PROPOSED HIPAA SECURITY RULE COMPLIANCE CHECKLIST

These updates may not be mandated (yet) but preparing now puts your organization ahead. Use this checklist to strengthen your security program and stay ready for potential HIPAA changes.

1. Strengthen Contingency Planning & Incident Response

COMPLETE

- [ ] Develop written procedures for restoring critical electronic information systems and data within 72 hours.
- [ ] Identify and prioritize critical systems that impact patient care and operations.
- [ ] Create a comprehensive Incident Response Plan (IRP) that outlines:
  - [ ] Reporting procedures for suspected or confirmed incidents.
  - [ ] Defined roles and responsibilities for key personnel.
- [ ] Conduct a regular Tabletop Exercise (TTX) to test your incident response plan's effectiveness.

2. Eliminate 'Addressable' vs. 'Required' Specifications

COMPLETE

- [ ] Review all current security measures.
- [ ] Ensure all specifications are uniformly applied without exception.

3. Implement Comprehensive Documentation

COMPLETE

- [ ] Maintain written documentation for:
  - [ ] Security policies and procedures.
  - [ ] Incident response plans.
  - [ ] System recovery plans.
  - [ ] Risk analyses and mitigation strategies.
- [ ] Regularly review and update these documents to reflect changes in your environment.

4. Update Definitions and Security Specifications

COMPLETE

- [ ] Review all current security measures.
- [ ] Ensure all specifications are uniformly applied without exception.

PROPOSED HIPAA SECURITY RULE COMPLIANCE CHECKLIST

5. Develop and Maintain an Asset Inventory

COMPLETE

- [ ] Create a comprehensive inventory of all technology assets that handle electronic Protected Health Information (ePHI).
- [ ] Establish a network map that shows ePHI data flow across systems.
- [ ] Update asset inventories and network maps annually or after any major system change.

6. Enhance Risk Analysis Practices

COMPLETE

Perform comprehensive risk analyses that include:

- [ ] Identifying vulnerabilities.
- [ ] Evaluating risks to ePHI.
- [ ] Developing strategies for risk mitigation.

7. Implement Tabletop Exercises (TTXs) for Real-World Preparedness

COMPLETE

Schedule routine TTXs to:

- [ ] Test your incident response plan.
- [ ] Identify weaknesses in restoration, recovery, and escalation procedures.
- [ ] Enhance coordination between IT, compliance, and leadership teams.

- [ ] Document outcomes from TTXs and use them to refine your response plans.

8. Educate and Train Staff

COMPLETE

- [ ] Train employees on updated security protocols, incident response steps, and reporting procedures.
- [ ] Regularly reinforce cybersecurity awareness throughout the organization.

9. FINAL STEP: Ongoing Review & Improvement

COMPLETE

- [ ] Conduct periodic reviews to ensure all security measures align with evolving regulatory changes and industry best practices.

NEXT STEPS

Need Help Preparing for HIPAA Changes? Contact Echelon Risk + Cyber to schedule a readiness assessment or a tailored tabletop exercise for your healthcare organization.