

PHARMACEUTICAL MANUFACTURING · DATA INTEGRITY

Your Checkweigher Is Now a GMP Data System

Are You Treating It Like One?

By Phillip Ruda · 1 October 2026



In this article

The regulatory direction is clear

A weight result is no longer just a number

Access control is not an IT inconvenience

An audit trail only has value if somebody can use it

Backup and archiving are not the same thing

The supplier relationship is part of the control strategy

Cybersecurity has entered the GMP conversation

Validation does not finish at SAT or PQ

What should manufacturers be asking?

Where the SADE SP 60 Series fits

Final thought

Sources

About CI Precision

The weighing mechanism may be familiar. The regulatory expectations around the data it creates are becoming much harder to ignore.

For many years, a tablet or capsule checkweigher was viewed primarily as a piece of production equipment. Product went in. A weight was measured. Acceptable and unacceptable units were separated. A batch report might then be printed or exported.

That description is becoming increasingly inadequate.

Modern pharmaceutical checkweighers can create thousands, sometimes hundreds of thousands, of electronic records during a single batch. They associate those measurements with products, users, timestamps, limits, classifications, alarms, configuration settings and operator actions.

Those records may subsequently support investigations, process decisions, batch recovery, validation activity or quality review.

At that point, the conversation is no longer only about weighing.

You are operating a computerised GMP system that happens to weigh tablets and capsules.

This changes what manufacturers should expect from the equipment — and what they should ask of the supplier.

The regulatory direction is clear

EU GMP Annex 11 already applies to computerised systems used as part of GMP-regulated activities and requires risk management throughout their lifecycle, validation of the application, appropriate access, data protection and lifecycle controls.

The direction of travel is even clearer in the proposed revision of Annex 11.

The European Commission's consultation draft significantly expands the structure of the Annex, with dedicated sections covering system requirements, supplier management, handling of data, identity and access management, audit trails, electronic signatures, periodic review, security, backup and archiving.

It also places greater emphasis on maintaining systems in a validated state throughout their lifecycle.

An important qualification is that, as of October 2026, the January 2011 revision of Annex 11 remains the operative version. The newer Annex 11 remains a proposed revision following consultation and should not yet be treated as an enforceable replacement.

Even so, it provides a useful indication of how regulators are thinking about modern computerised manufacturing systems.

And it raises a practical question for OSD manufacturers:

If your checkweigher generates GMP-relevant electronic records, are you managing the data with the same discipline as the physical weighing process?

A weight result is no longer just a number

Consider what actually happens when a modern weight sorter processes a tablet.

The machine may record the measured weight, product or batch information, configured limits, acceptance or rejection status, date and time and the user responsible for setting up or starting the operation.

There may also be records showing changes to recipes or limits, user logins, unsuccessful actions, alarms, acknowledgements, report generation and administrative changes.

That information provides context.

Without it, a value such as 201.3 mg tells us relatively little.

With the surrounding metadata, we can establish what product was being processed, which limits were active, who configured the operation, when the measurement occurred and what the system subsequently did with the unit.

The distinction between the result and its context is fundamental to data integrity.

MHRA guidance similarly emphasises the need to preserve records and their associated meaning, restrict administrative access appropriately and protect electronic records throughout their retention period.

Access control is not an IT inconvenience

One of the simplest examples is user access. A shared operator login may appear convenient on the production floor. From a data-integrity perspective, it immediately weakens attribution.

If several people operate under the same identity, it becomes difficult to establish who changed a weight limit, altered a product setting, acknowledged an alarm or initiated a batch.

This becomes critical when an investigation begins months later.

MHRA guidance expects system-administrator access to be restricted to the minimum number of people necessary and administrator actions to be attributable to individuals through unique credentials.

The proposed Annex 11 revision goes further by making Identity and Access Management a dedicated section.

The wider principle is straightforward: access should reflect responsibility.

Operators need the functions required to operate the machine. Supervisors may require different authority. Administrators need configuration capability. Quality personnel may require review access.

Giving everyone the same permissions may simplify administration, but it weakens control.

An audit trail only has value if somebody can use it

Audit trails are another area where specifications can sound more reassuring than the practical reality.

It is easy to say that a system "has an audit trail."

The more useful questions are:

- What events are actually recorded?
- Are previous values retained?
- Can changes be attributed to an individual?
- Is the date and time recorded?
- Can the audit trail be filtered and reviewed?
- Can an ordinary user disable or modify it?

An audit trail should help reconstruct what happened.

For example, imagine that a batch unexpectedly produces a higher reject rate.

If the audit trail shows that the batch was halted, a weight limit was changed, and the batch was then restarted or rerun under the revised setting, QA has valuable evidence.

If it shows who made the change, when it occurred, what the previous value was and when processing resumed, the investigation becomes considerably stronger.

If the only surviving information is the final configuration, part of the history has disappeared.

FDA Part 11 guidance recognises the importance of audit trails and other controls where electronic records can be created, modified or deleted, with their application based on the relevant predicate requirements and documented risk assessment.

The presence of an audit trail therefore should not be the end of the conversation.

Its usefulness depends on what it captures and whether the organisation has a sensible process for reviewing it.

Backup and archiving are not the same thing

This detail is frequently overlooked.

A backup primarily supports recovery after data loss or system failure.

An archive preserves records for long-term retention and later retrieval.

They solve different problems.

A nightly server backup may provide excellent disaster recovery but still be a poor long-term GMP archive if records cannot readily be searched, reconstructed or interpreted years later.

MHRA guidance distinguishes backup for disaster recovery from archiving for protected long-term storage. It also expects retention arrangements to protect records from alteration or loss throughout the required retention period.

Current Annex 11 also requires archived data to remain accessible, readable and intact, including after relevant system changes.

That creates questions which should ideally be answered before equipment is purchased, rather than when the first server is replaced.

- Where does the data reside?
- Who owns it?
- How is it backed up?
- How is it archived?
- Can it still be read if the original machine is retired?
- What happens when software is upgraded?
- Can records be exported in a usable format without losing their meaning?

A machine may have a lifecycle of ten, fifteen or twenty years.

The data may need to survive technology changes during that period.

The supplier relationship is part of the control strategy

There is another consequence of treating production equipment as a computerised GMP system.

The supplier becomes more than a machinery vendor.

Software design, configuration, updates, remote support, cybersecurity, documentation and validation support can all influence the integrity of the system.

Current Annex 11 already requires regulated users to consider supplier competence and reliability and to establish appropriate agreements where third parties provide, configure, maintain, modify or retain computerised systems or data.

The proposed revision further strengthens supplier and service management and makes clear that outsourced activities do not transfer the regulated user's responsibility for compliance.

Procurement therefore needs to look beyond mechanical performance.

A supplier may offer excellent weighing accuracy but still create unnecessary lifecycle risk if software support, access management, update control, validation documentation or long-term data availability are weak.

Cybersecurity has entered the GMP conversation

Historically, cybersecurity and GMP validation could sometimes be treated as separate disciplines. That separation is becoming harder to justify.

A compromised account, unsupported operating platform or poorly controlled remote connection can affect the integrity and availability of GMP records just as surely as a software defect can.

The proposed Annex 11 revision explicitly introduces stronger expectations around information security and ongoing awareness of new threats to GMP systems.

This does not mean every checkweigher needs to become a cybersecurity project in its own right.

It does mean that connectivity has consequences.

Once equipment communicates with a corporate network, historian, SCADA platform or other manufacturing system, IT security and GMP system ownership need to meet in the same conversation.

Validation does not finish at SAT or PQ

One of the more important ideas within the proposed revision is lifecycle management. A computerised system should be validated before use and then maintained in a validated state throughout its lifecycle.

That is significantly different from treating validation as a project milestone completed shortly after installation.

- Software changes.
- User roles change.
- Infrastructure changes.
- Operating systems age.
- Interfaces are added.
- Servers move.
- Security threats evolve.
- Suppliers issue updates.

Each change does not automatically require full revalidation, but its impact should be understood and controlled.

This is where periodic review, documented configuration, change control and supplier support become part of the long-term compliance position.

A machine that passed IQ/OQ ten years ago is not automatically a well-controlled computerised system today.

What should manufacturers be asking?

For a checkweigher generating GMP-relevant electronic records, I would expect the equipment assessment to go well beyond accuracy and throughput.

A useful starting set of questions is:

- Are users individually identifiable, with permissions appropriate to their roles?
- Which actions and changes are captured in the audit trail, and can that information be reviewed easily?
- Are the original electronic records retained with the context and metadata needed to understand them?
- Can records be exported and retrieved throughout the required retention period?
- How are backup, disaster recovery and long-term archiving handled?
- What happens to historic records following software upgrades or equipment retirement?
- How are configuration changes and software updates controlled?
- What validation documentation is available from the supplier?
- How is remote access managed?
- Who is responsible for maintaining the system in a validated and secure state through its lifecycle?

Those questions are not confined to large MES, LIMS or ERP platforms.

They increasingly apply to intelligent production equipment as well.

Where the SADE SP 60 Series fits

The SADE SP 60 Series was developed for pharmaceutical environments where the weighing result and its supporting electronic record both matter.

The systems support audit trails, configurable user access and electronic records, with secure data handling and options for CSV reporting and OPC UA integration.

CI Precision also provides validation support appropriate to implementation within regulated pharmaceutical environments.

These capabilities do not make compliance automatic.

No piece of equipment can do that.

Compliance ultimately depends on how the manufacturer specifies, validates, operates, reviews and maintains the system within its own pharmaceutical quality system.

But equipment design can either support that responsibility or make it considerably harder.

And that should influence how checkweighers are evaluated.

Final thought

Pharmaceutical manufacturing equipment has changed.

The stainless steel is still visible. The weighing mechanism is still important. Accuracy, repeatability, throughput and product handling still matter.

But behind the machine now sits something equally important:

A body of electronic evidence describing what happened to the product.

That evidence may eventually be used by Production, QA, Validation, auditors or inspectors to reconstruct a decision made months or years earlier.

Treating the checkweigher purely as a mechanical asset therefore misses part of its role.

If its electronic records are relied upon for GMP activity, the question is no longer simply:

"Does the machine weigh accurately?"

It is also:

"Can we trust, understand and retrieve the data throughout the life of the system?"

That is a much higher standard.

And increasingly, it is the right one.

How does your organisation classify intelligent production equipment: primarily as machinery, or as part of the site's computerised GMP system landscape?

Sources

- European Commission, EudraLex Volume 4, Annex 11: Computerised Systems, Revision January 2011.
- European Commission, Stakeholders' Consultation on the Revision of GMP Chapter 4, Annex 11 and New Annex 22, including the draft revised Annex 11, 2025.
- MHRA, GxP Data Integrity Guidance and Definitions, Revision 1.
- US FDA, Part 11, Electronic Records; Electronic Signatures — Scope and Application.
- CI Precision, SADE SP 60 Series product documentation and technical specifications.

About CI Precision

CI Precision specialises in precision weighing technologies for the pharmaceutical and related life science sectors. Our systems are designed to support robust, data-driven quality control where measurement integrity, process understanding, and defensible decision-making matter.

We are proud to be the only manufacturer of an off-the-shelf semi-automated high precision implant weight sorter. Built specifically for the challenges of development, tech transfer, and operational quality control of medicated implants in both pharmaceutical and veterinary pharmaceuticals applications.