Rules and Regulations

In May 2018, the new GDPR will come into effect, giving the already well-governed area of clinical trials even more regulations to comply with. The GDPR will harmonise data protection regulations in the EU and replace the present Data Protection Directive and national laws. The impact on clinical trials, sponsors, CROs and the software used will need executive attention and immediate action.

Christer Nilsson at Trial Online

This article will focus on electronic data capture (EDC) software services. Nonetheless, CROs and sponsors have comprehensive regulatory work ahead in order to comply with the GDPR and need to contract expertise immediately if they do not have it in-house.

In the thousands of ongoing clinical trials in the EU today only a few are in compliance with the General Data Protection Regulation (GDPR). The EDC systems do not adhere to the new regulations in terms of user authentication and data encryption.

Collecting health information from subjects falls into the 'special category' of data defined in the GDPR. In clinical trials, the subject's physical identities are pseudonymised using a unique identification code, but the data are still considered to be in this 'special category' of sensitive data with regard to the GDPR due to the fact that pseudonymised data allow for re-identification. This applies even when the code envelope is locked in a safe with only one person maintaining the key code.

When it comes to EDC systems, there are several security measures to take into account. Some may need deep remanufacturing of the software and some may be easier to implement, but this depends on the architecture of the software and how it is designed. Taking into consideration that developing software for clinical trials is a regulated environment, where qualification of the service is mandatory and time-consuming, implementing new features may take months or even a year to complete.

Multi-Factor Authentication

EDC systems should maintain a multifactor authentication service in order to comply with the GDPR. The 'rule of thumb' is that the user authentication relies on 'one thing you know and one thing you have'. Normally, there is a combination of username, password and a token from either a mobile app or a dedicated device, but which EDC systems provide this feature today?

Given the fact that the regulation of strong authentication is similar in the present Data Protection Directive – however differently adapted in national laws – most, if not all, trials conducted in the EU are in breach of this regulation today.

For instance, in 2015, the Swedish Data Protection Authority reviewed four ongoing clinical studies; a key finding was the noncompliant use of single factor authentication, and the sponsors were issued an injunction.

Encryption of Data

EDC systems should also encrypt all sensitive and personal data collected. This may be easy to implement for EDC systems with the appropriate architecture, but others may go out of business in their struggle to comply.

Sanctions

Another big shift in the GDPR compared to the present Directive is the introduction of discretionary fines if or when in breach. These can amount to up to €20,000,000 or 4% of global revenue – whichever is higher – and must be effective, proportionate and dissuasive, and settled by the national authorities. This sanction applies both to the controller (sponsor/CRO) and the processor (EDC provider).

The Time for Transition is Now

Given that clinical trials can run from a couple of months to several years, some will be ongoing when the new Regulation comes into effect. For an ongoing trial, the task to comply with the new regulation is a tall order and, in some instances, it may not even be possible with the service providers in use. The GDPR does not state any transition regulation other than the time from when the regulation was adapted to the date when it comes into effect. So by 28 May 2018, you should be compliant with the GDPR or face the risk of sanctions.

Selecting the Right EDC Provider

Additional factors to consider when choosing an EDC system include the following:

- Your EDC provider should perform continuous reviews of security measures and have frequent testing of security measures implemented
- IT operations should provide redundancy
- The EDC system and provider should support the stated 'right to be forgotten'

- The backup solution provided should be secured to the extent that it is protecting sensitive data from becoming corrupt. The physical protection of the backup solution should also be adequate
- Standard operating procedures should include managing a data breach. Authorities and, in some cases, the person affected should be notified within 72 hours from when a breach is known to the processor
- You and your EDC provider should have a data protection officer appointed (an estimated 28,000 are to be recruited in the EU according to a recent study by the International Association of Privacy Professionals)
- A data processing agreement must be established between the controller (sponsor/CRO) and the processor (EDC service provider)

Not Only GDPR – New GCP in June

The new ICH Good Clinical Practice (R2) – ICH GCP (R2) – adds the present digital landscape to the 20-year old guideline and will come into effect in June 2017.

When the ICH GCP was first issued, trial records were managed in paper format and electronic systems were not available. Since then, we have seen guidelines and best practice guides on how to adapt the paper regulations applied to the digital environment. The second addition of ICH GCP is a welcome update that will require substantial consideration from the industry.

Independent Copy of Source Data

The new ICH GCP states that the sponsor "should ensure that the investigator has control of and continuous access to the CRF [case report form] data reported to the sponsor", and that "the sponsor should not have exclusive control of those data".

This will add an additional responsibility to the sponsor; data exported on a CD-ROM will not suffice anymore. We will see EDC providers offer long-term archive services to maintain electronic CRFs and records, and have them be accessible for the investigator and sponsors after the study.

New service functionality may have to be implemented in many EDC systems in order to avoid the risk of having the data altered in any way, as they should only be available for viewing purposes.

RBM and EDC

The ICH GCP (R2) states that the sponsor should develop a risk-based approach to monitoring, but sponsors and CROs have different solutions on how to move into risk-based monitoring (RBM). Some CROs develop their own procedures and ask for a tailored RBM solution to be implemented into the supporting IT system they use, while others adapt their RBM process to match the way their IT service solution is built. At this point, there is no standard way to move forward with RBM, but it may be easier to adapt a flexible EDC system to an organisation's workflow and processes than have them adapt to the workflow of a system.

Final Note

Furthermore, using Microsoft Excel for data collection should now be a thing of the past. With this approach, compliance with the GDPR and the ICH GCP (R2) will simply not be possible. The risk of sanction fees is imminent and will cause the value of the data collected to become dubious.

About the author

Christer Nilsson is an entrepreneur and the Chief Executive Officer at Swedish data service provider Trial Online, offering EDC and electronic patient-reported outcome solutions. He has a track record of developing several successful business ventures in the past 20 years.

Email: christer@trialonline.com