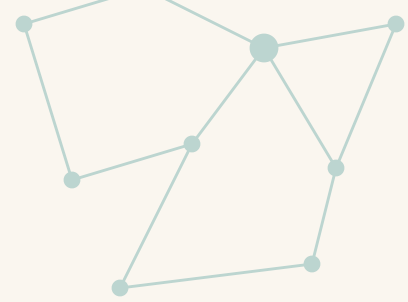


Data Is the DNA of Credentialing



Provider data does not stay in the credentialing file. Other people and systems use it to make decisions about access, operations, payment, and care.

A data defect becomes an enterprise problem when another person or system uses it to make a decision.

WHERE ONE RECORD TRAVELS

Provider record: identity, role, location, privileges, and effective dates

→ **Scheduling**
and patient access

→ **Directories**
referrals, clinical
communication

→ **Enrollment**
claims and payment

→ **Quality**
reporting, analytics,
automation

Note: One incorrect field can create several problems. The impact depends on which decisions rely on it.

The MSP contribution

- 1 Explain what provider information means in real workflows.
- 2 Help define trusted sources, validation rules, and exception paths.
- 3 Bring operational knowledge into governance and technology decisions.

Governance checklist

Shared enterprise ownership needs clear accountability. For each important data element, identify:

- ☐ A named steward
- ☐ An authoritative source
- ☐ A clear definition
- ☐ A validation rule
- ☐ An escalation path when information conflicts

Turn expertise into clear rules

You do not need to become a programmer. You need to explain what the data means and how the organization should handle it.

Data element	What information are we defining?	Meaning	What does it mean in this workflow?
Source	Which source should be trusted?	Owner	Who maintains or validates it?
Relationships	Which organization, location, role, or privilege is it connected to?	Timing	When does it become effective, and when does it end?
Rule	What values or evidence are acceptable?	Exception	What happens when information is missing or sources disagree?

Automate the routine. Keep people accountable for judgment.

TECHNOLOGY CAN HELP WITH

- Document intake and classification
- Data extraction and source comparison
- Expiration monitoring and routine reminders
- Routing, packet preparation, and status updates

PEOPLE REMAIN ACCOUNTABLE FOR

- Competence and clinical relevance
- Conflicting or concerning evidence
- Conduct and privileging decisions
- Exceptions and acceptance of risk

Technology should assemble better evidence and direct attention to the right issues. It should not quietly make decisions that belong to the medical staff or organization.

Three things to make a vendor prove

- 1 Data provenance:** Where did each field come from, when was it checked, and has it changed?
- 2 Relationships and timing:** Can the system connect a practitioner to the correct organization, location, role, privilege, and effective date?
- 3 Exception handling:** What happens when information conflicts, is incomplete, or cannot be confidently matched?

Try this challenge: Give the vendor an imperfect case: conflicting names, multiple locations, an expired document, and a changed group relationship. Ask them to show the source of each field, the audit trail, what happens when the system is uncertain, and how the data can be exported in a usable format.

ONE ACTION TO TAKE THIS WEEK

Choose one recurring provider-data problem. Map where the information starts, where it goes, which decisions depend on it, who is responsible for it, and what should happen when it is wrong.

Your expertise belongs wherever provider data is defined, shared, automated, or used to make decisions.

Adapted from themes discussed during the NAMSS 50th Annual Conference panel, “Data Is the DNA of Credentialing,” facilitated by Brigitte Tebow, nationally recognized Master Data Management leader, including panel responses from Victor M. Vargas, MD, MBA, CPE and Delaine Christie, CPCS, CPMSM, FMSP.