Session 2 Handout: Laws, Contracts, and Data

FAST-10 AI Governance, Risk, Ethics, and Responsible Use · 7formations · Instructor: Wadood Chaudhary · All examples fictional · Training, not legal advice

> **Training, not legal advice.** This handout summarizes rules as of October 2026 so you can spot issues. Confirm specific duties with counsel.

Why this session matters

Massachusetts has no general AI statute as of October 2026, but that does not mean AI is unregulated. The Attorney General's April 2024 advisory makes the point directly: existing consumer-protection, anti-discrimination, and data-security laws apply to AI. Most AI risk for a small business comes from putting the wrong data in the wrong tool, or letting AI influence decisions about people.

Key concepts

1. G.L. c. 93H and 201 CMR 17.00

- **Personal information:** a Massachusetts resident's first name or first initial and last name **plus** an SSN, a driver's license or state ID number, or a financial account or credit/debit card number.
- **201 CMR 17.00:** a written information security program (WISP) with safeguards, employee training, and **vendor oversight**: select vendors that can protect the data and require it by contract.
- **Breach:** notify affected residents, the **Attorney General**, and the **Office of Consumer Affairs and Business Regulation**, as soon as practicable and without unreasonable delay.
- Pasting personal information into an unapproved AI tool can be an unauthorized disclosure.

2. HIPAA and AI

- PHI only in tools covered by a **business associate agreement** (BAA), for a use the policy allows.
- **Minimum necessary:** share only what the task needs.
- Chatbots, transcription, and ambient tools need special review.
- Breach of unsecured PHI: notify individuals without unreasonable delay, **no later than 60 days**; HHS; media if 500+ in a state.

3. Fairness in hiring and lending

- AI screening can repeat past bias. **G.L. c. 151B** prohibits employment discrimination, however the decision is made.
- Credit: adverse-action notices need **specific reasons**, even with complex models (CFPB Circular 2022-03).
- Insurance: Division of Insurance Bulletin 2024-10 expects insurers to govern AI-supported decisions.
- Other states: **Colorado SB26-189** (May 2026) replaced the 2024 Colorado AI Act and applies to automated decisions about Colorado residents from January 1, 2027.

- Keep a human decision-maker for decisions about people; test outputs across groups.

4. EU AI Act (if you sell into the EU)

Date	What applies
Feb 2, 2025	Prohibited practices; AI literacy
Aug 2, 2025	General-purpose AI model obligations
Aug 2, 2026	Most transparency obligations
Dec 2, 2027	High-risk systems in Annex III (for example, employment, credit), as moved by the 2026 AI Omnibus
Aug 2, 2028	High-risk AI in regulated products (Annex I)

5. Vendor terms: the five questions

1. Are our inputs used to train the vendor's models?
2. How long are prompts and files kept, and can we delete them?
3. Where is data stored, and who can access it?
4. What does the vendor do, and how fast, on a breach?
5. Is a BAA (or other required agreement) available, and on which plan?

Business plans often differ from free plans.

Worked example (fictional)

Charles River Family Dental compared two chatbot vendors. Vendor A: no training on inputs, 30-day retention, U.S. storage, BAA on the Business plan, 72-hour breach notice. Vendor B: trains on inputs unless you opt out, keeps data while the account is active, any-country processing, no BAA. **B is disqualified for PHI.** A is acceptable with conditions: signed BAA, correct plan, retention set, breach contact named, WISP updated.

Checklist

- ☐ Each AI use mapped to the data it touches.
- ☐ Obligations listed per use (93H/17.00, HIPAA, 151B, credit, contract).
- ☐ Vendor terms answered for each approved tool.
- ☐ Questions for counsel written down.

Do and don't

Do	Don't
Read the actual terms for your plan	Rely on the vendor's marketing page
Keep people deciding about people	Let AI reject applicants or deny credit on its own
Note the date you read each term	Assume terms never change