Strengthening Healthcare Cybersecurity Against Evolving Federal Scrutiny

The 2025–2026 cybersecurity landscape shows heightened scrutiny of healthcare resilience amid shifting federal capabilities. With the Department of Justice increasingly treating privacy failures as **high-stakes government investigations**, organizations must assume greater responsibility for detection and response.

WHEN TO TAKE ACTION

Do not wait for a data breach to evaluate your vulnerabilities. Take action if:

- **You rely on third-party IT vendors:** Supply-chain exposure is a primary driver of modern healthcare breaches.
- **You discover regulatory compliance gaps:** Rapid policy shifts can leave organizations unsure which controls are mandatory, increasing the risk of **regulatory enforcement**.
- **Your incident response plan is untested:** Relying on external parties without internal capacity magnifies the chance of clinical disruption.

HOW TO TAKE ACTION

- **Harden Foundational Technical Controls:** Prioritize multifactor authentication, encryption, and secure backups to reduce your attack surface.
- **Strengthen Third-Party Governance:** Implement continuous vendor monitoring and contractual security obligations.
- **Formalize Resilience Planning:** Maintain documented risk assessments and incident response playbooks tied to clinical continuity.
- **Engage White Collar Counsel:** Involve our **federal criminal defense** team early to ensure that your cybersecurity investments are documented as a proactive defense against potential **government investigations**.

Contact Dykema's White Collar Defense and Government Investigations practice today for a confidential consultation.

Mark Chutkow
Member, Bloomfield Hills
248-203-0715
mchutkow@dykema.com

Jennifer Beidel
Member, Bloomfield Hills
248-203-0506
jbeidel@dykema.com

Leigha Simonton
Member, Dallas
214-462-6444
lsimonton@dykema.com