AI IN HEALTHCARE: EMPLOYEE WHISTLEBLOWER AND RETALIATION COMPLAINTS—WHAT YOU NEED TO KNOW

Date: 22 December 2025

US Labor, Employment, and Workplace Safety Alert

By: Isabella F. Sparhawk

As artificial intelligence (AI) tools integrate into clinical labs and diagnostics, healthcare employers face greater risk of whistleblower and retaliation claims by employees who report concerns about how these tools are being used. While AI driven diagnostic support systems, automated lab processes, intelligent workflow automation, and other AI tools can increase efficiency, they can also create patient safety, privacy, data misuse, and other legal and regulatory compliance issues if they are not used correctly, if they are relied upon too heavily, or if there is insufficient human oversight and analysis. A federal bipartisan AI whistleblower law was introduced in May 2025 and is in its early stages.[1] While this bill makes its way through Congress and federal efforts to preempt state AI laws advance, employers must be aware that employees who report concerns about AI tools in healthcare diagnostics may be protected by existing whistleblower laws. Employers who mishandle those complaints may face costly litigation, reputational harm, and regulatory scrutiny.

EXISTING WHISTLEBLOWER STATUTES

Employees who raise concerns about AI use in clinical labs and diagnostics may be protected by the following laws[2]:

The Occupational Safety and Health Act

Employees who report that AI tools are creating an unsafe work condition or jeopardize patient safety may be protected under the Occupational Safety and Health Act (OSH Act), which requires employers to maintain safe working conditions for their employees.[3] For example, a lab technician who reports that an AI-driven diagnostic tool put a patient's safety at risk because it produced inaccurate cancer test results may be afforded protection under the OSH Act. Failure to properly handle such reports can trigger Occupational Safety and Health Administration investigations, citations, and penalties.

The Health Insurance Portability and Accountability Act

Employees who report that AI tools are mishandling protected health information (PHI) may be protected under the Health Insurance Portability and Accountability Act (HIPAA). AI systems that access, process, or generate PHI must comply with HIPAA's Privacy and Security Rules, which prohibit the use and disclosure of PHI without patient authorization, except for treatment, payment, or healthcare operations. Failure to properly handle such reports can result in privacy-related lawsuits and investigations by the Office for Civil Rights. For example, a case pending in the US District Court for the Northern District of California, San Francisco, *Sloan v. Verily Life Sciences*

©2005-2026 K&L Gates LLP. All Rights Reserved.

LLC,[4] concerns a former executive who is alleging that his employer retaliated against him after he reported HIPAA breaches involving unauthorized use of patient data by AI systems.

The False Claims Act

Employees who report that AI tools are misclassifying tests and thereby generating fraudulent bills to Medicare or Medicaid may be protected under the False Claims Act (FCA).[5] The FCA imposes liability on any person who submits a false or fraudulent claim for payment to the federal government. For example, if an AI diagnostic test misclassifies normal results as "abnormal," this error could cause the provider to order additional tests that are not medically necessary and bill the unnecessary tests to Medicare, which could constitute a false claim under the FCA. Failure to properly handle such FCA reports may lead to monetary penalties.

State Whistleblower Statutes

Finally, many state laws also protect employees who report legal violations or public health risks associated with AI use. The Trump administration's recent Executive Order, *Ensuring a National Policy Framework for Artificial Intelligence*, aims to establish a national AI policy framework and preempt conflicting state AI laws.[6] Employers should maintain compliance with current state mandates while monitoring federal guidance and litigation.

PROPOSED AI WHISTLEBLOWER STATUTE

Congress is considering the bipartisan AI Whistleblower Protection Act (S.1792, H.R.3460), which was introduced on 15 May 2025, by Senators Chuck Grassley (R-IA) and Chris Coons (D-DE) in the Senate and Representatives Jay Obernolte (R-CA) and Ted Lieu (D-CA) in the House of Representatives. The bills were referred to the Senate Health, Education, Labor and Pension and House Energy and Commerce Committees, each with at least one cosponsor on the committee of jurisdiction, which increases the likelihood of committee consideration. Various whistleblower and AI groups have voiced their support for the bills, including the National Whistleblower Center,[7] the Center for Democracy and Technology, and the Government Accountability Project. While the proposed legislation is not limited to the healthcare industry, the bill would make it illegal to retaliate against current and former employees and independent contractors who report AI security vulnerabilities or violations, including those that create risks to patient safety, data privacy, or regulatory compliance.

BEST PRACTICES

Healthcare employers are at the intersection of AI innovation and increasing regulatory oversight. As AI continues to reshape healthcare diagnostics, whistleblower protections will likely expand, both legislatively and through enforcement. Proactively preventing retaliation claims can reduce legal risk and strengthen employee trust in AI-related changes.

Best practices include:

Develop Reporting Policies and Retaliation Protections

Maintain up-to-date policies on reporting AI-related errors, including policies for protections against retaliation.

Create Robust Reporting Channels

©2005-2026 K&L Gates LLP. All Rights Reserved.

Establish internal systems for employees to raise concerns about AI tools confidentially, with documented investigation protocols.

Maintain Clear AI Governance Policies

Define how AI tools are implemented, validated, and monitored. Establish clear frameworks for accountability, transparency, fairness, and safety. Assign responsibility for quality assurance and compliance.

Train Supervisors and Managers

Educate leaders on how to respond appropriately to complaints, emphasizing nonretaliation obligations under federal and state law.

Audit Vendor Contracts

Ensure contracts with AI providers include compliance, quality control, and liability-sharing provisions.

Document Corrective Actions

When issues are raised, record all investigations and remediation efforts to demonstrate good faith compliance.

Risk Management

Conduct regular audits, risk assessments, and bias testing of AI systems. Monitor performance and address issues promptly. Organizations must conduct regular risk assessments, vulnerability scanning, and penetration testing for AI systems. Technical safeguards include encryption, access controls, and data anonymization.

Our Labor, Employment, and Workplace Safety lawyers regularly counsel clients on a wide variety of topics related to emerging issues in labor, employment, and workplace safety law, and they are well-positioned to provide guidance and assistance to clients on AI developments.

FOOTNOTES

[1] The AI Whistleblower Protection Act (S. 1792) (H.R. 3460)

[2] This list is not all inclusive. Employers should contact K&L Gates if they are interested in laws that impact their workforce.

[3] 29 U.S.C. § 651 *et seq*.

[4] *Sloan v. Verily Life Scis. LLC*, No. 24-CV-07516-EMC, 2025 WL 2597393 (N.D. Cal. Sept. 8, 2025)

[5] 31 U.S.C. §§ 3729–3733.

[6] Exec. Order, *Eliminating State Law Obstruction of National Artificial Intelligence Policy*, (Dec. 11, 2025), https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

[7] *See, e.g.*, National Whistleblower Center (Sept. 19, 2025), https://www.whistleblowers.org/campaigns/the-urgent-case-for-the-ai-whistleblower-protections-congress-must-pass-the-ai-whistleblower-protection-act/.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



ISABELLA F. SPARHAWK
ASSOCIATE

CHARLESTON
+1.843.579.3456
ISABELLA.SPARHAWK@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.