Electronic Record Security
Overview for PerkinElmer ES Products Using Databases

Introduction
21 CFR Part 11 mandates that electronic records used to support Good Manufacturing Practice (GMP) processes must be maintained in an environment protected from unauthorized access, use or tampering. One method of providing this environment is by use of a database within a software product. Many PerkinElmer ES (Enhanced Security) products use a database or number of databases as a fundamental part of their electronic record security provision. The databases can only be accessed by the PerkinElmer application software. They are not open to access by third party database packages, editors or other software. Only authorized users of the PerkinElmer application can use the product to write data or results to the database or browse the database contents.

This white paper discusses the levels of security provided in the PerkinElmer products using Enhanced Security databases for a typical pharmaceutical installation. The security environment can be regarded as being composed of six elements:

- Physical security
- Procedural security/ user training
- Operating system security
- Software application security
- Database security
- Prime analytical data encryption

Creating and maintaining this environment is the joint responsibility of the user of the system and PerkinElmer. This includes PerkinElmer providing the security functionality within the application software and the user establishing and maintaining the physical, procedural and operating system security.

The following guidelines have been used to produce this document:

- GAMP 4: GAMP Guide for Validation of Automated Systems
- ISPE/PDA: Good Practice and Compliance for Electronic Records and Signatures

www.perkinelmer.com
Security Level 1 – Physical Security

The first level of Electronic Record Security is the physical security employed by a pharmaceutical company to protect its buildings and assets. This may include:

- Site perimeter security
- Building access security
- Room access security

These will stop unauthorized access to the site, building and room containing the PC running the analytical system and holding the electronic records.

Security Level 2 – Procedural Security / User Training

Pharmaceutical companies will typically have policies and procedures covering the security of their electronic records. These will cover:

- How user-ID and passwords are allocated, controlled and should be kept secret and secure
- How IT assets such as PCs and networks are protected and controlled
- How software installations are controlled and supported

Training is conducted to ensure that the staff understands the importance of PC security, how electronic records are secured, the appropriate precautions to be taken to protect password security and the disciplinary implications of password abuse or misuse.

Security Level 3 – Operating System Security

Level 3 security is provided by the operating system itself. The operating system access is set up to require an individual to have an operating system user ID and secret password before the PC can be accessed. This limits and controls access to the PC running the PerkinElmer ES application to authorized staff only.

PerkinElmer provides an operating system ‘lockdown’ script as part of the installation of its ES applications. This ‘lockdown’ prevents the use of Windows Explorer and other such utilities that could be used by an unauthorized individual to view file structures, copy and delete files. It sets read/write and delete permissions to directories critical to the protection of e-records. It is highly recommended that this script is not disabled by users if the highest levels of security are required.

This level of security is additional to that provided by the separate PerkinElmer ES product security.

Security Level 4 – Software Application Security

A high degree of electronic record security is maintained via the PerkinElmer ES application itself. PerkinElmer ES products have a completely separate, self-contained login security feature from that of the operating system. Each user has their unique user ID and secret password for the application, giving them specific permissions in the application. This login security is technically compliant with 21 CFR Part 11 and includes user definable features such as:

- Minimum password length
- Password aging
- Failed login detection and lockout

This database is highly encrypted for security and CRC check summed for tamper evidence.

Security Level 5 – Database Security

For PerkinElmer ES products using databases to store data, results and methods, the databases are encrypted and secured as a fundamental part of its electronic record security provision. The databases contain all the electronic records and can only be accessed by the PerkinElmer ES software; they cannot be opened for access by third party database packages, editors or other software.

Only authorized users of the PerkinElmer ES product can write data or results to the database or browse the database contents. The PerkinElmer ES product is the only legitimate conduit to the database.

21 CFR Part 11 technical compliance functions are ‘hard wired’ into the PerkinElmer ES software functionality. Routine users of the application cannot delete data, results or other forms of prime electronic data or corrupt them – it is not possible from within the application.

PerkinElmer ES database products use a JET database engine not an off-the-shelf database application. Only the PerkinElmer application has access rights to the databases. The key to these rights is not made available to users or third parties and is kept highly secure within PerkinElmer, Inc. Without this key the database is secure.

Level 6 – Prime Analytical Data Encryption

The final level of security is that of prime analytical data encryption. The prime spectroscopic data (spectra) in the database are stored as binary large objects (BLOBS) and are in non-human readable form. The spectroscopic data are stored in a PerkinElmer propriety format. To identify if the database has been tampered with in any unauthorized way they have tamper evident CRC checksums in place.
How Secure Are the Electronic Records?

"How secure are electronic records within the laboratory environment?"

Unauthorized access to GMP software applications and their electronic records is a concern to all pharmaceutical organizations. For an unauthorized person to compromise the PerkinElmer ES database electronic record security the following would have to occur:

■ If the unauthorized person is not an employee of the pharmaceutical company, he/she would have to breach the physical security of the system.

■ To get onto the PC running the PerkinElmer ES application, the unauthorized person would need to have acquired an operating system user ID and secret password. This will need to be obtained from a legitimate user by an unethical route, poor security or collusion.

■ Assuming the operating system security is breached, a PerkinElmer ES product user ID and secret password are necessary to access the package. For the electronic data to be compromised by unauthorized access, the access permission would need to be at the administrator level.

■ If PerkinElmer ES product entry codes are not available, the unauthorized person could attempt to "hack" the database using IS tools. To do this, the operating system security would need to have been breached at a permission level high enough to install and run third party applications. In many pharmaceutical organizations this would be at the highest IT permission level of operating system administrator.

■ Assuming that the database could be "hacked," the unauthorized person would be confronted by prime analytical data being further protected by a PerkinElmer proprietary binary file format.

■ If the unauthorized person then makes a random change to the electronic record, the PerkinElmer ES security features would identify the tampered record by use of a CRC checksum feature.

Pharmaceutical company employees setting out to deliberately compromise the electronic record security in such a manner will be in gross breach of company procedures and security policies.

Summary

The PerkinElmer ES products have electronic records protected from accidental or deliberate tampering by a series of six security layers. Within the context of the risk based approach to GMP and 21CFR Part 11 compliance now being advocated by the FDA the PerkinElmer application databases are adequately protected from accidental or deliberate tampering and are technically compliant with 21CFR Part 11.