$1.5 million for HIPAA Training? You're Kidding.

Would you pay $1.5 million for a one-day HIPAA training? Of course not. That's a ridiculous amount of money. What about $31,000? Still too high? Unfortunately, if a one-day HIPAA seminar and a generic HIPAA manual comprise the entirety of your HIPAA compliance program, you might end up paying just that.

Consider this: There are over 60 administrative, technical and physical safeguards in the HIPAA Rule that need to be met and annual training only satisfies a small fraction of those requirements. **All it takes is one patient complaint or one stolen laptop containing protected health information to expose the holes in your HIPAA compliance program – and potentially millions of dollars in penalties.**

Civil Money Penalties for HIPAA Violations (enforced by the Office of Civil Rights)

Intent	Minimum Per Incident	Annual Cap
Did Not Know or Could Not Have Known	$100 - $50,000	$1.5 million
Reasonable Cause and Not Willful Neglect	$1,000 - $50,000	$1.5 million
Willful Neglect, but Corrected within 30 Days	$10,000 - $50,000	$1.5 million
Willful Neglect and Not Corrected Within 30 Days	$50,000	$1.5 million

Actual Fines

We've all heard of the million-dollar HIPAA fines being paid by big corporations. But the risk of HIPAA fines is just as great for the average covered entity. Here are just a few examples:

Failure to obtain authorization for a patient testimonial – $25,000

A physical therapy office was fined $25,000 for positing patient testimonials, including full names and photographic images of the patients, without obtaining HIPAA-compliant authorizations.

Adopting sample policies and procedures – $150,000

A non-profit was fined $150,000 in part because they were using sample HIPAA security policies but were not following any of the procedures outlined in those policies.

No Business Associate's Agreement – $31,000

A non-profit was fined $31,000 for not having a Business Associate Agreement (BAA) with a vendor that had access to the protected health information of their patients.

Stolen Unencrypted iPhone – $650,000

An organization was fined $650,000 for failing to have encryption and password protection on an employee's iPhone, which contained protected health information. The error was discovered after the iPhone was stolen.

HIPAA breaches can happen at any time. But establishing a HIPAA compliance program early can make all the difference. Contact LayerCompliance today and find out how we can help you reduce your risk.

Contact LayerCompliance Today

800.334.6071