how urgent or unscheduled an interaction feels.
- **The no-minors rule is understood by providers but not consistently reinforced with support staff scheduling sessions.** — A critical safeguard needs to be embedded across the whole team, not held only by the treating provider.
- **Remote interpreter access exists but connection quality issues sometimes lead to reverting to a family member mid-session.**

IMPLEMENTATION PLAN

When	What
Week 1	Review recent language-discordant consultations for interpreter engagement patterns.
Week 2	Establish reliable remote interpreter access, tested for connection quality alongside the platform itself.
Week 3	Brief all staff on the firm exclusion of children as interpreters, without exception.
Ongoing	Audit interpreter use records for consistency.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Interpreter engagement review	Reviews records for evidence of trained interpreter or cultural mediator engagement.
ASK	Minor-interpreter policy check	Asks providers directly whether minors are ever used to interpret, and confirms understanding that this is never acceptable.
OBSERVE	High-risk situation check	Checks whether family-member interpretation, where it occurs, is confined to genuinely low-risk situations.

SUPERVISOR TIPS

- **Ask staff directly whether a child has ever interpreted for a parent during a remote session.** — A direct question often surfaces what a general policy question won't.
- **Ask what happens if the remote interpreter's own connection fails mid-session.** — This reveals whether a genuine backup exists, not reversion to an unqualified family member.

EVIDENCE BASE

[38] WHO Competency Standard 3 explicitly states health workers have a responsibility not to engage minors to facilitate interpretation, given the associated significant risk, and identifies inaccuracy, information distortion, and compromised confidentiality as documented risks of family-member interpretation generally.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.4 Genuine Agency Is Respected, Not Treated as a Passive Technology Recipient

CORE

Refugee and migrant patients are genuinely treated as having real agency and competence in using telemedicine technology — not designed for or spoken to as passive recipients presumed incapable, an assumption real

research specifically warns against as its own documented harm.

In plain terms: Refugee and migrant patients are treated as capable people who can learn and use telemedicine — supported, not assumed helpless or handed off to a family member.

Facility category	Crisis	Transition	Small	Standard
Applicability	N/A	Full	Adapted	Full

WHY THIS MATTERS

There is a paternalism that looks like kindness: assuming the refugee patient cannot use technology, cannot make decisions, needs a relative to speak for them. It strips the patient of agency and often of privacy. Respecting agency means: teaching the patient to use the platform themselves; speaking to them directly, through an interpreter, not to their relative; asking their preferences; involving them in decisions; and recognising that someone who crossed a continent can learn a video app. Support is offered; capability is assumed.

WHAT GOOD LOOKS LIKE

- Technology competence is genuinely assessed per individual, not assumed from population background.
- Communication genuinely respects patient agency, not a presumptive tone.
- Staff are specifically trained on this documented risk of over-generalizing incapability.

COMMON FAILURE MODES

- All patients from this population are assumed uniformly incapable with technology.
- Communication is presumptive or simplified based on the patient's background alone.
- No specific training addresses this documented stereotype risk.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service serving migrant families.

BEFORE

Providers routinely spoke to the English-speaking child or spouse rather than the patient.

	Technology set-up was done with the family member. Decisions were discussed with the relative. Patients were passive observers of their own care.
ACTION	A patient agency protocol was written: the patient is the primary participant; an interpreter is used rather than a family member; tech set-up is done with the patient (with a family member present only at the patient's request); consent and decisions are discussed with the patient directly; the patient's own preferences about family involvement are asked and recorded. Providers completed training on agency and paternalism in migrant care.
AFTER	The Monitor reviewed the protocol, training records, and observed a session conducted directly with the patient through an interpreter. Interviewed a patient who described using the platform herself. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Watch three sessions with migrant patients. Who does the provider address?
2. Require interpreters instead of family members.
3. Do tech set-up with the patient, not the relative.
4. Ask the patient how they want family involved.

The most common mistake: Speaking to the English-speaking relative because it is easier — the patient has been made invisible in their own consultation.

SELF-ASSESSMENT QUESTIONS

1. Are patients genuinely assessed as individuals for technology competence, not assumed uniformly incapable based on background? — *Real, individual assessment, not a blanket assumption applied to the whole population.*

Evidence: N/A — tested directly

2. Does communication about technology use respect the patient's real agency, not speak to them as a passive recipient? — *Genuine, respectful communication, not language or tone presuming incapability.*
Evidence: N/A — tested directly

3. Are staff specifically trained to recognise this documented risk of over-generalizing incapability to this population? — *Real, specific training on this documented concern, not an assumption good intentions alone prevent it.*
Evidence: Staff training on agency and stereotype avoidance

COMMON REASONS FOR A PARTIAL ANSWER

- **Individual assessment happens for adult patients but assumptions persist more readily for older patients within this population.** — Age within this population doesn't determine genuine technology competence any more than population background does.
- **Staff avoid overtly presumptive language but subtly simplify explanations more than the individual patient's demonstrated understanding warrants.** — Genuine respect for agency means calibrating explanation to the actual person, not a background-based default.
- **Awareness of this concern exists informally but hasn't been specifically, formally trained.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current practice for genuine, individual assessment versus population-based assumption.
Week 2	Train staff specifically on this documented stereotype risk and how to avoid it.
Week 3	Build communication practices that calibrate to individual demonstrated competence.
Ongoing	Audit communication tone for continued respect of patient agency.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
OBSERVE	Individual assessment observation	Observes whether technology competence is genuinely assessed per patient, not assumed from population background.
OBSERVE	Communication tone observation	Observes provider communication for genuine respect of patient agency, not a presumptive, simplified tone.
DOCUMENT	Staff training review	Reviews training records for specific coverage of this documented stereotype risk.

SUPERVISOR TIPS

- **Observe how a provider explains platform use to a patient from this population, if possible.** — Direct observation reveals genuine, individually calibrated respect, not a presumptive default tone.
- **Ask staff whether they've received specific training on avoiding this documented stereotype.** — A specific, confident answer reveals genuine awareness, not an assumption good intentions are sufficient.

EVIDENCE BASE

[39] Research on refugee telehealth implementation specifically cautions that health technologies should be designed to create space for refugees to practice and demonstrate genuine agency, rather than treating them as passive beneficiaries of the technology, a framing that itself perpetuates harmful assumptions about their capabilities.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.5 Continuity Across Mobility Is Actively Supported Through Portable Records

NON-NEGOTIABLE

When a genuinely mobile or displaced patient's location changes, the service actively supports continuity through a portable, patient-accessible record — not treating each new location, or each new provider the patient might reach, as an entirely fresh start with no continuity from what came before.

In plain terms: When a displaced patient moves, the service gives them a portable record — a summary they hold, in a form that works anywhere — and keeps the connection going where possible.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Adapted	Full

WHY THIS MATTERS

Telemedicine's advantage for displaced people is that it can follow them — a patient who moves from a shelter to a city to another country can, in principle, keep the same provider. In practice, licensure (2.4) may prevent that. The fallback is a portable record: a summary the patient holds (paper and digital), in their language and the destination's, covering diagnoses, medications, results, vaccinations, and the service's contact. Where licensure allows, care continues; where it does not, the record travels and a handover is attempted.

WHAT GOOD LOOKS LIKE

- A genuinely portable, patient-accessible record format is actively provided.
- The record is genuinely kept current, particularly near a known relocation.
- Patients genuinely know how to access and use their own record independently.

COMMON FAILURE MODES

- Records remain locked within this service's own system, not genuinely portable.
- The record becomes outdated, not reflecting the patient's actual, recent status.
- Patients remain dependent on requesting their own information from this service each time.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service serving people in transit through a migration corridor.

BEFORE Patients moved on without records. A patient on TB treatment moved from one country to another; the service could not continue care and the patient had no documentation; treatment was interrupted for six weeks.

ACTION A portable record is now issued to every mobile patient at each session: a PDF on their phone and a printed copy where possible, in their language and English, with diagnoses, medications and duration, results, vaccinations, and the service's contact. When a patient reports a move, the licensure check (2.4) determines whether care can continue remotely; if not, the service attempts a warm handover to a provider or NGO at the destination. High-priority conditions (TB, pregnancy, serious mental illness) get a follow-up call at two weeks.

AFTER The Monitor reviewed 20 portable records issued, 6 relocation cases with continued remote care, and 4 with documented handover attempts. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Give every mobile patient a portable summary at every session.
2. Make it a PDF on their phone and a print if possible.
3. When they move, check licensure; continue or hand over.
4. Follow up high-priority conditions at two weeks.

The most common mistake: Keeping excellent records the patient cannot take with them.

SELF-ASSESSMENT QUESTIONS

1. Does the service provide a genuinely portable record, not one locked within a single system? — *A real, portable format the patient can carry forward, not accessible only here.*

Evidence: Portable record format documentation

2. Is the record genuinely updated close to a known relocation, not left outdated? — *Real, current information reflecting the patient's actual status, not a stale record.*

Evidence: N/A — tested directly

3. Does the patient know how to access and use this record themselves? — *Real, patient-controlled access, not continued dependency on this service.*

Evidence: Patient record access instruction

COMMON REASONS FOR A PARTIAL ANSWER

- **A portable record format exists but isn't proactively offered unless the patient specifically requests it.** — A patient who doesn't know to ask shouldn't be less likely to receive genuine continuity support.
- **The record is current at creation but isn't genuinely updated as the ongoing relationship continues.** — Continuity value depends on the record reflecting the patient's actual, current status, not only their status at one point in time.
- **Patients are given the record but not specific instruction on how to actually use or share it with a future provider.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current record practice for genuine portability versus system lock-in.
Week 2	Establish a standard, portable, patient-accessible record format, proactively offered.
Week 3	Build a process for keeping the record genuinely current, particularly near known relocations.
Ongoing	Confirm patients understand how to access and use their own record independently.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Portable record review	Reviews whether patients genuinely receive a portable, accessible record format.
DOCUMENT	Record currency review	Reviews whether the record is genuinely kept current, particularly near a known relocation.
ASK	Patient access interview	Asks a patient whether they know how to access and use their own portable record.

SUPERVISOR TIPS

- **Ask a patient whether they have their own accessible copy of their health record, and whether they know how to use it.** — A real, specific answer reveals genuine portability, not a record locked within the service's own system.
- **Ask how the record is updated when a patient reports an upcoming relocation.** — A specific, confident answer reveals genuine, proactive practice, not passive record-keeping.

EVIDENCE BASE

[40] Refugees experience genuine difficulty accessing their medical records and maintaining continuity of care due to mobility-related challenges, with the absence of standardized, interoperable procedures between health systems resulting in fragmented records, incomplete medical history, and documented medical errors.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.6 Evidence-Informed Care for Refugee and Migrant Populations CORE

Staff use evidence-informed guidelines specific to refugee and migrant health where they exist, recognise where the health needs of this population differ from the general population, and identify where evidence gaps remain — not

applying general telemedicine guidelines uncritically to a population with documented, different health needs.

In plain terms: Staff use clinical guidelines specific to refugee and migrant health where they exist, know where evidence is thin, and adapt sensibly.

Facility category	Crisis	Transition	Small	Standard
Applicability	N/A	Full	Adapted	Full

WHY THIS MATTERS

Refugee health has specific evidence: screening for TB, hepatitis B, and parasites by region of origin; vaccination catch-up schedules; recognition of conditions rare in the host country; management of trauma-related mental illness. Applying host-country guidelines without adaptation means missing conditions the host population does not have and over-testing for ones the refugee population does not. Where evidence exists — WHO, UNHCR, national refugee health guidelines — staff should use it. Where it does not, they should know that, and adapt with judgment rather than guess.

WHAT GOOD LOOKS LIKE

- Staff are aware of and use population-specific evidence-informed guidelines where they exist.
- Staff can describe specific, genuine differences in this population's health needs.
- Practice is genuinely adapted where population-specific evidence indicates it should be.

COMMON FAILURE MODES

- General telemedicine guidelines are applied uncritically with no population-specific awareness.
- Staff cannot describe any specific way this population's needs differ.
- Awareness exists but doesn't translate into any actual practice adaptation.

WORKED EXAMPLE

IN PRACTICE

A 14-clinician telemedicine service that had started receiving

refugees from a region with high hepatitis B and TB prevalence.

BEFORE	Refugee patients were assessed using standard domestic protocols. Hepatitis B screening was not routine. Two cases of active TB were diagnosed late after multiple presentations. Clinicians were unaware of the WHO and national refugee health screening recommendations.
ACTION	The Coordinator obtained the national refugee health guideline and the WHO recommendations for the relevant region. A refugee health screening protocol was written: TB screening, hepatitis B and C, HIV with consent, parasitic infection screening, vaccination status, mental health screen. Clinicians received a one-hour briefing. The guideline was reviewed annually with an infectious diseases specialist.
AFTER	The Monitor reviewed the protocol with its sources, training records, and 20 refugee patient records showing protocol-based screening. Two hepatitis B cases identified and treated. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Find your national refugee health guideline, or the WHO/UNHCR one for your region.
2. Compare it to what you currently do for refugee patients.
3. Write a screening protocol based on the guideline.
4. Brief clinicians and review annually.

The most common mistake: Applying the domestic screening protocol to refugee patients from regions with a completely different disease burden.

SELF-ASSESSMENT QUESTIONS

1. Are staff aware of evidence-informed guidelines specific to refugee and migrant health where they exist? — *Specific, current awareness, not general clinical knowledge assumed to be sufficient.*
Evidence: Guideline awareness record

2. Do staff recognise where this population's health needs genuinely differ from the general population? — *Genuine, specific recognition, not an assumption that general guidelines always apply equally.*

Evidence: N/A — tested directly

3. Is practice adapted where population-specific evidence indicates a different approach is warranted? — *Actual practice adaptation, not awareness without application.*

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **Awareness exists for well-known differences but not for more specific or recent evidence.** — Evidence in this area continues to develop, and awareness needs to stay genuinely current.
- **Guidelines are known but not consistently applied under time pressure.** — Consistent application under real conditions is what gives awareness genuine protective value.
- **Evidence gaps are acknowledged but staff default to general population assumptions rather than flagging genuine uncertainty.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current awareness of population-specific evidence-informed guidelines.
Week 2	Establish access to current, relevant guidelines for staff.
Week 3	Train staff on specific, genuine population differences relevant to practice.
Ongoing	Refresh awareness as evidence in this area develops.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Guideline awareness review	Reviews whether staff have access to and awareness of population-specific evidence-informed guidelines.

Method	What	Detail
ASK	Population-difference interview	Asks staff to describe a specific way this population's health needs differ from the general population.
OBSERVE	Practice adaptation check	Checks whether practice genuinely reflects population-specific evidence where it exists.

SUPERVISOR TIPS

- **Ask staff for a specific example of a practice adaptation based on population-specific evidence.** — A real example reveals genuine application, not just familiarity with the concept.
- **Ask how staff would handle a genuine evidence gap for this population.** — A thoughtful, honest answer reveals genuine engagement rather than a default assumption.

EVIDENCE BASE

[41] WHO Competency Standard 7 requires health workers to use evidence-informed guidelines specific to refugee and migrant health where they exist, recognise where the health needs of this population differ from the general population, and identify where evidence gaps remain.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.7 Staff Reflective Practice, Bias Awareness, and Self-Care in Migration Contexts

NON-NEGOTIABLE

Staff maintain active awareness of their own culture, beliefs, and potential biases through structured reflective practice, and the service actively fosters a supportive environment with genuine access to psychological support — not assumed self-awareness or an assumption that staff will manage vicarious trauma exposure on their own.

In plain terms: Staff actively reflect on their own biases and culture, the telemedicine service supports this through structured practice, and staff working with traumatised patients are looked after.

Facility category	Crisis	Transition	Small	Standard
Applicability	N/A	Full	Adapted	Full

WHY THIS MATTERS

Every clinician has assumptions about people from other cultures, and most are unaware of them. The nurse who assumes a refugee is exaggerating pain, the doctor who is impatient with a patient who will not make eye contact, the receptionist who is curt with someone who does not understand the form — each is acting on bias, and each affects care. Reflective practice — structured time to examine one's reactions — reduces this. The second element is staff wellbeing: hearing accounts of torture and loss every day takes a toll, and staff who are burned out become staff who withdraw. Supervision, peer support, and access to counselling are not luxuries in a telemedicine service serving refugees.

WHAT GOOD LOOKS LIKE

- A structured reflective practice process genuinely exists and is used, not just assumed.
- Genuine, accessible psychological support exists and staff actually use it.
- Staff can describe specific, real examples of both bias adaptation and vicarious trauma awareness.

COMMON FAILURE MODES

- No structured reflective practice process exists beyond an assumption of individual self-awareness.
- Psychological support exists only nominally, with no evidence staff actually access it.
- Staff cannot describe any specific example of adapting practice or recognising vicarious trauma.

WORKED EXAMPLE

IN PRACTICE

A 15-clinician telemedicine service where a third of patients are refugees.

BEFORE	No reflective practice existed. Staff complained about refugee patients in the break room; some described them as 'demanding.' A nurse who had heard multiple accounts of sexual violence had started avoiding female refugee patients. There was no supervision or support for staff exposed to trauma narratives.
ACTION	Monthly facilitated reflective practice sessions were introduced for clinical teams, led by a psychologist from a partner NGO, using real (anonymised) cases. An implicit bias workshop was run once for all staff. A peer support scheme was set up. Confidential counselling access was arranged through the NGO. Attendance was tracked.
AFTER	The Monitor reviewed session records (10 sessions, average 70% attendance), workshop records, and the counselling access agreement. Interviewed three staff who described the sessions as valuable and gave examples of changed practice. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Listen in the break room. What do staff say about refugee patients when they think no one is listening?
2. Arrange one implicit bias workshop with an NGO or university.
3. Start monthly reflective practice sessions with a facilitator.
4. Arrange confidential counselling access for staff.

The most common mistake: Training staff in cultural competence once and assuming bias is fixed — it is a practice, not a certificate.

SELF-ASSESSMENT QUESTIONS

1. Does the service have a structured process for staff reflective practice regarding bias and cultural awareness? — *A defined process, not an assumption that staff will naturally self-reflect adequately.*
Evidence: Reflective practice process description

2. Does the service provide genuine, accessible psychological support and a real space to discuss difficult cases? — *Actual, used support and a real, regular opportunity, not a theoretical benefit or informal hope.*

Evidence: Psychological support access record

3. Can staff describe a specific instance of adapting their practice after recognising a bias, and do they recognise signs of vicarious trauma in themselves? — *Genuine, concrete examples, not general statements of good intentions or awareness.*

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **Reflective practice happens informally but is not structured into any genuine, regular process.** — Individual good practice does not reliably generalise without a defined, shared process.
- **Support exists but is genuinely difficult to access given remote staff working independently across locations.** — A benefit's existence does not guarantee genuine, comfortable access to it, particularly for a dispersed remote team.
- **Support exists for acute incidents but not for the cumulative emotional weight of this work over time.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current training content and support access for genuine coverage of bias and staff wellbeing.
Week 2	Establish a structured reflective practice process feasible for a remote or dispersed team.
Week 3	Identify genuine, accessible psychological support options appropriate to remote practice.
Ongoing	Revisit reflective practice and wellbeing periodically, using real case examples where appropriate.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
DOCUMENT	Reflective practice process review	Reviews the service's structured process, if any, for staff reflective practice on bias and cultural awareness.
DOCUMENT	Support access review	Reviews what psychological support and debrief structure genuinely exist and whether they are actually used.
ASK	Staff example interview	Asks a staff member for a specific instance of recognising and adapting for their own bias, and how they process the emotional weight of this work.

SUPERVISOR TIPS

- **Ask for a specific personal example, not a general statement of awareness.** — A concrete instance distinguishes genuine reflective practice from familiarity with the concept.
- **Ask directly whether support has been used, not just whether it exists.** — Genuine uptake, not nominal availability, is the real test.

EVIDENCE BASE

[42] WHO Competency Standards 8 and 9 (Refugee and Migrant Health: Global Competency Standards for Health Workers, 2021) require health workers to maintain structured awareness of their own biases and institutional discrimination's impact, and to engage in self-care within a supportive team environment addressing the wellbeing impacts of migration-context care.

[ASF training courses on GMJ Academy →](#)

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.8 Digital Privacy Concerns Specific to Displaced Populations Are Genuinely Addressed

NON-NEGOTIABLE

The service genuinely recognises and addresses the specific, heightened digital privacy concerns displaced populations face — including the real possibility that health-related digital data could be requested or analyzed by immigration or asylum authorities — not treating this population's privacy needs as identical to a general patient's under standard confidentiality practice.

In plain terms: The service knows that displaced people have specific fears about digital privacy — surveillance, data reaching authorities or persecutors — and addresses them concretely, not with a generic privacy notice.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Adapted	Full

WHY THIS MATTERS

A refugee who fled a state that surveilled her may reasonably fear that a video consultation is being watched. A migrant without legal status may fear that health data will reach immigration authorities. An LGBTQ+ asylum seeker may fear disclosure to their community. These fears are rational and they suppress care-seeking. Addressing them means: an explicit statement of what data is collected, who can see it, and — crucially — who cannot (immigration authorities, employers, home-country governments); the legal protections that apply; the option of minimal data collection; and a conversation, in the patient's language, that takes the fear seriously.

WHAT GOOD LOOKS LIKE

- The service genuinely recognises and addresses this population's distinct digital privacy concerns.
- Specific, honest communication clarifies what is and isn't shared with any authority.
- Staff are specifically trained on this

COMMON FAILURE MODES

- This population's privacy needs are treated identically to general patients, with no specific recognition.
- Communication offers only vague, general privacy assurance, not specific clarity.
- Staff rely on general privacy training, with no

documented, distinct concern.

specific coverage of this distinct concern.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service serving asylum seekers.

BEFORE

The privacy notice was a standard legal document. Patients were reluctant to disclose mental health symptoms, HIV status, or sexual orientation on video. Interviews revealed fears that recordings would reach authorities or that the platform was monitored.

ACTION

A plain-language privacy explanation was written in the patients' languages: what is collected, where it is stored, who can access it, who cannot (with legal basis), that sessions are not recorded (6.3), and that the patient can request minimal data. It is discussed at intake, with time for questions. A pseudonymous registration option was introduced for those who need it. Providers were trained on the specific fears and how to address them. The service's data-sharing agreements were reviewed to ensure no pathway to immigration authorities.

AFTER

The Monitor reviewed the privacy explanation in six languages, intake records with the discussion documented, the pseudonymous option, and the data-sharing review. Interviewed a patient who described feeling safe to disclose. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Ask five displaced patients what they fear about their data.
2. Write a plain-language explanation that names who cannot see their data.
3. Discuss it at intake in their language.
4. Offer minimal-data or pseudonymous registration.

The most common mistake: Sending a standard privacy notice to a person who fled state surveillance.

SELF-ASSESSMENT QUESTIONS

1. Does the service genuinely recognise this population's specific digital privacy concerns? — *Real, specific recognition, not general confidentiality practice assumed sufficient.*

Evidence: N/A — tested directly

2. Is there honest communication about what genuinely is and isn't shared with any authority? — *Real, honest, specific communication, not a vague general assurance.*

Evidence: Patient privacy communication materials

3. Are staff specifically trained on this concern, not assuming general privacy training suffices? — *Real, specific training, not general health privacy training assumed sufficient.*

Evidence: Staff training on migration-specific privacy concerns

COMMON REASONS FOR A PARTIAL ANSWER

- **Recognition exists informally among some staff but isn't consistently, formally addressed across the whole team.** — Every staff member interacting with this population deserves the same genuine, formal understanding.
- **Communication is honest but not proactively offered, relying on the patient to raise the concern themselves.** — A patient may not know to ask, and proactive communication reaches concerns that would otherwise go unaddressed.
- **Training references data privacy generally but doesn't specifically name this population's documented, distinct concern.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current practice for genuine recognition of this population's distinct digital privacy concerns.
Week 2	Build specific, honest, proactive patient communication addressing this concern directly.
Week 3	Train all staff specifically on this documented, distinct concern, not general privacy training alone.

When	What
Ongoing	Revisit communication and training as the relevant regulatory landscape evolves.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
ASK	Recognition interview	Asks staff whether they specifically recognise and address this population's distinct digital privacy concerns.
DOCUMENT	Patient communication review	Reviews materials for genuine, specific, honest communication about data sharing with authorities.
DOCUMENT	Staff training review	Reviews training records for specific coverage of this documented, distinct privacy concern.

SUPERVISOR TIPS

- **Ask staff directly whether they've discussed this specific concern with patients from this population.** — A specific, real answer reveals genuine recognition, not an assumption general privacy practice covers it.
- **Ask to see the actual, specific language used to communicate this to a patient.** — A real, specific example reveals genuine, honest communication, not a vague general assurance.

EVIDENCE BASE

[43] Some governments have begun analyzing migrants' phone data as part of asylum adjudication processes, establishing genuine, documented grounds for displaced patients' distinct privacy concerns regarding digital health data, separate from general patient confidentiality practice.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.9 Legal Status Diversity Recognition

CORE

The service can name which legal status categories it actually serves — asylum seeker, recognised refugee, stateless person, and others — and demonstrates it doesn't apply a single, uniform assumption about access rights across all of them.

In plain terms: The telemedicine service can name which legal status groups it serves — asylum seekers, recognised refugees, stateless people, internally displaced, undocumented — and knows what each group is entitled to.

Facility category	Crisis	Transition	Small	Standard
Applicability	N/A	Full	Adapted	Full

WHY THIS MATTERS

An asylum seeker in many countries is entitled to emergency care only. A recognised refugee has the same entitlements as citizens. A stateless person may have no entitlement at all under the letter of the law. An undocumented migrant may be entitled to nothing — or to everything, depending on the jurisdiction and the type of care. A telemedicine service that does not know these distinctions either turns away people who are entitled to care or treats people it cannot be reimbursed for without knowing it. Knowing the categories, the entitlements, and — critically — the telemedicine service's own policy on treating people regardless of entitlement is the foundation for consistent, fair, and legally defensible practice.

WHAT GOOD LOOKS LIKE

- Staff can name the specific legal status categories this service actually serves.
- Policy genuinely differentiates access considerations across status categories.

COMMON FAILURE MODES

- Staff have only a general sense that "migrants" are served, without specific categories.
- A single, uniform assumption about access rights is applied regardless of status.

- A specific, defined process exists for verifying unclear status.

- No process exists for verifying status when it's genuinely unclear.

WORKED EXAMPLE

IN PRACTICE

A 15-clinician telemedicine service in a country with five legal categories for displaced people and different entitlements for each.

BEFORE

Registration staff did not know the categories. Patients were sometimes turned away because 'refugees are not covered' when in fact they were. Others were treated and the telemedicine service could not claim reimbursement because the correct category was not recorded. The telemedicine service had no written position on treating people outside any entitlement.

ACTION

The Coordinator obtained the legal entitlements for each category from the Ministry and UNHCR. A one-page reference was created for registration staff. A telemedicine service policy stated: emergency care for everyone regardless of status; other care per entitlement; and a defined charity fund for those with no entitlement. Registration records the category (with the patient's consent) for reimbursement purposes only — it does not affect clinical care.

AFTER

The Monitor reviewed the entitlement reference, the policy, and 20 registration records with category correctly recorded. Interviewed two registration staff who correctly described entitlements for three categories. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. List the legal status categories that exist in your country for displaced people.
2. Find out what each is entitled to — ask the Ministry or UNHCR.
3. Write a one-page reference for registration staff.

4. Decide and write down what you will do for people with no entitlement.

The most common mistake: Treating all displaced people as one category — 'refugees' — when the law treats them differently and the telemedicine service's obligations differ.

SELF-ASSESSMENT QUESTIONS

1. Can staff name the specific legal status categories this service actually serves? — *Specific, named categories, not a general sense that "migrants" are served.*

Evidence: N/A — tested directly

2. Does the service avoid applying a single, uniform assumption about access rights across all statuses? — *Genuine differentiation, not treating all categories identically.*

Evidence: Status-specific access policy documentation

3. Is there a specific process for verifying which category applies when it's genuinely unclear? — *A real, defined process, not guesswork or assumption when status is ambiguous.*

Evidence: Status verification process

COMMON REASONS FOR A PARTIAL ANSWER

- **Staff can name the most common category served but not less frequent ones the service still encounters.** — Even infrequent categories deserve genuine, specific awareness, not the risk of misapplied assumptions.
- **Differentiation exists in one provider's own understanding but isn't shared with the wider team.** — Every staff member interacting with patients benefits from the same genuine understanding.
- **A verification process exists but staff are inconsistently confident applying it.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current staff awareness of the specific legal status categories actually served.
Week 2	Build specific, differentiated access guidance for each relevant status category.

When	What
Week 3	Establish a clear verification process for genuinely unclear status.
Ongoing	Refresh staff awareness periodically, particularly for less frequently encountered categories.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
ASK	Status category awareness interview	Asks staff to name the specific legal status categories this service actually serves.
DOCUMENT	Status-specific policy review	Reviews documentation for genuine differentiation across status categories, not a uniform assumption.
DOCUMENT	Verification process review	Reviews the process for verifying status when it's genuinely unclear.

SUPERVISOR TIPS

- **Ask staff to name every specific legal status category the service has served recently.** — Specificity reveals genuine, current awareness rather than a general assumption.
- **Ask what happens when a patient's specific status is genuinely unclear.** — A confident, specific answer reveals a genuine process, not improvisation.

EVIDENCE BASE

[44] WHO's Competency Standards explicitly distinguish these legal status categories throughout, noting that access to health care and legal entitlements vary meaningfully by status and by country, and that health workers need specific awareness of this rather than a single generalised assumption.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

8.10 Care Is Documented and Provided Regardless of Immigration or Legal Status

Care is provided and fully documented for every patient regardless of immigration or legal status, with no differential standard of care, documentation practice, or record-keeping applied based on status — not a lesser or informal standard applied to patients without documented status.

In plain terms: Every patient receives the same care and the same documentation regardless of immigration status — no lower standard, no incomplete record, no 'informal' sessions.

Facility category	Crisis	Transition	Small	Standard
Applicability	Full	Full	Full	Full

WHY THIS MATTERS

The principle is the same across every facility type. In telemedicine, the temptation is to serve undocumented patients 'off the platform' to protect them — which leaves them with no record, no continuity, and no protection. The policy must be explicit: identical care and documentation; status not asked; data protections that actually prevent disclosure to authorities (8.8); funding handled separately.

WHAT GOOD LOOKS LIKE

- Care and documentation are genuinely consistent regardless of status.
- Staff are specifically trained on this principle, not assumed to understand it.
- Confidentiality protection is applied equally without exception.

COMMON FAILURE MODES

- Care or documentation practice differs based on a patient's known or assumed status.
- No specific training addresses this principle.
- Status-related information is handled less carefully than other confidential information.

WORKED EXAMPLE

IN PRACTICE

A telemedicine service serving a mixed-status migrant population.

BEFORE	Some providers saw undocumented patients on personal video apps without creating records, believing this protected them. Those patients had no continuity, no prescriptions on file, no follow-up.
ACTION	A written policy: same care, same platform, same record for everyone; immigration status not asked; data-sharing agreements reviewed to confirm no pathway to immigration authorities; funding handled by the administrator after care. Providers were briefed on why informal care harms patients. All patients were moved onto the platform with records created.
AFTER	The Monitor reviewed the policy, the data-sharing review, and 20 records of migrant patients with full documentation. Verified.

IF YOU ARE STARTING FROM ZERO — DO THIS FIRST

1. Ask providers whether any patients are seen off the platform.
Why?
2. Write the one-sentence policy.
3. Confirm your data agreements do not allow disclosure to immigration authorities.
4. Bring every patient onto the platform with a record.

The most common mistake: Protecting undocumented patients by not documenting them.

SELF-ASSESSMENT QUESTIONS

1. Is the same standard of care applied and documented the same way regardless of a patient's immigration or legal status? — *Genuinely equal treatment, not a lesser or informal standard for undocumented patients.*
Evidence: N/A — tested directly
2. Are staff specifically trained that immigration status is never a reason to withhold or alter care or documentation? — *Specific,*

documented training, not assumed understanding.

Evidence: Staff training record

3. Is patient information protected with the same confidentiality standard regardless of status, with no informal sharing of status-related information? — *The same confidentiality protection extended to every patient, without exception.*

Evidence: N/A — tested directly

COMMON REASONS FOR A PARTIAL ANSWER

- **The principle is understood by treating providers but not consistently by administrative or scheduling staff.** — A patient's first interaction is often with administrative staff, where the same principle needs to hold.
- **Care is consistent but documentation habits vary informally based on individual staff assumptions.** — Consistency needs to extend to documentation practice specifically, not only the clinical care itself.
- **The principle is followed but has never been specifically, formally trained.**

IMPLEMENTATION PLAN

When	What
Week 1	Review current practice for any differential treatment based on status.
Week 2	Establish specific staff training on this principle, covering all staff, not only clinical roles.
Week 3	Confirm documentation practice is genuinely consistent regardless of status.
Ongoing	Reinforce training periodically, particularly for new staff.

HOW THE MONITOR VERIFIES THIS

Method	What	Detail
OBSERVE	Care standard observation	Observes whether care and documentation practice is genuinely consistent regardless of patient status.

Method	What	Detail
DOCUMENT	Staff training review	Reviews training records confirming staff understand immigration status is never a basis for differential care.
ASK	Confidentiality practice interview	Asks staff how patient status information, where known, is protected.

SUPERVISOR TIPS

- **Ask administrative or scheduling staff, not only providers, about this principle.** — This reveals whether the principle genuinely extends beyond clinical staff.
- **Ask how patient status information, where it becomes known, is protected.** — A specific, confident answer reveals genuine practice, not just a stated value.

EVIDENCE BASE

[45] Equal standard of care and documentation regardless of immigration or legal status, without differential record-keeping practice, is established practice in international guidance on healthcare access for migrant and refugee populations.

ASF training courses on GMJ Academy →

Foundation courses A-00 to A-03 are live. Criterion-specific modules are being developed and will link here when published.

← **Telemedicine Standards**
— all standards

Self-assess against these criteria →

← **Standard 7 — Governance & Provider Credentialing**