**The requirements are specific to GMP. However, Cogstate complies to almost all the requirements as per GCP and 21 CFR Part 11 requirements.**

**The following are our responses:-**

**General**

1. ***Risk Management***

Risk management should be applied throughout the lifecycle of the computerised system

taking into account patient safety, data integrity and product quality. As part of a risk

management system, decisions on the extent of validation and data integrity controls should

be based on a justified and documented risk assessment of the computerised system.

We are in the process of implementing a formal Risk Analysis procedure for the software development lifecycle (where regulatory and legal risks are being considered and taken into account). This will be implemented by Q1 2015.

Although a formal risk assessment has not been carried out, during the product design stage, an informal review of data integrity, security is always done and product quality assured through thorough validation (i.e. complete validation of developed systems).

Cogstate system is not a medical device, hence we have not implemented risk management procedures for patient safety in particular.

2. ***Personnel***

There should be close cooperation between all relevant personnel such as Process Owner,

System Owner, Qualified Persons and IT. All personnel should have appropriate

qualifications, level of access and defined responsibilities to carry out their assigned duties.

We have job descriptions and training plans for all staff. All our systems have various access levels for authorized personnel. Please refer to the attached 21 CFR Part statement.

3. ***Suppliers and Service Providers***

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install,

configure, integrate, validate, maintain (e.g. via remote access), modify or retain a

computerised system or related service or for data processing, formal agreements must exist

between the manufacturer and any third parties, and these agreements should include clear

statements of the responsibilities of the third party. IT-departments should be considered

analogous.

3.2 The competence and reliability of a supplier are key factors when selecting a product

or service provider. The need for an audit should be based on a risk assessment.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed

by regulated users to check that user requirements are fulfilled.

3.4 Quality system and audit information relating to suppliers or developers of software

and implemented systems should be made available to inspectors on request.

We do not engage any external developers or suppliers for any software development work nor do we purchase off-the-shelf software to deliver services for clinical trials.

**Project Phase**

4. ***Validation***

4.1 The validation documentation and reports should cover the relevant steps of the life

cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria,

procedures and records based on their risk assessment.

4.2 Validation documentation should include change control records (if applicable) and

reports on any deviations observed during the validation process.

4.3 An up to date listing of all relevant systems and their GMP functionality (inventory)

should be available.

For critical systems an up to date system description detailing the physical and logical

arrangements, data flows and interfaces with other systems or processes, any hardware and

software pre-requisites, and security measures should be available.

4.4 User Requirements Specifications should describe the required functions of the

computerised system and be based on documented risk assessment and GMP impact. User

requirements should be traceable throughout the life-cycle.

4.5 The regulated user should take all reasonable steps, to ensure that the system has been

developed in accordance with an appropriate quality management system. The supplier should

be assessed appropriately.

4.6 For the validation of bespoke or customised computerised systems there should be a

process in place that ensures the formal assessment and reporting of quality and performance

measures for all the life-cycle stages of the system.

4.7 Evidence of appropriate test methods and test scenarios should be demonstrated.

Particularly, system (process) parameter limits, data limits and error handling should be

considered. Automated testing tools and test environments should have documented

assessments for their adequacy.

4.8 If data are transferred to another data format or system, validation should include checks

that data are not altered in value and/or meaning during this migration process.

All our systems comply to 21 CFR Part 11 requirements for validation. There is a specification (user requirements documents) for each system. We have Validation Plans put in place and test scripts are generated for testing to occur. Upon completion, there is a Traceability summary and report generated and signed off. The reports identifies any deviations, exceptions and other limitations (if any).

**Operational Phase**

5. ***Data***

Computerised systems exchanging data electronically with other systems should include

appropriate built-in checks for the correct and secure entry and processing of data, in order to

minimize the risks.

The only communication between systems happens during the test data transfer from the USB drive to the secure DataPoint website. This transfer occurs via internet using Security Certificate Layer using encryption to ensure data integrity and data security. Please refer to the Part 11 statement attached.

6. ***Accuracy Checks***

For critical data entered manually, there should be an additional check on the accuracy of the

data. This check may be done by a second operator or by validated electronic means. The

criticality and the potential consequences of erroneous or incorrectly entered data to a system

should be covered by risk management.

There are no manual entries to data on the test software.

7. ***Data Storage***

7.1 Data should be secured by both physical and electronic means against damage. Stored

data should be checked for accessibility, readability and accuracy. Access to data should be

ensured throughout the retention period.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup

data and the ability to restore the data should be checked during validation and monitored

periodically.

We have secure archiving and retrieval procedures. Please refer to the Part 11 statement for details.

8. ***Printouts***

8.1 It should be possible to obtain clear printed copies of electronically stored data.

8.2 For records supporting batch release it should be possible to generate printouts

indicating if any of the data has been changed since the original entry.

Our systems have the capability to print these records.

9. ***Audit Trails***

Consideration should be given, based on a risk assessment, to building into the system

the creation of a record of all GMP-relevant changes and deletions (a system generated "audit

trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit

trails need to be available and convertible to a generally intelligible form and regularly

reviewed.

We have systems and procedures in place. Please see the 21 CFR Part 11 statement attached.

Cogstate never deleted source data.

10. ***Change and Configuration Management***

Any changes to a computerised system including system configurations should only be made

in a controlled manner in accordance with a defined procedure.

We have internal procedures defining these processes and controls.

11. ***Periodic evaluation***

Computerised systems should be periodically evaluated to confirm that they remain in a valid

state and are compliant with GMP. Such evaluations should include, where appropriate, the

current range of functionality, deviation records, incidents, problems, upgrade history,

performance, reliability, security and validation status reports.

At Cogstate, we revaluate our systems every 2 years by carrying out re-validation of the entire systems.

12. ***Security***

12.1 Physical and/or logical controls should be in place to restrict access to computerised

system to authorised persons. Suitable methods of preventing unauthorised entry to the

system may include the use of keys, pass cards, personal codes with passwords, biometrics,

restricted access to computer equipment and data storage areas.

12.2 The extent of security controls depends on the criticality of the computerised system.

12.3 Creation, change, and cancellation of access authorisations should be recorded.

12.4 Management systems for data and for documents should be designed to record the

identity of operators entering, changing, confirming or deleting data including date and time.

We gave access controls (username/password) and audit trails. Please refer to 21 CFR Part 11 statement attached.

13. ***Incident Management***

All incidents, not only system failures and data errors, should be reported and assessed.

The root cause of a critical incident should be identified and should form the basis of

corrective and preventive actions.

We have an internal procedure outlining these processes and controls.

14. ***Electronic Signature***

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the

company,

b. be permanently linked to their respective record,

c. include the time and date that they were applied.

We do not utilise digital/electronic signatures in any Cogstate systems.

15. ***Batch release***

When a computerised system is used for recording certification and batch release, the system

should allow only Qualified Persons to certify the release of the batches and it should clearly

identify and record the person releasing or certifying the batches. This should be performed

using an electronic signature.

This is not applicable as there is no batch release.

16. ***Business Continuity***

For the availability of computerised systems supporting critical processes, provisions should

be made to ensure continuity of support for those processes in the event of a system

breakdown (e.g. a manual or alternative system). The time required to bring the alternative

arrangements into use should be based on risk and appropriate for a particular system and the

business process it supports. These arrangements should be adequately documented and tested.

We have a documented Disaster Recovery Plan in place.

17. ***Archiving***

Data may be archived. This data should be checked for accessibility, readability and integrity.

If relevant changes are to be made to the system (e.g. computer equipment or programs), then

the ability to retrieve the data should be ensured and tested.

As in 7 above.