

# Patient Data Security Paramount Issue in Clinical Trial Recruitment

Roger Smith, Sr. Vice President, Operations, Acurian

*The threats to patient data are increasing, and increasingly public. They typically do not come from some nefarious hackers, either. Rather, security breaches are usually the result of human error.*



THE VAST MAJORITY OF THESE SECURITY FAILURES, INCLUDING THE LARGEST ONES, STEMMED FROM A LAPTOP OR DISK BEING LOST OR STOLEN.

For example, the Department of Health and Human Services (HHS) reported in April 2010 that over just six months, 64 healthcare organizations suffered breaches of patient medical records so serious that they warranted public reporting under the Health Information Technology for Economic and Clinical Health Act (HITECH) provisions of the 2009 stimulus act. HITECH requires prompt notification of breaches of “unsecured protected health information” involving 500 or more individuals. The April list, documenting security failures from September 2009 through March 2010, involved 23 hospitals, 13 insurance plans, 13 physician practices and four clinics. And while the median size breach affected 2,667 records, one insurer had almost one million records exposed. These weren’t the result of criminal schemes — the vast majority of these security failures, including the largest ones, stemmed from a laptop or disk being lost or stolen.

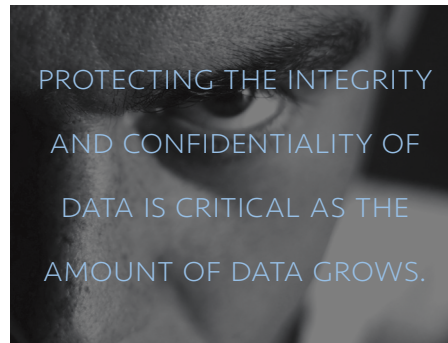
The privacy of patient data is particularly complex in the context of clinical trials, where a delicate balancing act is required to protect the confidentiality of individuals and access to information by clinicians and the trial’s sponsor. The pharmaceutical sponsor of a trial must be one step removed from the recruitment process, and yet the security policies of the two entities must mesh. The starting point in choosing a patient recruitment vendor, therefore, should be an open and frank discussion about which standards should apply during recruitment methods, both in terms of custom software developed by the vendor and hosted software.

When considering a vendor for patient recruitment for clinical trials, a life sciences company must look far beyond the ability to identify, screen and refer patients. Recruitment firms must also be able to ensure the safety and security of the reams of personal

information gathered on each patient, both during the collection process and storage. The ability to safeguard the personal information of those patients can be just as critical to the success or failure of a trial as any adverse events that may occur.

Increasingly, pharmaceutical companies, under the tutelage of their legal departments, are auditing the ability of vendors to offer state-of-the-art technology and rigorous privacy standards to protect the privacy of patients. However, increased scrutiny brings about delays in clinical trial enrollment. Legal departments and information technology teams charged with ensuring that the vendor operates according to promised security standards are usually under no pressure to take into consideration the timelines developed by the clinical teams; they are most concerned that the sponsor will not be put at undue risk. These security audits can easily take six months from start to finish, throwing development plans far off schedule.

It is not uncommon for a pharmaceutical company to actually hire a third-party firm to find weaknesses in these privacy safeguards, and a failure to withstand such scrutiny can lead to the entire trial being shut down. Consequently, clinical teams need recruitment firms that can handle the privacy, legal and technology security issues demanded by their trial sponsors. Recruiters must invest in the expertise to protect personal information on tens of millions of people in their databases, and be able to demonstrate the thoroughness of that protection



whenever asked. This high demand for iron-clad security protections calls for substantial, continuous investments of time and money in both the physical network and recruitment processes—investments that fewer and fewer patient recruitment firms will be able to sustain.

Protecting the integrity and confidentiality of data is critical as the amount of data grows. The risk of loss or compromise involved in collecting patient data is more subtle, perhaps, than those faced by the banking and financial industries, but privacy can be just as crucial to a patient with a debilitating disease. Patients want assurance that their personal medical histories will not be leaked all over the Internet, and the trial sponsor needs to be able to trust that the patient recruiter can offer that assurance. At the same time, sponsors must have access to information—creating a fine and often shifting line.

Patient recruitment companies must be able to provide valuable intelligence to pharmaceutical and device makers about their own experience with security software, and how that experience has helped define and modify policies. This intelligence can run both ways. Pharmaceutical

companies have seen their own security troubles—as in 2002, when a large drug maker inadvertently sent out a mass email containing the Internet addresses of all 669 patients who had signed up for a medication reminder service. The Federal Trade Commission (FTC) launched an investigation that resulted in the company being ordered to develop software safeguards—and the FTC reviews those safeguards every year. A painful event, but also an educational one, for both the company and its vendors.

In short, vendors and sponsors are learning from each other at a time when new methods of recruitment and data management are emerging that may not have decades of experience on which to draw. With the emergence of social media such as Facebook, Twitter and YouTube—all eagerly embraced by patients—new privacy processes must be developed. Many people have shown little hesitation in posting their medical data for all to see on patient engagement sites such as PatientsLikeMe.com. That data, which can no longer be considered private by any legal standard, is a valuable resource for clinical teams. But new media still requires best practices, and Acurian is developing standards on how to both approach potential patients online, and provide security for their information.

The need to reassure patients about the safety of their most personal data makes patient recruitment very much a consumer issue. Although recruiters are not subject to HIPAA rules on medical data security, nor do they handle or access actual medical

records, the concept of data security must be treated almost as rigorously. Acurian has established a set of golden rules designed to reassure both patients and clinical sponsors, explained in detail in a thorough, nine-page privacy policy for patients, available for all to see on its website.

### The four core principles stated up front are:

1. We will not share your personal information with anyone without your prior permission.
2. We will never use your personal information for any purpose without your permission, and then we will use it only for that purpose.
3. We will keep your personal information private and secure.
4. Patients have the right to withdraw their consent, in an easy and straightforward manner, at any time, for whatever reason.

*All of the firm's software, policies, procedures, computer infrastructure and personnel training are based on these core principles.*

This responsibility to the patient does not end at the U.S. borders. Clinical trials are typically international in scope, and a recruitment firm must be able to meet the security requirements of any number of different nations. Although such internationalization can be complicated in practice, a vendor should be able to demonstrate its business is aligned with global standards.

That being said, compliance with global privacy standards is a steep learning curve and requires considerable investment of time and expense. Trial sponsors will not be satisfied with service providers whose only global capabilities are subjective deliverables like translated posters and brochures provided to sites; the recruitment industry has to develop global capabilities that are metric driven and transparent. Again, only a handful of firms can sustain such an investment in an infrastructure that supports services that are objectively measurable.

Acurian now offers truly global services that are as measurable and accountable as its U.S. operation, but the effort required to do so was intense. Much of that investment focuses on personnel training. Policies and procedures are only as good as the people who carry them out, and pharmaceutical companies must and should scrutinize the staff that will be interacting with patients and their data. Training, then, becomes a key aspect that clinical teams should take into account when considering a recruitment firm. Acurian realizes this, and puts its employees through 40 to 60 hours of training when hired. It is also more than reasonable that clinical teams should expect recruitment vendors to have the depth of personnel in all key areas to handle the verification process. Acurian's chief privacy officer is always available to work with the trial sponsor's legal team to explain how privacy standards will apply—removing that burden from clinical team members.

The average clinical team, however, does not typically put as much consideration into the nitty-gritty of such security issues as is necessary when choosing a recruiter. Privacy and information security should in fact be a key variable when the team is determining which vendor to work with. Security is increasingly a top-down mandate from the pharmaceutical companies, and sponsors are saying that information security readiness will need to be demonstrated as a condition of awarding a contract. Therefore, clinical teams must require that prospective vendors demonstrate in the request-for-proposal process that their recruitment services will not be held up or shut down by the inability to meet standards.

The end result of this industry focus on information security will almost certainly be fewer recruitment firms capable of providing advanced, global services to trial sponsors because they cannot meet rigorous demands for standards. It will be difficult for boutique recruitment firms to maintain the continual investment in legal expertise and technology infrastructure necessary to pass comprehensive audits. Only large, well established recruitment firms with expertise in data collection and handling will ultimately survive and thrive in this environment.

## ACURIAN WHITEPAPER SERIES



### About Acurian

Acurian is a leading full-service provider of clinical trial patient recruitment and retention solutions for the life sciences industry. Through its proprietary patient panel of over 65 million patients, centralized advertising capabilities, and a fully hosted enrollment management technology platform, Acurian is able to identify, contact, prescreen, and refer patients into clinical trials, all while supporting investigator sites with services to maximize the randomization potential of every referred patient. Since 1998, Acurian has supported over 400 protocols for more than 60 companies. Acurian's investors include Euclid SR Partners, ProQuest Investments, JP Morgan Partners, Flatiron Partners, CDP Capital Technology Ventures, and Merck Capital Ventures.

### For More Information

For more information about Acurian, visit [www.acurian.com](http://www.acurian.com)