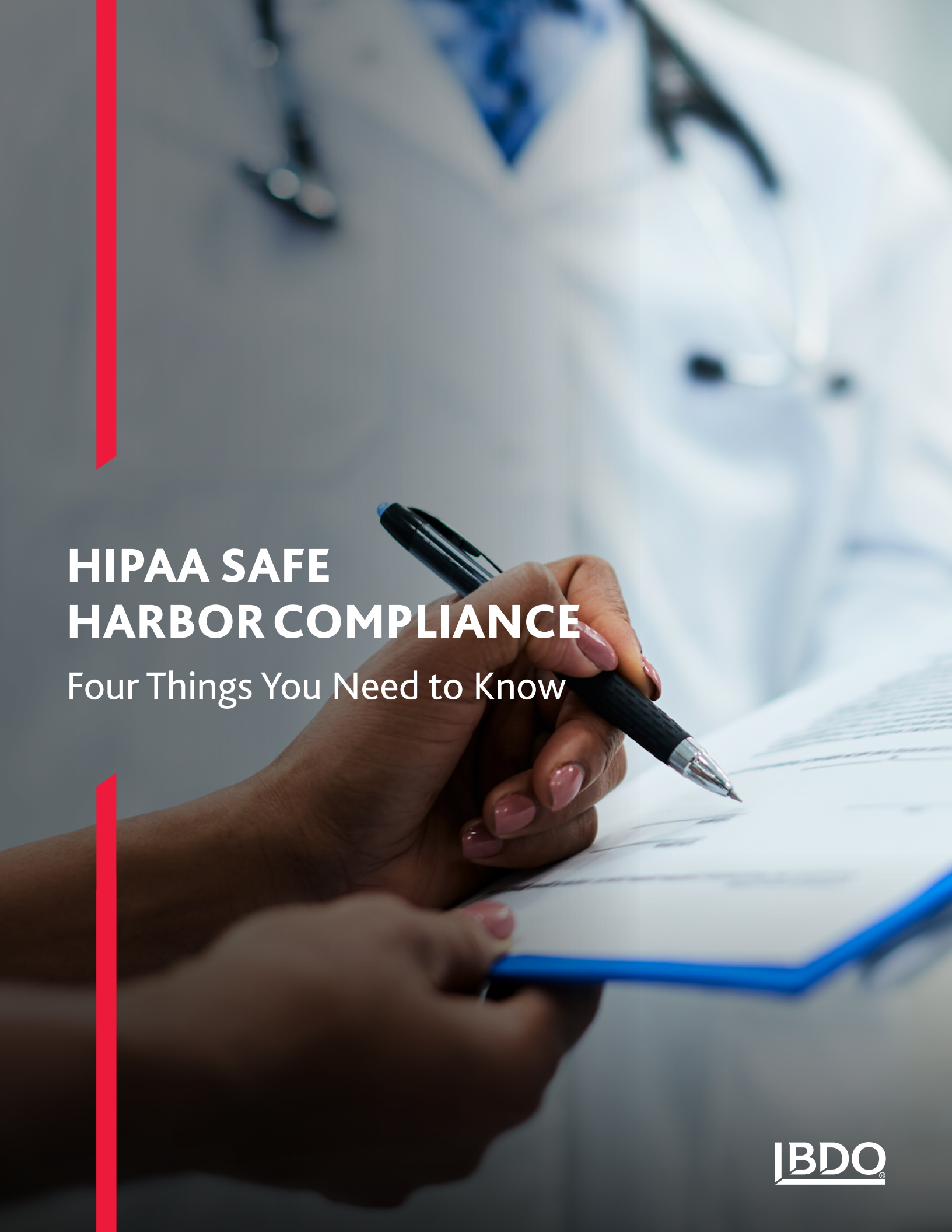


HIPAA SAFE HARBOR COMPLIANCE

Four Things You Need to Know

BDO

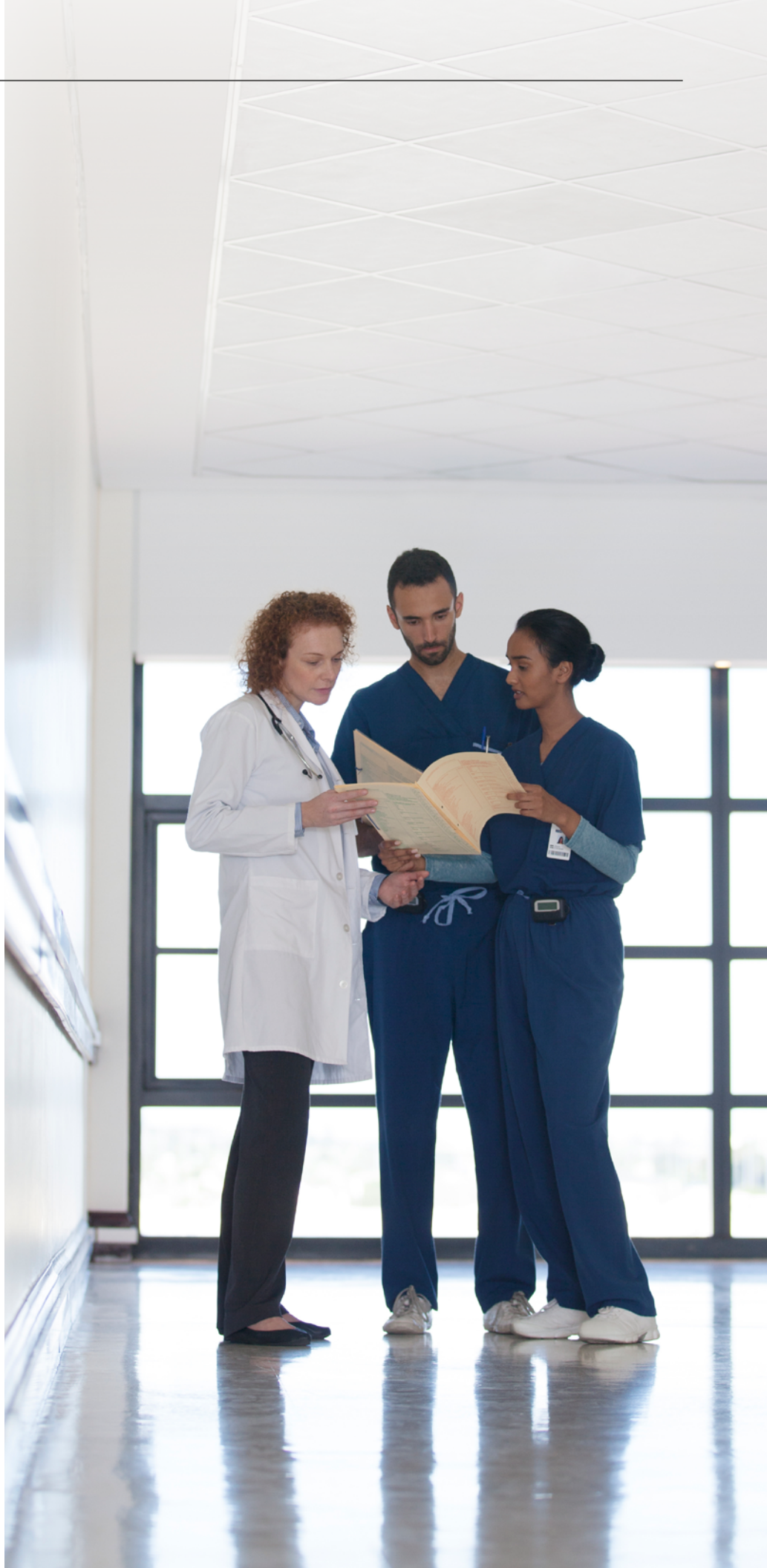
#1: The Landscape Has Shifted

The 2021 Safe Harbor Law changed the way organizations coordinate HIPAA regulations and internal data protection protocols. Under the Safe Harbor Law, to reduce exposure and address ongoing data protection obligations, risk assessments and compliance checklists must be done annually.

Failing to comply with Safe Harbor laws increases risk for:

- Monetary penalties
- Office for Civil Rights (OCR) audits
- Increased obligations under correction agreements

Now, more than ever, adopting recognized data protection practices and risk reduction frameworks can bridge the difference between optimized compliance and costly violations.



#2: HIPAA Non-Compliance Is Still Costly

Factors used to assess penalties include organizational risk awareness, internal procedures addressing risk, and corrective post-violation actions.

Recently, the Department of Health and Human Services (HHS) issued a $1.5 million penalty against a Massachusetts provider for several violations, including failing to safeguard protected health information (PHI).

Tier 1 - Unaware of Violation
$100 - $50,000 per violation

Tier 2 - Lack of Due Dilligence
$1,000 - $50,000 per violation

Tier 3 - Willful Neglect Without Correction
$10,000 - $50,000 per violation

Tier 4 - Willful Neglect Without Correction
$50,000 per violation

Tier 1 penalties range from $100 to $50,000 per violation, with a $1.5 million annual cap. Tier 4 penalties—involving willful neglect of protected health information—start at $50,000 per violation, also with a $1.5 million annual cap.*

#3: Risk Assessment Methodologies Must Be Solid

BDO professionals follow a carefully developed methodology when helping clients address HIPAA Safe harbor regulations:

Step 1
Gather information about standards, safeguards, and organizational requirements

Step 2
Assess privacy and cybersecurity practices aligned with risk and remediation goals

Step 3
Record observations, risks, and recommendations

Step 4
Design and implement controls to achieve HIPAA compliance

Step 5
Compile risk assessment report and remediation action plan

Throughout the process, our goal is to deliver concrete, actionable recommendations to drive ongoing HIPAA compliance.

WHY BDO?

We help companies protect their data with a balanced approach that drives security and compliance without stifling innovation.

Our team has certifications in privacy, information management, records management, IT, security, digital forensics, e-discovery, and project management. Members of our team have worked in the healthcare industry and understand the operational aspects of managing a privacy and cybersecurity program, as well as the regulatory obligations each organization may have for compliance with laws such as HIPAA.

#4: We're Dedicated to Keeping Clients on Track

BDO Forensics offers a wide range of services to help clients assess, develop, and optimize HIPAA Safe Harbor compliance programs.

1. Risk Assessment
Reviewing current standards, practices, and safeguards

2. Target Roadmap
Developing remediation plans

3. Roadmap Execution
Aligning business units with necessary controls and changes

4. HITRUST
Facilitating HITRUST pre-assessments and validated assessments

5. Governance and Monitoring
Establishing frameworks and monitoring requirements

Case Studies

CASE STUDY 1

The Problem
A prominent, global pharmaceutical company needed support to build out its digital health platform which was designed to send patient data to providers to support remote patient monitor through a data subscription model.

The Approach
BDO was engaged to help design and implement HIPAA Privacy and Security operational processes to address key regulatory requirements and contractual obligations. The company was able to identify when it held higher obligations as a Business Associate and where it could reduce risk related to regulatory requirements.

The Result
The company was able to mature its HIPAA compliance program to support a new service model and revenue stream, thereby empowering the business to use data in a strategic and revenue-producing way.

CASE STUDY 2

The Problem
A global medical device company acquired a new healthcare technology company and wanted to understand the security controls in place for a commercial product. A HIPAA Security Risk Analysis, data inventory, and data flow map did not exist to identify compliance with HIPAA or the GDPR.

The Approach
BDO performed a HIPAA Risk Analysis and documented the data collected, transmitted, and stored at the client site servers, in the cloud, and within the company's assets. BDO worked with product teams, engineers, and security professionals to identify how data was protected and opportunities to consider security and privacy during the software development life cycle.

The Result
The company identified risks to data and was able to implement tools to provide greater protections to data in transit. Identifying risks and documenting data flows better prepared the organization to remediate security gaps and positioned the organization to move into new markets.

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!