AI in Physician Practices: Compliance, Risk, and Contracts

Elizabeth Shirley, CIPP/US, CIPM, AIGP
Partner, Birmingham

BURR & FORMAN

Agenda

1. Legal Issues When Using AI in Patient Care and EHR Workflows
2. Implicated Laws, Regulations, and Standards
3. Risks and Benefits of GenAI in Clinical and Administrative Settings
4. AI Vendor Due Diligence for Physician Practices
5. Contract Provisions to Include in AI Vendor Agreements
6. Practical Checklist

BURR&FORMAN

Part 1: Legal Issues in Using AI for Patient Care and EHRs

BURR & FORMAN

Part 1: Legal Issues in Using AI for Patient Care and EHRs

- **Privacy and security of PHI**. Any AI that processes PHI raises HIPAA Privacy and Security Rule issues.
- **FDA oversight for clinical AI**. Software functions that analyze or interpret patient-specific data for diagnosis or treatment may be regulated as medical devices.
- **For tools claiming to be non-device decision support**, confirm that a healthcare professional can independently review the basis of the recommendation.
- **EHR (Electronic Health Record) and interoperability obligations**. AI features embedded in certified EHR technology must align with applicable certification criteria and information blocking rules.

BURR & FORMAN

Part 1: Legal Issues in Using AI for Patient Care and EHRs

- **Patient rights and transparency**.
- **Bias, fairness, and civil rights**.
- **Professional liability and standard of care**. Automation bias and overreliance on AI can lead to clinical errors.
  - Healthcare providers must also adhere to risk management frameworks.
  - Human in the loop.
- **Web and mobile technologies**.
- **Inventory current and planned AI tools.**

BURR&FORMAN

Part 2: Implicated Laws, Regulations, and Standards

BURR & FORMAN

Part 2: Implicated Laws, Regulations, and Standards

- **HIPAA Privacy and Security Rules**.
  - Limit uses/disclosures to permitted purposes,
  - Implement administrative/physical/technical safeguards,
  - Conduct risk analyses, and
  - BAAs with vendors handling PHI.
- **FDA regulation of clinical AI**.
- **ONC (Office of the National Coordinator) certification and information blocking**.

BURR&FORMAN

Part 2: Implicated Laws, Regulations, and Standards

- **The FTC polices unfair or deceptive practices.**
  - **FTC Health Breach Notification Rule** requires vendors of PHI records and related entities to notify consumers following a breach involving unsecured information.
- **Comprehensive privacy laws** (e.g., California, Colorado, Connecticut, Virginia, etc.)
  - Notice
  - Data privacy rights
  - Privacy Policy
  - Data governance obligations

BURR&FORMAN

Part 2: Implicated Laws, Regulations, and Standards

- **CCPA ADMT Regulations:**
  - ADMT is "any technology that processes personal information and uses computation to replace human decision-making or substantially replace human decision-making."
  - "Significant decisions" include determinations that impact health care services.
  - Before collecting personal information for ADMT's use, businesses must post clear notices to consumers:
    - Purpose of the business's ADMT use,
    - Consumer's right to opt out and how to exercise this right,
    - Consumer's right to access certain information about the business's ADMT,
    - Description of how the ADMT works, what data influences its outputs, and how its outputs are used to make a significant decision,
    - Alternative decision-making process if the consumer opts out of the use of ADMT, and
    - Statement prohibiting retaliation against a consumer for exercising his or her right to access this information.

Part 2: Implicated Laws, Regulations, and Standards

- **CCPA ADMT Regulations:**
  - Consumers must have the option to opt out of ADMT used for significant decisions, subject to narrow exceptions.
  - Upon request, businesses must provide:
    - The purpose of their ADMT use,
    - Information about the logic of the ADMT,
    - How outputs were used in decision-making, and/or
    - Plans for future use of outputs.
  - **Businesses must conduct risk assessments for ADMT used in significant decisions**.
    - Risk assessments must determine "whether the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing."

BURR&FORMAN

Part 2: Implicated Laws, Regulations, and Standards

- **Security and AI governance standards**. NIST AI Risk Management Framework and the NIST Cybersecurity Framework provide practical governance structures for identifying, measuring, and mitigating AI and cybersecurity risks.

BURR & FORMAN

Part 3: Risks and Benefits of GenAI in Healthcare Practices

BURR & FORMAN

Part 3: Risks and Benefits of GenAI in Healthcare Practices

- **Hallucinations, outdated or non-localized medical content, poor sourcing, and automation bias** can harm patients.
- **Privacy and security risks**. Exposure of PHI during prompt entry, model training on your data without proper authorization, data leakage to third parties, and cyberattacks on AI pipelines.
- **Bias, fairness, and equity risks**. Training data gaps and proxy variables can drive disparate outcomes.
  - Bias assessment documentation
  - Training data composition
  - Independent auditor credentials
  - Audit recency

BURR&FORMAN

Part 4: AI Vendor Due Diligence for Physician Practices

BURR & FORMAN

Part 4: AI Vendor Due Diligence for Physician Practices

- **Determining the Use Case.**
- **Assess vendor stability**, leadership experience in healthcare, and regulatory track record. Review any prior breaches, recalls, or enforcement actions.
- **Data governance and PHI handling**.
- **Model transparency and performance**.
- **Review bias assessments** across demographics, monitoring plans, and procedures for addressing adverse events.
- **Evaluate security program** maturity against recognized frameworks.
- **Understand how model updates are tested, documented, and communicated**.
- **Review service levels, uptime, disaster recovery, backup and restoration testing, and incident response**.

Establish a standard AI due diligence questionnaire and require proof before procurement.

BURR & FORMAN

Part 5: Contract Provisions for AI Vendor Agreements

BURR & FORMAN

Part 5: Contract Provisions for AI Vendor Agreements

- **Roles and data rights**. Clearly define covered entity and business associate roles and execute a robust BAA.
- **Regulatory compliance representations**. Require representations and warranties of compliance with applicable law and security standards.
- **Security commitments and audits**. Mandate administrative, physical, and technical safeguards appropriate to PHI.
- **Breach and incident response**. Set breach definitions aligned to HIPAA and state laws, tight notification timelines, cooperation obligations, forensic support, and allocation of costs for regulatory notifications, mitigation, and credit monitoring where legally required.
- **Insurance**.
- **Define service levels.** Require response and resolution times, and maintenance windows.
- **Require human-in-the-loop design**, configurable thresholds (permitted limits that, when breached, cause alerts), and safety guardrails.

BURR&FORMAN

Part 5: Contract Provisions for AI Vendor Agreements

- **Change management**. Establish notice and approval processes for material updates.
- **Bias testing and remediation**. Obligate the vendor to conduct pre- and post-deployment bias analyses.
- **IP and content warranties**. Secure warranties of non-infringement.
- **Indemnification and insurance**. Obtain indemnities for data privacy/security violations, regulatory penalties arising from vendor breaches, IP infringement, product liability for device-regulated features, and third-party claims.
- **Liability framework**. Negotiate meaningful caps with carve-outs for breaches of confidentiality, data security incidents, IP infringement, willful misconduct, and violation of law.
- **Subcontractors and flow-downs**. Require pre-approval of subcontractors handling PHI or model components and flow-down of all privacy, security, transparency, and audit obligations.
- **Termination and transition**. Provide termination rights for material breach, security incidents, failure to meet regulatory requirements, or significant performance degradation.

Practical Checklist

BURR & FORMAN

Practical Checklist

- Inventory AI tools, categorize by clinical vs. administrative use, and map applicable laws.
- BAAs with precise data-use restrictions.
- AI governance committee, adopt NIST-aligned AI risk management, and define acceptable use policies.
- Configure human oversight, logging of AI-influenced decisions, and routine bias/performance monitoring.
- Calibrate coding/documentation guardrails and auditing to manage revenue integrity risks.
- Standardize vendor due diligence and require transparency artifacts and security attestations.
- Update contract playbooks: compliance reps, data rights, change control, bias remediation, and indemnities.

BURR&FORMAN

Questions?

BURR & FORMAN

About the Speaker

Elizabeth Shirley, CIPP/US, CIPM, AIGP

Partner, Birmingham

T: 205.458.5186

E: bshirley@burr.com

Elizabeth has 25 years of experience in advising clients on commercial litigation, cybersecurity, and data privacy matters. As Co-Chair of Burr & Forman's Cybersecurity and Data Privacy Team, she counsels clients on data privacy law compliance, data breach response and investigations, breach notification, privacy programs, electronic contracts, and litigation arising from these areas and other commercial business relationships. Her commercial litigation practice also focuses on breach of contract, fraud, intellectual property rights, and breaches of other legal duties or obligations.

Elizabeth holds both a CIPP/US certification as a Certified Information Privacy Professional and a CIPM/IAPP certification as a Certified Information Privacy Manager and represents companies of varying sizes and industry sectors in cybersecurity matters. She also holds an AIGP certification from the IAPP.

BURR&FORMAN

Thank you

Connect with us | www.burr.com

www.linkedin.com/company/burrforman

BURR&FORMAN