with that complexity. One especially promising technique highlighted in several talks was the 'adaptive' clinical trial, which allows researchers to avoid being locked into a single, static protocol for the duration of the trial. Instead, investigators can evaluate data as they come in, and use that information to change a trial's structure (see page 1258).

Such flexibility is particularly important in cancer research. Investigators have struggled to plan clinical trials that can incorporate an ever-proliferating list of molecular biomarkers — features such as mutations or gene-expression patterns that can be used to distinguish one person's tumour from the next person's. The idea is to find markers that can identify a subset of people for which a given therapy is working, even when it seems to have little effect on the patient population as a whole. Adaptive trials thus allow investigators to analyse the data midstream, correlate those results with known biomarkers, and then alter the course of the trial in light of that information — perhaps by enrolling additional people with cancer on the basis of their biomarker status. The trial then continues, targeting those people most likely to benefit.

Researchers have dabbled with such experiments for years. But it was only in 2007 that the European Medicines Agency (EMA) published a paper outlining appropriate adaptive-trial conduct, and only in February 2010 that the US Food and Drug Administration (FDA) followed suit with its draft guidance to industry. The FDA draft is open for public comment until 1 June.

Guidance from these key agencies is likely to spur interest in the trials, but it will take more than that to fully exploit the technique's potential. Because adaptive trials require more statistical sophistication than conventional ones, for example, medical researchers will have to work with statisticians on trial design from the outset. And because the trials require extra months of planning time, pharmaceutical companies will have to revise the common practice of financially rewarding the speed with which a clinical-trial team enrols its first patient, to avoid tempting researchers to shortcut the planning.

And there are potential pitfalls with adaptive trials. Perhaps most importantly, researchers who use adaptive techniques will have to take care that they do not fool themselves. By changing the patient population to one that is more likely to benefit from the treatment, they can inflate the risk of reaching a false-positive conclusion. They also run the risk that the interim data required to take that step might compromise a trial's double-blind safeguards, influence patient and investigator behaviour, and colour the results even further. For these reasons, the FDA and the EMA advise against using an adaptive trial when a standard trial will do, and urge extra caution in designing the late-stage clinical trials that are crucial to determining drug approvals.

"Undertaking adaptive clinical trials is an experiment in itself: there is much still to be learned about the unforeseen pitfalls, and what the best practices are."

The two documents also outline the statistical methods that can be used to control the false-positive rate, and call for appointing an independent body to handle the interim review. But these guidelines cannot be taken as the final word. Undertaking adaptive clinical trials is an experiment in itself: there is much still to be learned about the unforeseen pitfalls, and what the best practices are. As always in science, investigators must be ready to adapt their approaches as the data come in. ■

Security first

Scientists must be more proactive in encouraging good cybersecurity practices.

Most scientists, like most Internet users, probably think of cybercrime as a misfortune that happens to others — to banks, say, or to online retailers who are careless with customers' credit-card information, or to individuals who fall for a get-rich-quick e-mail from Nigeria.

But the unsettling truth is that academic institutions are among hackers' prime targets. Not only do campuses tend to be richly supplied with personal computers, servers and other computing resources, but they are connected to the world by high-bandwidth networks and populated by inexperienced, casual and sometimes reckless students (see page 1260). This wide-open computational environment is ripe for being co-opted, whether it is to send out spam, run illegal file-sharing sites or launch further cyberattacks.

Worse, from researchers' point of view, is that much — if not all — of their hard-won laboratory data live in that environment, where the information is vulnerable to theft and malicious damage. Computer security has moved up the agenda of universities and other research institutions over the past decade, and most places now have teams of professionals to monitor suspicious traffic and maintain a safe environment.

But such structured, centralized efforts can result in controls that raise scientists' hackles and violate their impulse to do things their own way. As a result, too many researchers set up their own computer systems and ignore any security help the university's professionals can give them.

This attitude is unhelpful, bordering on reckless. University information-technology administrators do need to manage things with as light and as unobtrusive a hand as possible — for example, by making sure that researchers retain the freedom to use the software they choose. But laboratories, especially the smaller ones, need to avail themselves of the professionals' skills as much as possible.

Larger research projects with heavy data needs may have the resources to exercise more autonomy. But even so, it is imperative that such projects put a qualified person in charge of cybersecurity who can take sole responsibility for keeping up with the fast-moving requirements that security issues present.

Large group or small, the ultimate responsibility for protecting data and other resources has to rest with the laboratories that own them. Every lab director must be aware of the risks, and must treat cybersecurity with the same respect as laboratory safety, patient safety and scientific integrity. ■