



# Key Artificial Intelligence (AI) Issues Facing U.S. Counties

**PRACTICAL INSIGHTS**

*NACo Executive Technology Reserve Corps*

---

**2026**

# About This Report

---

## What is in this report:

A curated list of 10 key AI-related issues that counties across the U.S. are actively encountering in their IT operations.

## Who compiled this report:

NACo's Tech Xchange team of County Senior Leadership members—with nearly 70 years of hands-on Chief Information Officer (CIO) and Chief Information Security Officer (CISO) experience modernizing county IT—to deliver practical, battle-tested insights.

## How was it compiled:

NACo compiled input for this report provided through direct county feedback and peer networks, as well as real-world implementation attempts and deployments. This input was combined with the authors' experience in navigating counties through past technology shifts—such as Enterprise Resource Planning (ERP) implementations—to respond to county operational challenges.

The AI issues below are organized by theme. Each issue includes why it matters to counties and practical recommendations drawn from real-world county IT modernization efforts.

## Why it matters:

County governments across the United States are entering a period of accelerating AI adoption. Generative AI tools, automated decision systems and AI-powered chatbots are increasingly embedded in permitting, human services, public safety and resident-facing workflows. Yet many jurisdictions still lack the governance frameworks, staffing capacity and implementation experience needed to deploy these technologies responsibly.

The stakes are high: poorly governed AI will expose sensitive constituent data, introduce bias into public services and erode the public trust on which county government depends.

## 1. Legacy Systems and Data Silos Block AI Integration

---

The best way to prepare for newer technology is to ensure your foundational systems are up to date. Counties frequently operate on fragmented, decades-old platforms for core functions like jails, courts, health records, permitting, finance and public safety (CAD/RMS). These systems produce inconsistent, incomplete or inaccessible data, causing AI models to hallucinate, underperform or fail entirely.

### Why it matters:

Counties cannot replace core systems overnight without risking 24/7 operations in public safety, elections or human services. Poor data foundations also amplify downstream risks such as bias and compliance violations.

### Insights and recommendations:

Phased data-readiness approaches can allow counties to progress without full rip-and-replace projects. Key steps include inventorying high-value datasets, implementing lightweight data lakes or federated access layers, and leveraging middleware and integration patterns used in past ERP and Criminal Justice Information Systems (CJIS) projects. Data-quality checklists, interoperability standards such as the National Information Exchange Model (NIEM) and low-risk use cases like document processing or internal chatbots help reduce early failures.

## 2. Counties Struggle with AI Policy Development

---

Most counties lack formal AI inventories, usage policies, oversight bodies or risk-tiering processes. This leads to widespread “shadow AI,” in which staff use unvetted tools for reports, case notes or citizen communications.

### Why it matters:

Counties must comply with the Freedom of Information Act (FOIA), the Commission on Accreditation for Law Enforcement Agencies (CALEA), the Health Insurance Portability and Accountability Act (HIPAA), CJIS and state breach notification requirements. A single uncontrolled use of AI can expose sensitive data, trigger audits or allow pilots to drift into unauthorized areas—such as a chatbot dispensing legal or health advice.

### Insights and recommendations:

Prioritize use cases by strategic value, budget and the impact of success or failure. Build on existing HIPAA, CJIS and CALEA governance with the following measures:

- **Risk-tiered usage policies** with approval workflows and human-in-the-loop requirements for sensitive uses.
- **Cross-departmental steering committees** spanning IT, legal, risk and elected leadership to maintain ongoing oversight.
- **A standardized scoring rubric** evaluating technical feasibility, strategic alignment and measurable public benefit.

- **A tiered risk matrix** classifying projects as Low (internal efficiency), Medium (citizen-facing), or High (resource allocation or enforcement).
- **A registry** of all AI systems in use.

#### Recommended first 90-day action steps for governance:

- **Form an AI Steering Committee** spanning IT, legal, risk management and at least one elected official to provide ongoing oversight.
- **Create an approved AI tools inventory** and require all departments to register tools already in use, including free or personal accounts staff may be using on county work.
- **Adapt existing cybersecurity and data governance policies** to explicitly address AI oversight. Many counties already have the policy infrastructure; it simply needs to be extended to cover AI use cases.

### 3. Workforce Skills Gaps and AI Literacy Deficits

---

County staff—in counties of all sizes—often have limited AI training. Counties can address staff fears by focusing on approved tools and upskilling the existing workforce, rather than on self-guided discovery.

#### Why it matters:

Counties cannot easily recruit specialized AI talent, and uneven literacy slows adoption while increasing risk. This will be increasingly important as AI agents—systems that can autonomously plan and execute multi-step tasks—are adopted, and employees will be required to work with, manage and supervise AI agents.

#### Insights and recommendations:

Role-specific playbooks, AI champion programs and peer mentoring circles help build skills. These approaches mirror past transitions from mainframes to cloud and desktop to mobile computing and can be implemented through existing training budgets or partnerships with community colleges and peer networks.

### 4. Cybersecurity Risks Amplified by AI

---

AI tools increase the potential attack surface. They consume and produce significant amounts of personal and organizational data.

#### Why it matters:

Counties are frequent ransomware targets and must maintain public trust while protecting sensitive information.

Cybersecurity has always been about protecting data, and AI does not change the three core tenets of the CIA Triad—Confidentiality, Integrity and Availability—which remain the foundation for securing AI systems. AI does add a critical component, ethics, addressed in the next section.



*InfoSec Core Principles — the CIA Triad: protecting Confidentiality, Integrity and Availability of data. (medium.com)*

The trusted AI frameworks are risk-based. They include the National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF), Gartner's AI TRiSM (Trust, Risk and Security Management), the Open Worldwide Application Security Project (OWASP) Top 10 for Large Language Models (LLMs), and the EU AI Act, which builds on the foundation the General Data Protection Regulation (GDPR) established in 2018.

### Insights and recommendations:

Cybersecurity fundamentals matter—now more than ever.

1. Define county data for all county staff.
2. Employ multi-factor authentication: 100%, every account, every login.
3. Enact a data backup strategy that is immutable, tested and appropriate to the data being stored.
4. Use the tools that you already have. Ensure your systems, including vendor-supported systems, are properly configured with best-practice security in mind.

Beyond cybersecurity basics: county chatbots are increasingly attacked, and as they evolve into AI agents that plan and execute multi-step workflows, the attack surface grows. Foundational protections start with private AI instances, zero-trust integrations, vendor security reviews and red-team testing, integrated with data minimization, encryption and AI-specific incident response. Given AI agent risks, counties should layer on:

- **Strict human-in-the-loop approval** for critical actions, with semantic validation applied to all inputs and outputs.
- **Least privilege access** by cataloging and restricting agent permissions to only the tools and data each task requires.
- **Behavior “drift” monitoring of agents** that indicates potential manipulation, and security of all third-party plugin integrations.

A pressing and often overlooked threat involves widely used AI assistants such as OpenAI ChatGPT, Anthropic Claude, Google Gemini and Microsoft Copilot. By default, many of these tools save and

AI-Assisted Drafting Notice: Portions of this document may have been developed with the assistance of artificial intelligence tools to support drafting, synthesis or editing. All content has been reviewed, validated and approved by NACo Executive Technology Reserve Corps members and subject matter experts.

reuse the queries and responses users provide. Counties should decide deliberately whether assistants will be browser-based, application-based, or enterprise deployments; who will have access; and how that access will be governed or blocked. Security groups, firewalls and purpose-built LLM firewalls—which can filter and redact prompts, retrievals and responses—are part of a sound control set.

### **An AI cybersecurity and governance readiness checklist—questions every county should be able to answer:**

- Are you incorporating risk management—identifying, assessing, mitigating and continually monitoring AI vulnerabilities and threats—into every stage of the AI lifecycle, and performing annual or semi-annual Information Security Assessments (ISAs)?
- Have you mapped all of your AI data flows, especially those involving sensitive data?
- Have you considered AI legal and regulatory compliance and the potential financial and reputational costs of getting it wrong?
- Do you have an AI security and governance team, and have you taken a holistic approach—cataloging and validating all AI processes?
- Have you performed a risk assessment on your AI vendors?
- Do you maintain a formal, written Information Security Program (ISP) that is reviewed and updated annually, and is your information-security maturity sufficient to support AI—or are you flying blind?
- Are you compliant with existing data-protection laws and keeping pace with new ones?
- Do you monitor AI events, support the reporting of AI compliance issues, and log and track AI findings?
- Do you provide or require security and AI awareness and proficiency training, and do you have stakeholder support and reporting in place?
- **Bottom line: Is your organization AI trustworthy?**

## **5. Bias, Equity and Ethical Concerns in Public Service AI**

---

AI used for eligibility screening, sentencing support or resource allocation can reinforce historical bias.

### **Why it matters:**

Counties serve diverse communities with varying needs and experiences. As AI becomes more integrated into public services and operations, county leaders must ensure these tools support fair and equitable outcomes. Proactively addressing bias helps protect public trust, improve service delivery and ensure that all residents benefit from innovation.

### **Insights and recommendations:**

Bias audits, disparate-impact testing and community engagement strategies can help ensure fairness. Mandatory impact assessments and diverse oversight committees support ethical AI deployment.

XAI (Explainable AI) is a critical part of AI ethics, which refers to being able to explain the logic and decisions made by the model, providing truth through transparency. - providing .

## 6. Procurement Challenges and Vendor Management

---

Traditional procurement rules often conflict with the rapid evolution of AI technologies.

### Why it matters:

Counties must commit to multi-year contracts while AI tools change quickly, increasing risk if a solution underperforms. All technology contracts need to be reviewed for AI use, and county IT policies regarding AI need to be incorporated into all contracts, even non-technical ones, such as services contracts, to best agree how your providers can use AI in delivering products and services to you.

### Insights and recommendations:

Model RFPs, responsible AI evaluation criteria, audit rights and bias-testing clauses should be included in contracts. Pilot-first procurement strategies allow counties to evaluate tools before long-term commitments. Vendor AI questions from sources such as the GovAI Coalition are valuable resources.

### Recommended contract protections:

- **Require a structured pilot period** (60–90 days) using real county data and workflows before committing to a multi-year contract. Ensure the pilot operates in a sandbox so that any county data ingested can be removed after the pilot, if necessary.
- **Negotiate shorter initial terms** (1–2 years) with renewal options tied to measurable performance milestones, rather than locking into standard 3–5 year agreements.
- **Include explicit audit rights and explainability requirements** so counties can inspect model behavior, challenge outputs and verify that the system remains accurate over time. Contracts should clearly identify who owns the data.

## 7. Scaling AI Pilots, Budget Constraints and Managing Shadow AI

---

Counties navigating AI adoption face three interconnected pressure points: sustaining pilots beyond the proof-of-concept stage, absorbing the unpredictable cost structures associated with consumption-based AI tools and controlling the spread of unsanctioned employee use when approved options are limited. These challenges do not resolve on their own, they require deliberate action across fiscal planning, governance policy and outcome measurement.

### Why it matters:

Taxpayer-funded environments demand measurable value. Stalled pilots erode public credibility, while budget structures built around fixed annual allocations are poorly matched to Application Programming Interface (API)-driven pricing that can spike at various times during the year. Meanwhile, when employees independently adopt AI tools outside approved systems, sensitive constituent data can be exposed without any governance guardrail in place. Without structured

approaches to budgeting, policy enforcement and performance measurement, counties risk both fiscal overruns and reputational harm.

### Insights and recommendations:

Approaches from prior county technology projects translate well to AI—but require both fiscal discipline and structured outcome measurement.

### Planning and budgeting:

- **Define success criteria early** and align phased road maps to budget cycles.
- **Earmark a percentage of IT funds** for ongoing digital compliance and remediation.
- **Establish a budget reserve** for token-based or pay-as-you-go tools to absorb mid-year usage spikes.
- **Offset rising AI costs** by continuing to automate high-volume, revenue-generating workflows such as property assessments.
- **Pursue consortiums or partnerships** to share specialized infrastructure and data science expertise.

### Curbing shadow AI:

- **Provide sanctioned enterprise AI toolkits** with built-in controls so staff do not reach for unvetted tools.
- **Update acceptable-use policies** and pair them with safe-usage training.

### Measuring outcomes:

- **Tie return on investment (ROI) calculators to county metrics** such as processing time and error rates to guide scaling decisions.
- **Commission independent audits** to verify AI systems remain accurate and unbiased after deployment.
- **Open resident feedback channels** so users can flag errors that feed back into retraining.
- **Publish public-facing dashboards** reporting on AI accuracy, throughput and error rates.

## 8. Lack of Transparency, Explainability, and Public Accountability

---

“Black-box” AI decisions in permitting, benefits or enforcement raise due-process, FOIA and trust issues.

### Why it matters:

Counties operate under open-government laws and direct public scrutiny.

### Insights and recommendations:

Explainability requirements, audit logs and public dashboards developed for citizen-facing systems can be applied to AI. Plain-language explanations and transparency reports help meet FOIA obligations and maintain accountability.

## 9. Regulatory Compliance Across Fragmented Jurisdictions

---

AI-Assisted Drafting Notice: Portions of this document may have been developed with the assistance of artificial intelligence tools to support drafting, synthesis or editing. All content has been reviewed, validated and approved by NACo Executive Technology Reserve Corps members and subject matter experts.

Counties must navigate evolving federal (NIST AI RMF), state and local rules while managing cross-jurisdictional services such as multi-county health or justice systems.

### Why it matters:

Regulatory requirements for AI, accessibility, privacy and digital services continue to evolve. Counties that proactively incorporate compliance into AI planning are better positioned to avoid costly disruptions, strengthen public trust and scale innovation responsibly.

### Insights and recommendations:

Mapping tools, compliance playbooks and peer networks help counties track evolving requirements. On accessibility specifically:

- **Build accessibility into AI interfaces** (chatbots, data visualization) with ADA keyboard navigation and ARIA markup.
- **Vet AI hiring tools carefully** so candidates with disabilities are not screened out—e.g., video tools that misread speech patterns or facial expressions.
- **Verify AI-generated summaries** of complex documents rather than relying on them unchecked.
- **Avoid accessibility overlay widgets**, which face mounting litigation and can disrupt users' own screen readers.
- **Pair automated remediation with manual testing** by people with disabilities for real-world usability.
- **Require Voluntary Product Accessibility Templates (VPATs)** in procurement for all new AI software so vendors are legally accountable for accessibility.
- **Publish a clear accommodations process** telling the public how to request alternatives when an AI-driven service is hard to use.

## 10. Build and Maintain Public Trust in AI-Driven Services

Skepticism from constituents and elected officials about AI replacing human judgment in benefits, permitting or emergency response can slow adoption or create backlash.

### Why it matters:

AI is not just a technology challenge; it is a human perception challenge as well. Counties need to address both. Trust is foundational to county legitimacy and service uptake. Internally, AI gains stall when cultural fear or training gaps fuel resistance, so change must be managed at the organizational level too.

### Insights and recommendations:

Address external trust and internal change management in parallel.

### Building public trust:

- **Use communication playbooks** and pilot transparency reports drawn from previous technology rollouts.
- **Be clear about when AI is used.**

AI-Assisted Drafting Notice: Portions of this document may have been developed with the assistance of artificial intelligence tools to support drafting, synthesis or editing. All content has been reviewed, validated and approved by NACo Executive Technology Reserve Corps members and subject matter experts.

- **Engage residents directly** through town halls and plain-language FAQs.
- **Frame AI as augmentation** under human oversight, not as a replacement for staff judgment.

### Managing internal change:

- **Engage staff early** on AI's impact on job descriptions and reskilling needs to head off grievances.
- **Involve frontline workers** in co-designing AI tools so new systems complement rather than disrupt workflows.
- **Build a grassroots champions network** who can mentor colleagues, drive adoption and provide oversight while using engagement data to recognize emerging expertise.
- **Codify human accountability** in policy: designated humans remain the final decision-makers responsible for validating AI outputs.

## Moving Forward: Counties Do Not Have to Navigate This Alone

---

County governments are at an inflection point. AI adoption is no longer optional—it is already happening across departments nationwide, with or without governance structures in place. The question is not whether counties will use AI, but whether they will do so responsibly. The governance frameworks, phased implementation strategies and procurement protections outlined in this paper provide a practical path forward—one grounded in fiscal discipline and operational experience rather than vendor promises or one-size-fits-all mandates.

The NACo Executive Technology Reserve Corps understands the political, fiscal and operational constraints unique to county government because its members have lived them. They have led ERP implementations that survived budget cuts, built cybersecurity programs with skeleton crews, and managed technology modernization through elected leadership transitions. As AI adoption accelerates, that kind of trusted, peer-based advisership is exactly what county leaders need—to modernize confidently, protect their constituents and build the institutional capacity to govern AI responsibly for years to come.

## References

---

- GovAI Coalition. (2024). Artificial intelligence procurement guide for state and local governments. GovAI Coalition. <https://www.govaicoalition.org>
- National Association of Counties (NACo). (2024). AI County Compass: A guide to artificial intelligence for county governments. NACo. <https://www.naco.org/resources/ai-county-compass>
- National Institute of Standards and Technology (NIST). (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>
- National Information Exchange Model (NIEM). (2023). National Information Exchange Model standards and guidance. <https://www.niem.gov>
- U.S. Department of Justice. (2023). Criminal Justice Information Services (CJIS) security policy (Version 5.9.4). Federal Bureau of Investigation. <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>
- U.S. Department of Health and Human Services. (2023). HIPAA security rule guidance. Office for Civil Rights. <https://www.hhs.gov/hipaa/for-professionals/security/index.html>
- U.S. Department of Justice. (2024). Americans with Disabilities Act Title II web and mobile app accessibility final rule. <https://www.ada.gov/resources/2024-03-08-web-rule>
- U.S. General Services Administration. (2024). AI use cases in government: Federal agency practices and guidance. Office of Government-wide Policy. <https://www.gsa.gov/technology/artificial-intelligence>
- IBM Institute for Business Value. (2023). The ethics of AI: Building trust and transparency in artificial intelligence. IBM Corporation. <https://www.ibm.com/thought-leadership/institute-business-value/report/ai-ethics>
- Partnership for Public Service. (2024). Building the workforce of tomorrow: AI readiness in government. <https://ourpublicservice.org/publications>