

Cybersecurity Best Practices

September 2026

Table of Contents

Fiduciary Duties Regarding Cybersecurity	2
1. Have a Formal, Well Documented Cybersecurity Program	2
2. Prudent Annual Risk Assessments	3
3. Annual Third-Party Audits of Security Controls	3
4. Clearly Defined and Assigned Roles and Responsibilities	4
5. Strong Access Control Procedures	4
6. Cloud and Third-Party Asset and Data Security Assurance	4
7. Cybersecurity Awareness Training	4
8. Secure System Development Life Cycle Program (SDLC)	4
9. A Business Resiliency Program	5
10. Encryption of Sensitive Data Stored and in Transit	5
11. Strong Technical Controls	6
12. Responsiveness to Cybersecurity Incidents or Breaches	6
AI Applications in Health & Welfare Plans	7
Key Benefits	7
Key Risks	8
Fiduciary Best Practices	8
Broker and Employer AI Governance Considerations	9
Sample Vendor Questions	10
Bottom Line	10

This overview is intended for employers, plan sponsors, fiduciaries, brokers, and other benefits professionals responsible for selecting and monitoring service providers that handle plan data, participant information, or plan assets. Cybersecurity and AI-related risks can directly affect plan administration, participant outcomes, and fiduciary exposure, making prudent oversight an important part of plan governance.

Apex Benefits is not a law firm and cannot dispense legal advice. Anything contained in this communication is not and should not be construed as legal advice. If you need legal advice, please contact your legal counsel.

Fiduciary Duties Regarding Cybersecurity

Employee benefit plans often hold significant assets and sensitive participant information, which makes them attractive targets for cybercriminals. For that reason, plan fiduciaries should treat cybersecurity as an ongoing oversight responsibility, especially where service providers handle plan data, participant information, or plan assets.

Employer-sponsored group health plans subject to ERISA are generally also covered entities under HIPAA and therefore must comply with HIPAA's privacy and security requirements. While this guide focuses on fiduciary responsibilities related to cybersecurity, plan sponsors should recognize that many of the same cybersecurity practices also support compliance with HIPAA.

In 2024, the Department of Labor's Employee Benefits Security Administration (EBSA) updated its cybersecurity guidance and confirmed that it applies to all ERISA plans, including health benefit plans. The guidance gives fiduciaries a practical framework for evaluating whether service providers have cybersecurity programs, controls, and oversight processes strong enough to support prudent plan administration and fiduciary oversight. The framework is presented as the twelve practices listed and summarized below and can be found in its entirety here - [Compliance Assistance Release No. 2024-01](#)

1. Have a Formal, Well Documented Cybersecurity Program

Fiduciaries should confirm that each service provider maintains a documented cybersecurity program that addresses the confidentiality, integrity, and availability of plan data and related systems. At a minimum, the program should show how the provider identifies risks, protects systems and data, detects and responds to incidents, recovers operations, and communicates appropriately when issues arise.

Protecting Systems from Unauthorized Access, Use, or Other Malicious Acts

The cybersecurity program should enable the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect** each of the necessary assets, data and systems.
- **Detect** and **respond** to cybersecurity events.
- **Recover** from the event.
- **Disclose** the event as appropriate.
- **Restore** normal operations and services.

What to Look for in a Documented Cybersecurity Program

Rather than reviewing a long list of stand-alone policies in isolation, fiduciaries should look for a coordinated program that is approved by leadership, reviewed at least annually, explained to relevant personnel, aligned to a recognized framework, and validated through independent review where appropriate.

An effective way to evaluate the program is to confirm that it covers these core control areas:

- Governance and risk management, including leadership approval, annual review, risk assessment, and alignment to a recognized framework.
- Data protection and access controls, including data classification, privacy, disposal, identity management, privileged access, and multi-factor authentication.
- System security and maintenance, including vulnerability management, configuration management, patching, system hardening, and asset management.
- Operational resilience, including business continuity, disaster recovery, incident response, backup, and restoration processes.
- Vendor and development oversight, including third-party risk management, secure development practices, and controls over internally and externally developed applications.
- Workforce readiness and accountability, including training, assigned responsibilities, and independent testing or audit support.

The sections that follow expand on several of these areas and highlight the questions fiduciaries should ask when evaluating service providers.

2. Prudent Annual Risk Assessments

A risk assessment helps identify, prioritize, and document cybersecurity risks affecting systems and data. Part of the process should also involve how identified risks will be mitigated or accepted and what controls will be in place to manage changes in technology and business practices. For employers and fiduciaries, the key question is not whether a vendor says it performs risk assessments, but whether those assessments are current, documented, and tied to meaningful remediation and monitoring.

3. Annual Third-Party Audits of Security Controls

Independent review of security controls gives fiduciaries a more objective basis for vendor oversight. In practice, this may include System and Organization Controls (SOC) reports, penetration test summaries, independent assessments against recognized frameworks, and documentation showing that identified issues were tracked and remediated.

4. Clearly Defined and Assigned Roles and Responsibilities

A cybersecurity program is more credible when accountability is clearly assigned and supported by qualified personnel who engage in ongoing cybersecurity training. Fiduciaries should be able to identify who owns information security, who reports on it, and who is responsible for decision-making during a security incident or operational disruption.

5. Strong Access Control Procedures

Access controls should ensure that only the right people have the right level of access to plan-related systems and data. Fiduciaries should look for clear processes around identity verification, role-based access, password standards, multi-factor authentication, ongoing monitoring, and safeguards for distributions or other sensitive transactions.

6. Cloud and Third-Party Asset and Data Security Assurance

Cloud hosting and outsourced services do not eliminate fiduciary oversight responsibilities. If plan data is stored in the cloud or managed by a third party, fiduciaries should understand where the data resides, who can access it, what controls apply, and what contractual protections and independent reviews support the arrangement.

7. Cybersecurity Awareness Training

Training remains important because employees are often the first line of defense and, in some cases, the weakest link in maintaining cybersecurity. Training should be conducted at least annually and should reflect current cybersecurity risks by addressing threats such as phishing, impersonation of plan officials or participants, account takeover risks, and other tactics that could lead to fraudulent distributions or unauthorized access.

8. Secure System Development Life Cycle Program (SDLC)

An SDLC is a method used by organizations to design, build, test, and maintain high-quality and secure information systems. Even if an employer is not building software itself internally, this area still matters because many service providers rely on participant portals, mobile apps, integrations, automated workflows, and custom administrative tools. Fiduciaries should look for evidence that security testing, code review, vulnerability management, and penetration testing are built into how those systems are developed and maintained.

9. A Business Resiliency Program

Business resiliency is the ability to continue serving the plan through operational disruptions, cyber incidents, and other unexpected events. Fiduciaries should confirm that service providers maintain tested plans for business continuity, disaster recovery, and incident response, and that those plans include clear communication and escalation protocols.

The **Business Continuity Plan** is the written set of procedures an organization follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption.

The **Disaster Recovery Plan** is the documented process to recover and resume an organization's IT infrastructure, business applications, and data services in the event of a major disruption.

The **Incident Response Plan** is a set of instructions to help IT staff detect, respond to, and recover from security incidents.

An effective business resiliency program should:
• Reasonably define the internal processes for responding to a cybersecurity event or disaster.
• Reasonably define plan goals.
• Define the documentation and reporting requirements regarding cybersecurity events and responses.
• Clearly define and describe the roles, responsibilities, and authority levels.
• Describe external and internal communications and information sharing, including protocols to notify plan sponsor and affected user(s) if needed.
• Identify remediation plans for any identified weaknesses in information systems.
• Include after action reports that discuss how plans will be evaluated and updated following a cybersecurity event or disaster.
• Be annually tested based on possible risk scenarios.

10. Encryption of Sensitive Data Stored and in Transit

Encryption is a foundational safeguard for nonpublic information. Fiduciaries should confirm that service providers use current encryption standards for sensitive data both at rest and in transit, manage encryption keys appropriately, and apply related controls such as message authentication and hashing to help protect confidentiality and data integrity.

11. Strong Technical Controls

Fiduciaries do not need to validate every technical tool used by a service provider, but they should expect evidence that core technical controls are current, maintained, and periodically reviewed. This includes keeping hardware, software, and firmware up to date; implementing vendor-supported firewalls, intrusion detection and prevention tools, and regularly updated antivirus software; performing routine patch management; applying system hardening and network segmentation practices; and conducting routine data backups. Together, these controls help reduce the likelihood that known vulnerabilities, outdated systems, or weak network protections will expose plan data or operations.

12. Responsiveness to Cybersecurity Incidents or Breaches

When a cybersecurity incident occurs, service providers should respond promptly and in a way that protects both the plan and its participants. Fiduciaries should understand expected notification timelines, coordination responsibilities, participant communication obligations, and the provider's process for investigating the incident, addressing the root cause, and reducing the risk of recurrence.

Cybersecurity in Service Provider Selection

Use this checklist when evaluating or renewing a service provider that handles plan data, participant information, or plan assets. Ask for clear documentation, confirm the provider's controls, and make sure your contract includes strong cybersecurity protections.

Service Provider Cybersecurity Checklist	
☐	Request the provider's cybersecurity policies, standards, and most recent independent audit reports and confirm the provider follows a recognized security framework and uses an independent third party to validate controls.
☐	Confirm how the provider tests its controls and whether you may review audit results under the contract.
☐	Review the provider's security track record, including past incidents, claims, or litigation.
☐	Ask whether the provider has had a breach and how it responded and remediated the issue.
☐	Verify the provider carries cyber and related insurance that would respond to plan-related losses.
☐	Include contract terms that require ongoing cybersecurity compliance and clear accountability for security failures, including: • Annual independent security reporting. • Confidentiality and limits on data use and sharing.

	• Prompt breach notification and cooperation in investigation and response. • Compliance with privacy, security, retention, and destruction requirements. • Appropriate insurance coverage for cyber, privacy, and related losses.
☐	Identify who on your team will review the materials, document the decision, and monitor the provider over time.

AI Applications in Health & Welfare Plans

Artificial intelligence (AI) is becoming increasingly common in health and welfare plan administration, often embedded within systems that employers and participants already use every day. Health plans, third-party administrators, pharmacy benefit managers, and navigation vendors are using AI to support claims administration, customer service, enrollment assistance, fraud detection, utilization review, care management, and population health analytics. Brokers and consultants are also leveraging AI tools for benchmarking, renewal analysis, stop-loss forecasting, plan design modeling, and participant communication support.

On the participant side, employees may encounter AI through chatbots, provider search tools, symptom checkers, wellness applications, mental health support tools, or personalized benefits recommendations. In many cases, participants may not even realize AI is involved because the technology operates behind the scenes within existing vendor platforms.

As adoption expands, employers and fiduciaries should understand not only where AI is being used, but also how it may influence plan administration, access to care, claims outcomes, and participant experience.

Key Benefits

AI can create significant operational and participant value when implemented thoughtfully and governed appropriately. For employers and plan administrators, AI can help reduce administrative burden, streamline repetitive processes, improve fraud and waste detection, and provide faster access to data-driven insights. Many organizations are using AI to analyze claims trends, identify high-cost drivers, support population health initiatives, and improve forecasting during renewal planning.

For participants, AI can improve the overall benefits experience by making information easier to access and easier to understand. Tools such as virtual assistants and care navigation platforms can help employees locate providers, compare costs, understand plan options, and receive support more quickly than traditional service channels. AI may also help identify gaps in care earlier, enabling proactive outreach for chronic conditions, preventive care, or behavioral health support.

When properly supervised, AI can enhance efficiency and improve service quality without replacing the human judgment necessary for important benefit and healthcare decisions.

Key Risks

Despite its potential advantages, AI introduces substantial legal, operational, and fiduciary risks that employers and plan fiduciaries should carefully evaluate. One of the most significant concerns involves fiduciary responsibility under ERISA. Employers and fiduciaries cannot simply rely on vendor assurances that AI systems are accurate or compliant. If an AI-supported process influences claims administration, access to care, or plan operations, fiduciaries may still be responsible for prudently selecting and monitoring the vendor and its processes. The Department of Labor has consistently emphasized that fiduciary obligations focus heavily on prudent oversight and decision-making processes.

Another major concern involves discrimination and bias. AI systems trained on incomplete or biased data may unintentionally produce discriminatory outcomes or disproportionately affect certain populations. This risk is especially important in healthcare-related decision-making, including prior authorization, care management, and clinical recommendations. Federal regulators have increasingly focused on nondiscrimination obligations tied to automated decision-making and clinical support tools.

Privacy and cybersecurity risks are also significant. Many AI systems rely on large volumes of sensitive health information, creating concerns around HIPAA compliance, data sharing, cybersecurity vulnerabilities, and third-party access to protected health information (PHI). Employers should understand how vendors store, process, and potentially use participant data, particularly if information may be used to train or improve AI models. The Department of Health and Human Service's Office for Civil Rights continues to emphasize that covered entities and business associates remain responsible for safeguarding PHI regardless of the technologies involved.

In addition, employers should be cautious about "black box" decision-making. If vendors cannot clearly explain how AI-supported decisions are made, it may become difficult to evaluate fairness, consistency, appeals handling, or compliance with plan terms. This concern is particularly relevant when AI tools influence adverse benefit determinations or utilization management outcomes.

Fiduciary Best Practices

Employers and fiduciaries should approach AI governance as an extension of existing vendor oversight, cybersecurity governance, and fiduciary monitoring responsibilities. A prudent first step is developing an inventory of vendors and identifying where AI or automated decision-making tools are being used within health and welfare plan operations. Many employers are surprised to learn how broadly AI capabilities have already been integrated into carrier, third-party administrator, pharmacy benefit manager, navigation, and wellness platforms.

Once AI use cases are identified, employers should evaluate the relative risk associated with each application. Low-risk uses may include administrative automation or internal analytics, while higher-risk uses may involve claims decisions, prior authorization, eligibility determinations, or clinical recommendations. Higher-risk applications generally require more robust oversight, documentation, and monitoring.

Vendor transparency is critical. Employers and brokers should ask vendors detailed questions regarding how AI is used, what data supports the models, whether human review is involved, how bias

testing is conducted, and what safeguards exist for privacy and cybersecurity. Employers should also review whether participant or plan data may be used for model training purposes and whether subcontractors are involved in delivering AI-enabled services.

Human oversight remains essential, particularly when decisions may affect access to benefits or healthcare services. Employers should ensure that AI tools supplement — rather than replace — qualified human judgment for clinically significant or adverse determinations. Vendors should be able to explain how decisions are made and demonstrate that processes align with plan documents and applicable laws.

As a standing element of its vendor oversight function, fiduciaries, ideally by way of a fiduciary committee, should establish a charter to specifically govern the plan sponsor's obligations arising from plan vendors' use of artificial intelligence and automated decision systems in:

- Claims adjudication and payment accuracy;
- Prior authorization and utilization management (UM) determinations;
- Member-facing communications, virtual assistants, and grievance processing;
- Pharmacy benefit management, formulary placement, and step-therapy protocols;
- Stop-loss underwriting and risk assessment; and
- Network adequacy modeling and provider tiering.

Monitoring should also continue after implementation. Fiduciaries should periodically review claims trends, denial rates, appeal outcomes, participant complaints, prior authorization metrics, and cybersecurity reports to identify potential issues. Consistent documentation of oversight activities, vendor reviews, committee discussions, and corrective actions can help demonstrate a prudent fiduciary process if questions arise later.

Broker and Employer AI Governance Considerations

As AI adoption accelerates, brokers and employers may benefit from developing a more formal governance framework around AI use within health and welfare plans. Governance efforts do not necessarily require highly technical expertise, but they should establish clear expectations around accountability, oversight, risk management, and vendor transparency.

Many organizations are beginning to incorporate AI-related questions into RFPs, renewal discussions, and vendor due diligence processes. Employers may also consider updating service agreements, business associate agreements, cybersecurity provisions, and audit rights to specifically address AI-related risks and data use practices. Internal benefits or fiduciary committees should periodically review how AI is being used across the plan ecosystem and assess whether any new risks have emerged.

Training and education are also becoming increasingly important. HR, benefits, compliance, legal, and procurement teams should understand the basics of AI governance and know when additional review may be necessary. While AI can provide efficiencies and improve participant engagement, organizations should remain cautious about overreliance on automation without appropriate controls and human oversight.

Sample Vendor Questions

Employers and brokers should ask vendors direct and practical questions about their use of AI and automated decision-making tools. For example, organizations may want to ask whether AI is used in claims administration, prior authorization, care management, fraud detection, eligibility decisions, or participant communications. It is also important to understand whether AI recommendations are reviewed by qualified personnel before final decisions are made.

Questions around transparency and explainability can help employers assess whether vendors can adequately support appeals, audits, or participant inquiries. Employers may also want to ask how vendors evaluate models for bias or disparate impact, how participant data is protected, whether plan data is used to train models, and what subcontractors or third parties may have access to sensitive information.

Cybersecurity and incident response questions are equally important. Employers should understand how AI systems are secured, what safeguards apply to PHI, how vendors monitor for unauthorized access, and what notification obligations apply if a security incident occurs.

Bottom Line

AI has the potential to improve efficiency, participant engagement, and data-driven decision-making within health and welfare plans. At the same time, it introduces meaningful fiduciary, compliance, privacy, and operational risks that employers should not overlook. The most effective approach is one grounded in prudent oversight: understanding where AI is being used, evaluating associated risks, requiring transparency from vendors, preserving meaningful human review, protecting participant data, and documenting governance efforts along the way.

Organizations that approach AI thoughtfully and proactively will likely be in a stronger position to capture its benefits while minimizing legal and fiduciary exposure.