Control of Data		
Status: Published		Document ID: 1181
DATE EFFECTIVE 12/14/2022	APPROVED BY Quality Assurance Manager	PAGE 1 OF 4

Control of Data

1 Guiding Principles and Scope

1.1 When computer software and applications (such as the LIMS, Qualtrax, and Rees Temperature Monitoring System) are used for the acquisition, processing, recording, reporting, storage or retrieval of test data, the laboratory shall ensure that:

1.1.1 Calculations and data transfers are subject to appropriate checks in a systematic manner.

1.1.2 Computer software developed by the laboratory is documented in sufficient detail and is suitably validated as being adequate for use.

1.1.3 Procedures are established and implemented for protecting the data; such procedures shall include, but not be limited to, integrity and confidentiality of data entry or collection, data storage, data transmission and data processing.

1.1.4 Computer software and applications are maintained to ensure proper functioning and are provided with the environmental and operating conditions necessary to maintain the integrity of test data.

2 Procedure

2.1 Only Department of Forensic Biology staff members have unlimited access to the Forensic Biology network drive. Exceptions may only be granted by the Director or designee. Access is controlled by the OCME Information Technology (IT) Department. Unless otherwise authorized by an existing standard operating procedure, only the Quality Assurance Manager may authorize the release of data to any party (via any means) external to the Department of Forensic Biology.

2.2 Computer Software

2.2.1 A list of computer software used in the department is found in Qualtrax. When new or a new version of software is utilized, the Fbio_Software_Log workflow should be filled out to keep this log up to date.

2.2.2 Computer software may be used during the processing of case work; however, the results will be incorporated into the case record.

2.2.3 Any calculations and data transfers made using computer software are reviewed for its accuracy by a supervisor prior to its incorporation into a case record and/or are reviewed for its accuracy during the final technical review process of the case.

2.2.4 Computer software or software modifications developed by the laboratory are suitably validated depending on the purpose of the modification.

2.2.5 The appropriate Technical Leader must be consulted prior to validation to ensure that suitable validation tests are carried out. The Fbio Software Evaluation Workflow is utilized to determine necessary testing for new and modified software.

2.2.6 If the software is used to streamline/transfer data, sufficient proof must be furnished to document that the intended purpose of the software is achieved. This may be accomplished by entering a simple set of data to ensure that the streamline/transfer of data is accurate.

2.2.7 If the software is used to calculate data, sufficient proof must be furnished to document that the intended purpose of the software is achieved. This may be accomplished by inputting a simple set of data and comparing it to hand-calculated results to ensure that the calculations made are correct.

2.2.8 Computer software developed by the laboratory must be approved by the appropriate Technical Leader prior to its use in casework.

2.2.9 Validation records are stored by the Quality Assurance Unit and/or Technical Leader(s).

2.2.10 Once calculations and data transfers have been reviewed by a supervisor, they may be deleted from the Forensic Biology network drive. For some data, such as DNA electropherograms, the electronic data will be maintained indefinitely.

2.2.11 Maintenances and records that should be kept against software, but do not warrant a Fbio_Software_Evaluation Workflow should be recorded int the Fbio_Software_Maintenance Workflow.

2.3 Laboratory Information Management System

2.3.1 Data and information associated with laboratory activities are housed in the Laboratory Information Management System (LIMS). Access to LIMS is restricted to users who have an assigned login ID and password. A guide to the general use of LIMS can be found in the LIMS Process Manual.

2.3.2 OCME manages four different LIMS servers: Production, Training, Staging and Development. The Production server is where all applicable casework data is recorded, maintained and stored. The Training server is used for the training of analysts as part of the training program. The Staging and Development servers are environments used for troubleshooting, testing and development purposes.

2.3.3 Routinely, Production and Training LIMS may undergo application maintenance, changes and/or updates.

2.3.3.1 **Application Maintenance** may include, but is not limited to, the installing of server patches and the restarting/rebooting of servers. After any application maintenance, LIMS must be QC'd prior to use by the laboratory. The QC of LIMS will follow the steps as outlined in the LV8.1 QC Documentation.

2.3.3.2 **Application Changes** may include, but are not limited to, the deployment of bug fixes or the deployment of enhancements. Bug fixes or enhancements may be internal or external changes provided by OCME's IT department or the vendor, respectively. After the deployment of bug fixes and/or enhancements to the Production and/or Training servers, LIMS must be QC'd prior to use by the laboratory. The QC of LIMS will follow the steps as outlined in the LV8.1 QC Documentation.

2.3.3.3 **Application Updates** include master data changes and configuration changes. These updates are considered to be internal changes made by the LIMS Super Users but they may also be made by the vendor upon request. LIMS does not need to be QC'd after the deployment of master data changes and/or configuration changes.

2.4 Qualtrax

2.4.1 Qualtrax is a document control software that is shared between various departments within the OCME. Permissions are set to individual folders, documents, workflows, and other aspects of Qualtrax to restrict the accessibility between departments.

2.4.1.1 Due to the nature of Qualtrax, a few select personnel act as Qualtrax Administrators and will have access to all documents in the software.

2.4.2 Access to Forensic Biology specific documentation in Qualtrax is restricted to users who have an assigned login ID and password and are assigned to the Forensic Biology group, or other associated group that requires access, such as the Legal Department. This includes, but is not limited to Quality Assurance Records, Training Records, Standard Operating Procedures, Forms, Memos, and external controlled documents used for laboratory operations.

2.4.3 Documents, such as General OCME policies and procedures that are used by the entire agency can be accessed without the need to log in to Qualtrax.

2.4.4 The Qualtrax server is maintained by the OCME IT Department. Updates are coordinated by, and through, the OCME IT Department in liaison with the Qualtrax Company. As this is a document retention application only, no QC is needed after planned IT maintenance has occurred.

2.4.5 Testing of the Qualtrax Software will be performed after Qualtrax Software Version updates. Testing is scaled to the extent of the update and is coordinated between the Qualtrax Administrators within the Forensic Biology department. Records of this testing are maintained in Qualtrax.

2.5 Continuous Automated Temperature Monitoring System (Rees)

2.5.1 A temperature monitoring system is used to monitor refrigerators, freezers, air temperatures, heatblocks and incubators. Each refrigerator, freezer, laboratory room, heat block, and incubator has its own dedicated temperature probe.

2.5.2 Data and information associated with the temperature monitoring activities are stored in and accessed from the Rees Scientific Centron database and application servers. A guide to the general use of the temperature monitoring system software can be found in the Quality Assurance/Quality Control Manual.

2.5.3 OCME manages the Rees Scientific database and application servers. Access to the application server is restricted to users who have an assigned login ID and password. The application server is used for routine checks of all probes connected to the monitoring system.

2.5.4 Routinely, the server and application may undergo maintenance, changes and/or updates.

2.5.4.1 **Application Maintenance** may include but is not limited to, the installing of server patches and the restarting/rebooting of servers. After maintenance, the application does not need to be QC'd as it is a continuous automated system. The routine checks will identify any communication issues.

2.5.4.2 **Application Changes** may include, but are not limited to, the deployment of software upgrades and bug fixes. These software changes are provided and performed by the vendor and may occur during the annual system verification/calibrations. The application does not need to be QC'd prior to use by the laboratory. Documentation of the annual system verification/calibrations is provided by the vendor.

2.5.4.3 **Application Updates** include program changes to individual users and/or inputs being monitored. These updates are considered to be internal changes made by the OCME system administrators, but they may also be made by the vendor upon request. The application does not need to be QC'd prior to use by the laboratory.