PRINCIPAL INVESTIGATORS.ORG

"Helping leading researchers in all fields with their *non-science* duties and responsibilities."

(800) 303-0129
(239) 331-4333
Fax: (239) 676-0146

View

No. 9: Research Compliance: Lost Data

Mon, Dec 28th, 2009 12:00:00 am

Sign Up to receive free weekly articles like these

Research Compliance:

Lost Data

Reader Question: A month ago I was flying to a convention of my research specialty in San Francisco, and in one of my checked bags was my notebook computer and three discs of raw data (non-encrypted) on about 800 patients we have enrolled in a clinical trial. But the airline lost the bag in transit. Of course, I filed a "lost bag" claim with them, but no trace of it yet. Little hope now. I have heard there is some new law called HITECH that applies to lost data. What should I do at this point? Should I already have done anything?

Expert Comments: Brace yourself; we're going to have to deal with some "alphabet soup" of U.S. government acronyms while explaining your situation.

The Health Information Technology for Economic and Clinical Health Act, or HITECH, is the U.S.A. Federal law that requires you take immediate action and notify those affected by a loss of protected health information (PHI).

First, figure out if HITECH applies. In order for it to come into play, HIPAA (Health Insurance Portability of Accountability Act of 1996) has to apply to you. It does if you're working with patients. However, does HIPAA apply to the *particular* data you've lost? If you took all of the identifiers off the data, then you're ok because de-identified data isn't covered by HIPAA or HITECH.

But maybe you aren't so lucky, and the data contained the initials of patients and their diagnoses. Remember, even initials are identifiers under HIPAA. If the bag stays gone, HIPAA's in play, but not necessarily HITECH. Was that data encrypted? If so, HITECH's breach notification rules won't apply because HITECH only applies to "unsecured" PHI.

Let's assume your data wasn't encrypted. For HITECH to apply, the unauthorized disclosure must "compromise the security or privacy of the PHI by posing "a significant risk of financial, reputational or other harm to the individual" whose PHI was lost. If the data consists only of initials and diagnoses, you probably don't have a HITECH breach because there is not enough data to identify specific individuals, and thus the risk of harm would be slight.

If you had social security numbers on that disk, it's another story. These are considered sensitive financial data. Their loss definitely poses a risk of financial harm, so this is where it gets awkward. Once you're in the breach zone, HITECH requires you to send a written notice by mail to the persons whose data was compromised. The notice has to let them know what happened and when; the data that was disclosed; the actions you're taking to prevent harm from the disclosure; and contact procedures for people who have questions. You have to send the notice out "without unreasonable delay" and in no event later than 60 calendar days after you discover, or reasonably should have discovered, the breach.

But it can get worse. If you have ten or more people for whom you don't have an address, then you also will need to post your notice on your home website or in "major print or broadcast media." This notice must include a toll-free number available for people to call over the next ninety days to determine if their information was affected. Finally, if the breach involves more than 500 residents of a state (you did say you had data for 800 subjects, right?), then, you guessed it, the *mandatory* news media notice requirement kicks in! You will need to notify "prominent news media outlets" that serve the area (or areas) in which the individuals live, plus the Federal Secretary of Health and Human Services.

No one wants to go through that hassle and embarrassment. The solution lies in two simple steps: **de-identify and encrypt.**

If you must use identifiers, then use the fewest possible and encrypt! Everything can be encrypted --email, documents, hard disks, and even thumb drives. Encrypted data is not unsecured data, so HITECH won't apply even if it is lost. Finally, remember to always back-up your data – not just so you don't lose valuable research but also so you can figure out exactly what went missing.

*Comments by **Kristen H. West, J.D.,** Associate V.P. and Director, Office of Research Compliance, Emory University Atlanta*

Enjoy this article? Sign Up to receive these free every week

<< Back to list page - Email this Page

Comments

incredulous in idaho
HITECH aside, you may already be in violation of breach notification laws or perhaps other laws that require you to encrypt personal information. Certainly it is not best practice to carry around personal data (unencrypted!) and then put this into checked baggage. What were you thinking?!

Dec 22 2009 9:33AM

RealWorld
Dear "Incredulous": Who are you, the Christmas Grinch?. I agree that, viewed through the retrospectoscope, it is easy to see what to do in an ideal world. But when one is late packing for the meeting, and late leaving for the airport, not everybody can suck his thumb and think "Oh gee, I guess I better miss my plane so I can encrypt those last-minute data". I bet that, realistically, most of us would chance it. Too bad the writer, through a fluke, lost his bet.

Dec 25 2009 1:36PM

Patrick W.
The way some of our clinicl trial sites report, I can barely understand the data before encryption, even though I know what many elements are supposed to be. So I would't worry too much about what some street thief is going to extract from your disc.

Dec 27 2009 8:22AM

---

george
I know hind site is 20/20. Remember the good ole days, when you had to carry your slides with you to lecture, the common rule, was that you never checked your slides to go under the plane. Under no circumstance, should one ever, place there computer or CD's for that matter, under the plane.

Dec 29 2009 9:17AM

Anonymous
No one should EVER let a notebook computer with sensitive data out of his/her sight!

Dec 29 2009 10:08AM

Richard W
Participants in a clinical trial are told that their information is confidential and expect it to be guarded. The investigator has the responsibility to keep that trust - no excuses. Poor planning is no reason for data on 800 people to be lost. As george stated, the common rule is never place anything important under the plane (e.g. slides, posters etc). If one does that with personal property and it is lost, that is too bad. But it is other peoples personal information that is unforgivable.

Dec 29 2009 10:18AM

SY
Under new TSA guidelines, it will probably soon be illegal to carry your laptop OR slides. Or a CD, in case a terrorist wants to fashion it into a throwing star. It's all for our protection, right?

Dec 29 2009 10:20AM

Ouch
TrueCrypt...it's easy...it's secure...it's free

Dec 29 2009 10:24AM

Mike
I think some sound advice has been offered all around. I would just suggest that you also check the applicability of state requirements. As you may know, many states have laws regarding confidentiality, privacy and security safeguards, breach notification, breach remediation and associated penalties. These may apply to all types of information not just the PHI of covered entities under HIPAA.

Dec 29 2009 10:25AM

Tony
Also keep in mind that if the Veterans Administration is involved in anyway, you have an entirely new set of issues and requirement to manage.

Dec 29 2009 10:34AM

Tom in Raleigh
The essential problem is this: why put a laptop and data in checked luggage? The probability of theft is not high, but it's not trivial either. I have _never_ checked a laptop on any flight because I don't trust the airlines and the TSA to secure it from theft or damage. My first thought in reading this was "who would put a computer in checked baggage?" My university's IRB would freak out if I did such a thing, because we usually have to provide some evidence of data security; that security was clearly breached here. Lesson learned, I hope.

Dec 29 2009 11:30AM

Security Nut
With the "shoe bomber" and now the "underpants Christmas bomber", it's only a matter of time till we have some terrorist try to be a "laptop bomber". In the aftermath of that you'll no longer be able to carry into the plane cabin your computer and maybe even discs.Answer: stop CARRYING your data at all , in any way, shape or form. Ship it via Internet. Rent a computer at your destination.

Dec 29 2009 3:33PM

John L
As "Anonymous" pointed out, anything you do not want to lose should never be checked in. Never trust the airline to handle laptops and sensitive documents. Always carry these with you, and such a major breach in information security can easily be avoided.

Dec 30 2009 12:28PM

Victor
Dear "RealWorld": The situation you describe as a realistic scenario is actually an amateurish non-professional behavior and lack of organization. Any person preparing for the travel to the meeting like that should stop wasting time at socializing websites and computer games and maybe drink less, or be prepared to be booted from any serious job.

Jan 4 2010 8:11AM

TOM@NIH
The first person to call in any data loss scenario (right after your boss) is your agency PO. I agree with Victor that RealWorld and his or her ilk are probably in the wrong line of business. JohnL is also right on. There is no excuse for carrying un-encrypted raw data in a laptop - ever - that is why VPN and similar upload services exist.

Jan 4 2010 10:54AM

Alex Pauling
Data are more important than money

Jan 5 2010 8:27AM

---

strawdog
both the researcher and 'realworld' are either simpletons or just too naive to be entrusted with responsibility. In this day and age putting a laptop in checked baggage is an invitation to theft. Doing so with this kind of data is irresponsible. Both these individuals need a good dose of the consequences of being so presumptive. there is always another airplane!

Jan 5 2010 8:31AM

Ocean (StudentVision.org)
When we do experiments, we wait for the data. When we grow a fruit tree, we wait for the fruits. Science is data; finding it; looking at it, thinking about it. For much of the world data seems quite dull, but for the scientist, data contains hidden within it small sparks which can set the imagination on fire. Each spark of data generates new ideas, new seeds, which will grow in yet undiscovered gardens of research. If we know our own intentions well, there will always be ideas, data and seeds enough for our grand grand children to harvest and sow again to make the world a little more beautiful each morning. from www.studentvision.org It is very sad for any one to lose precious data? A good scientist (PI or not PI) should never lose his or her data. Should a good scientist publish (even not in a Journal) their data before they die? If they are not willing to publish or sharing their data, is there any difference from a data loss?

Jan 5 2010 8:41AM

---

outraged
Dear Ocean(Studentvision.org) Apparently, you are not even able to understand the problem discussed. It looks like your field should be not real science but rather philosophy. This way, although not doing any good to the mankind, your loony ways at least will do no harm.

Jan 5 2010 12:49PM

Share your opinion

Username:

Comment*:

** = required*

Please input the code above. This is to prevent spam.

Can't read the image? Load New Image

Post Comment

Principal Investigators Association
3565 10th St N, Suite B - Naples, FL 34103 USA
1 (800) 303-0129 | (239) 331-4333 | Fax: (239) 676- 0146
Email: info@PrincipalInvestigators.org