What Regulators Actually Look for in Privacy Programs: Lessons from HIPAA OCR, DOJ Bulk Data, and Global Enforcement Trends

Dr Bridget Bratt

How Regulators See Your Privacy Program

Two Views of Privacy Maturity

- Most organizations evaluate privacy maturity by what they've *built*: policies, frameworks, and governance bodies.

- Regulators evaluate maturity by what they can *verify*: how data is controlled, monitored, and restricted in real time.
  This gap — not intent — is where enforcement begins.

The Maturity Myth

The disconnect:

- “We have policies, committees, and frameworks”

  vs.

- “Show me how the data is actually protected”

Why organizations *feel* mature—but fail regulatory scrutiny

Key thesis:

- Regulators don’t audit intentions. They audit **evidence of control in operation**.

How Regulators Actually Conduct Reviews

What regulators are *not* impressed by:

- Aspirational policies
- Unused governance committees
- One-time risk assessments

What regulators consistently do:

- Trace **data** → **access** → **use** → **oversight**
- Ask for proof, not promises

Common review patterns across:

- HIPAA OCR
- DOJ Bulk Data reviews
- Financial services and global regulators

The Evidence-First Shift in Privacy Enforcement

What “evidence-first” actually means

- Controls must be:
  - Implemented
  - Measurable
  - Defensible
- Documentation must be:
  - Generated by operations—not written for audits

Regulators now expect proof of:

- Continuous control operation
- Monitoring and validation
- Governance decisions tied to real risk

The Five Control Areas Regulators Prioritize

Data Discovery & Classification at Scale

- Ability to *find* regulated, sensitive, and high-risk data
- Not just labels—but coverage, accuracy, and tuning
- Why "we don't know where the data is" is no longer defensible

Role-Based Access & Service Account Governance

- Least privilege enforced—not theoretical
- Service accounts as a top regulatory red flag
- Clear ownership, lifecycle controls, and monitoring

Audit-Ready Evidence Trails

- What regulators actually ask for:
  - Access logs
  - Incident artifacts
  - Exception approvals
  - Data lifecycle records
- Why screenshots ≠ evidence

Operationalized Processes

- How policies become:
  - Intake workflows
  - Approval paths
  - Enforcement mechanisms
- Regulators test execution—not wording

Cross-Regulatory Sensitivity Alignment

- Overlapping risk categories across:
  - HIPAA
  - GLBA
  - DOJ bulk & derived data
  - CFIUS-implicated data
- Why siloed compliance fails under scrutiny

What Enforcement Is Expanding *Beyond* Breaches

- Shift from “incident-only” enforcement to:
  - Overcollection
  - Purpose drift
  - Algorithmic use
  - Weak governance of derived data
- Emerging focus areas:
  - AI training data
  - Service account abuse
  - Unvalidated internal data sharing
- Global trend toward proactive examinations

What Actually Holds Up Under Scrutiny

Programs that survive reviews have:

- Evidence mapped directly to risk
- Repeatable, testable processes
- Clear accountability
- Technical controls aligned to legal obligations

Programs that fail reviews rely on:

- Policy volume
- Assumptions
- One-time documentation
- Unverified claims

Closing: Building a Defensible Privacy Program

- Stop designing for *optics*
- Start designing for *explainability*
- Ask the right internal question:

"If a regulator asked for proof tomorrow, could we produce it—quickly and confidently?"

Guidepost

HOW CAN WE HELP YOU?

CHALLENGE OR OPPORTUNITY, WE KEEP YOU MOVING FORWARD.

Guidepost

guidepostsolutions.com

WE ARE YOUR GUIDEPOST.