WHAT REGULATORS ACTUALLY LOOK FOR IN PRIVACY PROGRAMS: LESSONS FROM HIPAA OCR, DOJ BULK DATA, AND GLOBAL ENFORCEMENT TRENDS

Dr Bridget M. Bratt
Managing Director, Privacy Regulations and Enforcement, Guidepost Solutions

Joseph A. Emerson
Managing Director, Privacy and Data Protection, Protiviti

Organizations frequently invest in sophisticated privacy frameworks, yet many continue to overlook the operational elements that regulators prioritize when evaluating the maturity and effectiveness of privacy programs. Across sectors—including healthcare, insurance, financial services, gaming, and consumer technology—there remains a persistent disconnect between internal perceptions of compliance and the evidence regulators actually expect to see during investigations and reviews. This extended abstract addresses that gap by providing a practical, experience-based examination of how regulators assess privacy programs, drawing on direct involvement with HIPAA Office for Civil Rights (OCR) inquiries, U.S. Department of Justice (DOJ) Bulk Data and cross-border data restrictions, and a range of international enforcement regimes.

The Shift from Policy-Centric to Evidence-Centric Evaluation

Regulators increasingly evaluate privacy as an operational discipline rather than a documentation exercise. Written policies remain necessary, but their value is contingent upon demonstrable proof that the associated controls operate effectively in practice. As such, regulators routinely request artifacts that validate operational maturity, including:

- Evidence of functional data classification and scanning capabilities;
- Comprehensive access control inventories, including service and system accounts;
- System-level logs confirming least-privilege enforcement and appropriate access;
- Documentation of incident assessments, containment actions, and post-incident remediation;
- Data lifecycle evidence covering retention, deletion, and minimization practices grounded in system capabilities.

Technical Governance as a Core Privacy Control

Modern enforcement actions demonstrate that privacy oversight cannot be separated from technical governance. Regulators now routinely examine areas previously considered the domain of IT or security, including:

- Credential and key management hygiene;
- Segregation of duties between administrators, developers, and operations;
- Technical enforcement of privacy and data-handling policies;
- Accurate mapping of data flows across cloud, on-premises, and hybrid environments;
- Controls for high-risk data categories, including HIPAA PHI, DOJ-restricted data, biometric identifiers, and bulk datasets with national security implications.

Cross-Regulatory Expectations and Points of Convergence

Although regulatory frameworks vary in scope and terminology, they increasingly share common expectations. This presentation compares these converging priorities, with emphasis on:

- HIPAA OCR: persistent focus on risk analysis, system-level access controls, and complete, reviewable audit logs;

- DOJ Bulk Data & Cross-Border Rules: heightened expectations for classification accuracy, exporter controls, technical restrictions, service-account governance, and ability to detect and mitigate anomalous data activity;
- GLBA & Financial Sector Regulators: alignment with verifiable security governance, data minimization, vendor oversight, and operational control validation;
- International Regulators: increased scrutiny of transparency, purpose limitation, cross-border transfers, and sensitive data handling in both consumer and enterprise contexts.

Common Misconceptions and Recurrent Gaps

Drawing from practical experience supporting organizations through regulatory examinations, the session will highlight recurring misconceptions that contribute to findings, remediation requirements, and prolonged regulatory oversight. These include:

- Overconfidence in policies that do not reflect system behavior;
- Insufficient evidence of required safeguards, particularly related to access control;
- Limited visibility into cloud data locations, flows, and retention behaviors;
- Inadequate governance over vendor and service-account access;
- Misalignment between stated deletion practices and actual technical capabilities.

Emerging Enforcement Trends

The session concludes with an analysis of regulatory trends that will shape the next generation of privacy enforcement. These include:

- Increased scrutiny of AI governance, training data composition, and sensitive-data restrictions;
- Stronger cross-border controls for bulk, inferred, or aggregated datasets;
- Greater accountability for non-human identities and privileged service accounts;
- Elevated expectations for continuous monitoring, anomaly detection, and incident escalation;
- Expanded definitions of high-risk data categories, particularly where national security concerns intersect with consumer privacy.

By synthesizing these themes, the session provides policymakers, practitioners, and privacy leaders with actionable insight into the evidence-based expectations regulators apply in practice. Attendees will gain a clearer understanding of how to align privacy frameworks with real-world regulatory priorities, strengthen operational resilience, and bridge the longstanding divide between theoretical compliance and demonstrable program maturity.