Progress®

HIPAA Security Compliance Matters in Healthcare IT

Congress created the Health Insurance Portability and Accountability Act (HIPAA) in 1996, mandating establishment of federal standards to protect the integrity, confidentiality and availability of individually identifiable health information. As a result, a valuable commodity—personal health information, or PHI—today remains largely shielded from lawful commercial exploitation.

In the years since HIPAA's enactment and as more PHI has moved online—and then into the cloud—the safety of patients' information has become an urgent concern. By 2017, 86 percent of office-based physicians had digitized their patient health records. To provide standards for their confidentiality, integrity and security, the U.S. Department of Health and Human Services (HHS) issued the HIPAA Security Rule. Compliance with this rule is widely regarded as a best practice for protecting PHI.

Yet claiming compliance is one thing—showing it is something else. No health cloud solution should be considered before a qualified independent auditor attests to the condition of the vendor's HIPAA security controls and procedures. Assessing HIPAA compliance depends on several key components, which we'll get into later. First, it's worth reviewing why security is of particular importance when it comes to health records that are stored electronically.

Data Breaches in Healthcare

HHS requires hospitals and other healthcare providers to report data breaches that expose private medical or financial information. Providers also must notify everyone involved. If the breach affects 500 or more people, HHS will make the data breach report public.

Currently, more than 500 HIPAA breaches are under investigation by the HHS Office for Civil Rights (OCR). However, this number may not reflect the true scale of the problem. In the healthcare sector, cybersecurity risk is "underreported by orders of magnitude," HHS deputy chief information security officer Leo Scanlon said during a June 2017 U.S. House subcommittee hearing.

Neither is the pace of incidents slowing down. Healthcare data breaches rose 70 percent between 2010 and 2017, and these are just the larger breaches that OCR publishes. All told, they amount to 176.4 million health records.

Consequences of a Data Breach

Once lost or stolen, an individual's medical records can end up on the dark web where they sell for as much as $1,000. The records are valuable to cybercriminals because they can contain the patient's medical history but also Medicare or insurance policy numbers, payment account numbers and Social Security number, along with other identifying information. Armed with this data, criminals can fill prescriptions, run up credit card and medical debt, and empty bank accounts—all in the victim's name.

The harm to patients can be immeasurable. Victims have faced repercussions ranging from job loss to drug trafficking charges. Sensitive PHI can expose them to fraud and blackmail. In addition, if friends or family are part of the health record—perhaps as a responsible party or next of kin—they could become victims as well.

Cybercrime also takes its toll on healthcare organizations. A 2018 study by Ponemon Institute reveals that the cost of a data breach is $408 for each lost or stolen record. That's roughly twice what it costs in financial services, the next-most expensive industry for data breaches.

Then there's the legal and regulatory fallout. Under the Health Information Technology for Economic and Clinical Health Act—better known as the HITECH Act—healthcare organizations and independent software vendors (ISVs) can face penalties for failing to protect individuals' electronic PHI. Federal fines can be costly, reaching $50,000 per violation per record to a maximum of $1.5 million per year. On top of that, OCR has been known to file criminal charges for HIPAA violations.

Components of an Attestation Report

So how can ISVs verify the HIPAA and HITECH compliance of a health cloud solution? The most effective approach is to have the platform solution vendor produce an attestation report from a qualified independent auditor. The report will explain how the vendor's security, privacy and breach notification practices meet OCR requirements for covered entities and business associates.

An attestation report ordinarily includes four key sections:

There are three parts to this section. In the first, management tells readers about the information security program supporting the vendor's health cloud solution. This should include a description of the vendor's services, electronic PHI data flows, third-party services (as applicable) and breach notification tools and processes. In addition, look for program details such as:

- Human resource and security awareness training
- Access authentication and authorization
- Access requests and access revocation
- Data backup and disaster recovery
- Incident response
- System monitoring

Part two of this section describes the vendor's risk assessment program. The description should include the program's scope and current security measures along with the following processes:

- Threat and vulnerability identification
- Likelihood and impact analysis
- Risk level determination and documentation
- Risk management program monitoring and maintenance

Finally, this section should list the security rules and activities that apply to the performance of the vendor's information security program. Keep in mind that although OCR's audit protocol for HIPAA compliance is extensive, not every section or activity is necessarily relevant to a third-party software system. For instance, the Progress health cloud platform achieves HIPAA compliance by meeting six sections of security rules and five sections of breach notification rules, as Table 1 shows (HIPAA Compliance Criteria for the Progress Health Cloud Platform).

Management assertion. In this section, vendor management confirms that the program description fairly presents what they provide as part of their health cloud solution and that the program itself conforms to the applicable implementation

specifications within the HIPAA Security Rule and HITECH Breach Notification Requirements. This section also should list the criteria management used in making these assertions.

Audit results. This part of the report gets down to brass tacks. The auditor lays out the established performance criteria and audit inquiry for the rules and activities that apply. Then, next to each activity, the auditor reveals the results of its controls test. "No exceptions noted" means the auditor did, in fact, find the appropriate control to be in place. Ideally, every control should have no exceptions noted.

Auditor opinion. Here's where the audit firm states whether they believe management has fairly described the information security program in place, and whether the program conforms to the applicable implementation specifications within the HIPAA Security Rule and HITECH Breach Notification Requirements. For context, the auditor may state the scope of their examination along with their own and the vendor's responsibilities in the examination. They also might offer a reminder of the inherent limitations of controls and any restrictions on the use of the attestation report.

Table 1. HIPAA Compliance Criteria for the Progress Health Cloud Platform

Objective	Section	Key Activities
Security	164.306	General requirements Flexibility of approach Security management process
	164.308	Security management process (risk analysis and management, sanction policy, information system activity review) Assigned security responsibility Workforce security Information access management Security awareness, training and tools Security incident procedures Contingency plan Applications and data criticality analysis Business associate contracts and other arrangements
	164.310	Facility access controls Workstation use and security Device and medial controls
	164.312	System access control Audit controls Integrity Person or entity authentication Transmission security
	164.314	Business associate contracts
	164.316	Policies and procedures Documentation
	164.530	Training
Breach Notification	164.402	Definitions (breach risk assessment, breach exceptions, unsecured PHI)
	164.410	Notification by a business associate
	164.412	Law enforcement delay
	164.414	Burden of proof

The Value of HIPAA Compliance

With data breaches on the rise—and the consequences of a breach potentially severe—HIPAA security compliance has become essential to the safety of electronic PHI. Any health cloud solution vendor can claim compliance, but ISVs should limit their consideration to those who can produce an informed opinion from a qualified auditor. The attestation should rely on the same criteria that OCR uses for their audits, as applicable to the individual solution. And the results should boost confidence that the solution can deliver on its promises to healthcare organizations while doing its own part to protect the records of vulnerable patients.

To obtain a copy of the attestation report on the Progress Health Cloud information security program under HIPAA and HITECH, please contact healthcloud@progress.com.

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, award-winning machine learning that enables cognitive capabilities to be a part of any application, the flexibility of a serverless cloud to deploy modern apps, business rules, web content management, plus leading data connectivity technology. Over 1,700 independent software vendors, 100,000 enterprise customers, and two million developers rely on Progress to power their applications. Learn about Progress at www.progress.com or +1-800-477-6473.

Rev 2019/08 | RITM0053396

Progress®