Which is more secure: fax or email?

by Leo A. Notenboom

I work part-time for a mental health center in the IT department. Yesterday, I attended a mandatory HIPAA training meeting. In the training, I was told fax is the approved secure method and email was not. I'm really confused about this issue. I researched it on the net, but I haven't come up with a really solid reason why email is less secure than fax if it truly is. While I recognize the limitations of email, transferring via the net could be accessed at any point, yet I feel fax is even less secure. For one, the fax physically lies around until somebody picks it up and you have no assurance that it's the right person. Two, while I understand that a landline would be more secure than the net, if the fax goes directly from point A to point B, in reality, phone calls are transmitted via microwave towers as well and since fax is unencrypted, they could be accessed as easily as email. My feeling is that if we used PGP that email would be more secure than fax. My boss and I both respect your opinion. Can you clear up which is more secure?

Fax vs. email

So, the bottom line is that my opinion runs along the same lines as yours. I don't really consider fax to be any more or less secure than plain text email.
I understand why email would not be allowed. Because it is plain text, you are sending information from one person to another (potentially sensitive), but anybody who has access to the network or the computers in between those twopoints can essentially read that material.

The most common scenario, for example, might be on a service like Gmail or Hotmail. That email is sitting on a third-party server. It's not your server. It's not the recipient's server. It's some third-party (like Google or Microsoft) and theoretically, the email could be viewed by someone else. That of course is a violation of HIPAA regulations.

Fax is a little bit more difficult to argue along those lines, but I believe that the same thing is true. When you send a fax via phone… first of all realize that a fax is an audio transmission. It is (as you said) unencrypted so what that means is that you send a fax from point A to point B, anybody who can listen in on that phone line can receive the fax as well. Anybody with any kind of eavesdropping equipment, anybody who even happens to pick up the same line as that particular fax happens to be getting sent on can in fact receive the fax and as a result, see it.

I actually take this one step further. My concerns go a little bit further than this. A fax really is nothing more than an image of a document, which means that it's also very, very easy to forge. In fact, in many cases, fax signatures are considered legal. In other words, they are considered as binding as a physical signature on a piece of paper. Given how easy faxes are to forge, that just really boggles my mind.

Follow the laws

Now, the real problem here is not so much the technology involved but the laws. Again, I'm not a lawyer, I don't want to infer in any way that I am. But, I definitely would *strongly* recommend that you – whatever you do – you do what the HIPAA regulations require you to do whether they make sense or not. Because even when you do something that makes total technological sense, if it happens to run afoul of the regulations, you could still get in trouble which is kind of frustrating, I understand. But it is what it is.

Encryption

In reality, I'm with you also that PGP (any kind of encrypted email) is much more secure than any of the above.

What it really means is that the email is encrypted at the start. So anywhere between the start, between sending and reception, it is unintelligible to anybody who might actually happen to get a copy of it as long as they don't have the appropriate encryption or decryption key.
PGP, being a public key system, means that you could say that "this message" can be unencrypted by only "this" specific recipient, the specific recipient who holds this specific public key.

So, yeah, absolutely! Encryption of almost any sort (although it needs to be strong enough) is going to be stronger than, is going to be more secure than either fax (over voice lines) or email (plain text email) over the internet.

So, ultimately like I said, I won't really say that email or fax is stronger, or that fax or email is less secure (or more secure) than email or fax. I believe them to both be fairly unsecure.

Security is difficult

If I were writing the HIPAA regulations, for example, I would insist that all of that kind of communication be encrypted. The problem with encryption (and I've written about this before) is that encryption is… as it turns out, is "hard."

Not hard technologically. That's been solved. It's hard to *implement* in a public way – in a way that is consistent across multiple computers:

- Installing PGP? That's really hard to do in common email programs (Thunderbird happens to have a great plug-in that just does it).
- Having people manage their own public and private keys? That's really difficult for the average consumer.
- Same thing for other encryption schemes, other certificate schemes, other public and private key schemes, and so forth.

It's all a level of complexity that A) hasn't been standardized across email systems or email programs and B) is fairly confusing to the average consumer. And it usually is the average consumer who's at the receiving end of some of this protected communication.

So, I can't really give you an answer about what to do to make HIPAA more secure. You've just got to follow the rules of HIPAA. But, in terms of the technologies involved, I would prefer to see encrypted email.

In fact, one of the things that you will find if you've got a good health care provider is that they will not send you email. They will instead direct you to a web-based interface to their system on which you can read that message. The message may then be encrypted on their server. It's encrypted in transit because it's an https connection to their server. And thus, the only place it's visible to the user (to anybody) is when it's being displayed by the authorized and logged in consumer; or when it's being accessed by the authorized and logged in provider at the other end.