



INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

EU Data Act: Connected Medical Devices Data Access in 2026

Build practical AI for pharma and biotech with IntuitionLabs. We help life-science teams turn complex information and workflows into useful software, governed knowledge systems and AI tools.

Published by IntuitionLabs · 2026-10-28 · eu data act connected medical devices · medical device data access · data act compliance · access by design · medical device apis · gdpr · data sharing architecture · trade secrets

Original article: <https://intuitionlabs.ai/articles/eu-data-act-connected-medical-devices>



In this article

1. Executive Summary
 2. Introduction and Background
 3. Key Changes
 4. Implementation Considerations: Scope and Roles
 5. Data Classification and the Access Catalog
 6. Access Architecture: Direct Retrieval and Third-Party Transfer
 7. Privacy, Medical-Device Safety and Confidentiality Controls
 8. Contract Disclosures, Testing and the Evidence Pack
 9. Data Analysis and Evidence
 10. Implications and Future Directions
 11. Conclusion
-

Executive Summary

The EU Data Act applies to connected medical devices, and its **Article 3(1) design obligation applies to connected products and their related services placed on the market after 12 September 2026**. ([digital-strategy.ec.europa.eu](#)) ([traficom.fi](#)) Its general application date was **12 September 2025**, so the later design milestone should not be treated as the start of all user-access obligations. ([acm.nl](#)) For a manufacturer, the practical deliverable is a documented path from each relevant data field to an accessible output, associated metadata, an authorized user and an accurate pre-contract disclosure.

The scope assessment starts with the product, service and parties. A hospital owning equipment can be a user, while a patient represented in its measurements is a data subject; those roles require separate assessment. The Data Act does not itself supply a personal-data legal basis when the user is someone other than the data subject. ([bundesnetzagentur.de](#)) The Commission distinguishes accessible raw and pre-processed data from inferred or derived outputs. ([digital-strategy.ec.europa.eu](#)) Consequently, an implementation should classify measurements, operating events, service interactions and analytical outputs individually, rather than treating an entire database as either accessible or excluded.

Access by design does not mean unrestricted access. Direct access is required where relevant and technically feasible; a request route remains relevant where direct user access is unavailable. ([ccpc.ie](#)) ([acm.nl](#)) Users must receive access free of charge. ([acm.nl](#)) Privacy, identity verification, confidentiality and device safety should therefore be implemented within the access workflow. Health information remains subject to the General Data Protection Regulation (GDPR), including its special-category conditions. ([dataprotection.ie](#))

This report recommends a field catalog linked to interfaces, a policy service that evaluates requester and recipient rights, proportionate verification, and evidence showing what was disclosed and delivered. OpenAPI, Fast Healthcare Interoperability Resources (FHIR) and OAuth can support these components, but they are implementation options rather than Data Act mandates. ([spec.openapis.org](#)) ([hl7.org](#)) The proposed coverage calculation measures implementation completeness, not legal compliance. Finally, teams should track

legislative change: the Council agreed a Digital Omnibus negotiating position in October 2026, while Parliament's procedure remained at committee stage when checked for this report. Those records establish an ongoing legislative process, not completed replacement rules. (consilium.europa.eu) (oeil.europarl.europa.eu)

Introduction and Background

Connected medical equipment can generate operational records alongside clinical measurements. Determining who can retrieve those records requires more precision than a statement that a device is connected. The Commission explicitly identifies medical devices within the connected-product examples covered by the Data Act, and Germany's Bundesnetzagentur includes equipment used for monitoring and diagnostics. (digital-strategy.ec.europa.eu) (bundesnetzagentur.de) The appropriate starting point is therefore the individual product and its data flows, followed by an assessment of the applicable obligations and exceptions.

This report addresses product leaders, architects, privacy teams and regulatory counsel making release decisions for the European Union (EU). Its reference date is **28 October 2026**. The key statutory distinction is between the Data Act's general application and the later application of the design obligation to products and related services placed on the market after the specified deadline. (traficom.fi) A product program should record the relevant placement facts rather than assume that a model name or software release date settles that question.

IntuitionLabs' editorial perspective in this report is that an access commitment should be traceable to a working capability and its supporting evidence. The architecture below is an analytical recommendation. It does not represent a prescribed EU technical specification, and it does not replace a device-specific legal assessment.

Three kinds of material are kept distinct throughout: requirements drawn from the regulation, explanatory guidance from public authorities, and proposed engineering controls. That distinction matters because even useful official implementation guidance can be provisional. The Netherlands Authority for Consumers and Markets (ACM), for example, describes its published Data Sharing Guidelines as provisional pending further Commission guidance. (acm.nl) Readers should ask EU counsel to assess product scope, enterprise exceptions, personal-data permissions and proposed restrictions before relying on a particular interpretation.

Key Changes

Access becomes a design and release consideration

Article 3(1) requires product data, related-service data and necessary interpretive metadata to be accessible by default, easily, securely and free of charge, in a comprehensive, structured, commonly used and machine-readable format. Direct user access is required where relevant and technically feasible.

(publications.europa.eu) Ireland's Competition and Consumer Protection Commission (CCPC) identifies a built-in interface, an application or another technical tool as possible access mechanisms. (ccpc.ie)

The recommended release control is a documented access design reviewed alongside the product's data architecture. It should state which outputs are available locally, through a service, or through an electronic request. When direct access is unavailable, record the technical reasoning, affected fields and alternative

route. CCPC specifically recommends demonstrating and documenting the reasons for that decision. ([ccpc.ie](#))

A working screen alone is weak evidence of comprehensive machine-readable access. The implementation review should inspect the exported values, metadata and available history. This follows from the statutory emphasis on usable data and the request-based requirement for quality equivalent to that available to the holder. ([publications.europa.eu](#))

Disclosures become part of the product specification

Article 3(2) requires information before a purchase, rental or lease contract, including data types, formats, estimated volumes, continuous or real-time generation, storage, intended retention, access mechanisms and relevant terms or quality of service. Related-service disclosures under the following paragraph add information such as collection frequency, the data holder's identity and intended data uses. ([publications.europa.eu](#)) ([traficom.fi](#))

The engineering implication is to maintain these statements from the same controlled catalog that describes the actual outputs. A catalog change should trigger review of affected customer disclosures. ACM similarly emphasizes explaining what data are collected and how users can consult or request them. ([acm.nl](#)) This creates a useful acceptance test: the described retrieval method should work against the released configuration.

Sharing requires recipient and purpose controls

Article 5 gives users a route to request that readily available data and necessary metadata be supplied to a third party, without undue delay and free of charge to the user. ([publications.europa.eu](#)) Traficom lists user-requested third-party sharing among data-holder obligations. ([traficom.fi](#)) Product teams should therefore design delegated access, not assume that a personal download completes every sharing requirement.

The recipient workflow needs its own eligibility and purpose checks. Designated Digital Markets Act gatekeepers are not eligible third-party recipients under the relevant provision; recipient use is subject to agreed purposes and restrictions, including the prohibition on developing a competing connected product. ([publications.europa.eu](#)) These rules should be translated into recipient registration, contractual terms and authorization policy, with legal review of the proposed use.

The commercial workflow also needs a separate branch. Free user access does not eliminate the regulation's business-to-business compensation framework. A holder must explain the basis of compensation sufficiently for the recipient to assess it against the statutory conditions. ([publications.europa.eu](#)) Recommended access records should distinguish the user's request from any recipient agreement.

Implementation Considerations: Scope and Roles

Decide scope through product and role questions

Apply the following decision sequence to each product configuration. It is a proposed review method, not a substitute for the statutory definitions.

- **Product:** Determine whether the item obtains, generates or collects use or environmental data and communicates product data electronically, physically or through on-device access. ([publications.europa.eu](#))
- **Related service:** Test whether software is functionally linked to the product, including services whose absence prevents a function or which subsequently add or adapt functions. Do not classify every application used in a hospital as a related service. ([publications.europa.eu](#))
- **Territory:** Check EU-market placement and the relevant EU user relationship. A manufacturer's establishment outside the EU does not by itself remove the product from scope. ([publications.europa.eu](#))
- **Enterprise exception:** Have counsel test the qualified micro- and small-enterprise exclusion, including partner, linked-enterprise and subcontracting conditions. It is not a general exemption for every company describing itself as small. ([publications.europa.eu](#))
- **Temporary treatment:** The exception also addresses enterprises qualified as medium-sized for less than one year, and connected products for one year after placement by a medium-sized enterprise. Assess those time limits against documented company and placement facts. ([publications.europa.eu](#))
- **User:** Identify ownership, contractual temporary-use rights and receipt of related services. ([publications.europa.eu](#))
- **Data holder:** Identify the entity with the relevant right or obligation to use and make data available. Do not infer that role solely from the location of a server. ([publications.europa.eu](#))

Maintain separate requester, organization, product and patient identifiers. France's Commission nationale de l'informatique et des libertés (CNIL) notes that several users can coexist for one connected product. ([cnil.fr](#)) A fleet account should therefore be assessed against its entitlement to particular devices, time periods and records, rather than receiving access solely because it belongs to the same institution.

Data Classification and the Access Catalog

Product data concern data generated through product use and designed to be retrievable. **Related-service data** represent digitized user actions or product-related events recorded during the service. **Readily available data** are the relevant data that the holder lawfully obtains or can lawfully obtain without disproportionate effort beyond a simple operation. ([publications.europa.eu](#)) These categories answer different questions: origin, relationship to the service, and availability to the holder.

Do not equate "processed" with "inferred." The Commission includes raw and pre-processed data in its scope explanation while excluding inferred or derived data and content. ([digital-strategy.ec.europa.eu](#)) The recommended classification record should describe the transformation and explain its conclusion. Necessary metadata should travel with the accessible output; catalog interoperability can be supported by the World Wide Web Consortium's Data Catalog Vocabulary (DCAT). ([w3.org](#))

Table 1 illustrates a proposed field catalog. Every example is hypothetical; formats and frequencies below are design choices, not claims about a commercial device.

Illustrative field (Hypothetical Example)	Classification question	Proposed metadata and delivery record
Sensor measurement	Is it retrievable product data, and whose personal data does it reveal?	Unit, calibration context, observation time, source device, available history and access route. FHIR Observation offers an optional measurement model. (hl7.org)
Pre-processed measurement	Does the transformation prepare a reading for use, or generate a distinct inference?	Transformation description, source linkage, quality flag and classification rationale.
Operating event	Is it generated by product use and retrievable?	Event code, timestamp meaning, device identity, retention and export format.
Service interaction	Does it record a user action or event within a related service?	Actor role, affected product, event meaning, collection frequency and service access route.
Analytical score	Is it genuinely inferred or derived, and are its source measurements separately accessible?	Separate entries for the score and inputs, with the reason for each scope decision.
Patient identifier	What legal basis and special-category condition permit the proposed disclosure?	Recipient permissions, purpose and minimization controls. Health information requires particular assessment. (dataprotection.ie)
Metadata	What does a recipient need to interpret and use each output?	Schema, units, enumerations, timestamp semantics, provenance and version. Provenance can describe producing entities and activities. (w3.org)

For every field, the proposed catalog records its source, data holder, relevant user role, classification, format, units, generation and collection frequency, available history, retention and access route. Add quality-of-service characteristics such as delivery frequency and known gaps. Distinguish sensor generation from cloud collection and export availability; a statement that a device generates continuously does not describe every later stage. Keep those descriptions aligned with the pre-contract disclosure. ([traficom.fi](#))

The catalog should preserve distinctions that a database schema alone can obscure. A mixed record may contain accessible measurements, personal identifiers and an inferred output. The proposed approach is to classify components and assemble an authorized response, with explanations for any restriction. Metadata and endpoint descriptions should remain linked; DCAT includes descriptions of service operations and parameters. ([w3.org](#))

Access Architecture: Direct Retrieval and Third-Party Transfer

Provide a usable access path

Select the simplest architecture that meets the assessed obligations and device constraints. A local export, an authenticated service or an application programming interface (API) can support different workflows. CCPC's examples are technology-neutral, while ACM describes an easy online request route where direct access is technically unavailable. ([ccpc.ie](#)) ([acm.nl](#))

For request-based access, preserve the statutory conditions in the acceptance criteria: relevant readily available data and metadata, without undue delay, at the quality available to the holder, securely and free of charge to the user. Continuous real-time delivery is qualified by relevance and technical feasibility.

(publications.europa.eu) An implementation should record available sampling and delivery characteristics without presenting an arbitrary engineering service target as a legal deadline.

Separate extraction, policy evaluation and delivery in the proposed service. Maintain a versioned interface contract: OpenAPI describes Hypertext Transfer Protocol (HTTP) APIs, using JavaScript Object Notation (JSON) documents. (spec.openapis.org)

Implement a controlled transfer sequence

Recommended transfer sequence:

- **Register the requester:** Bind the account to the asserted organization or individual and the relevant device entitlement. The United States National Institute of Standards and Technology's (NIST) Internet of Things (IoT) capability catalog identifies unique logical and physical device identification as a useful security capability. (pages.nist.gov)
- **Verify proportionately:** Request the evidence needed for the access decision. The Irish Data Protection Commission advises limiting additional identification information to what is necessary and proportionate when handling data rights. (dataprotection.ie)
- **Register the recipient:** Record its identity, service and proposed purpose; assess legal eligibility before issuing access.
- **Record the instruction:** Capture the user's requested fields, devices, period and recipient. Keep the instruction separate from the personal-data legal-basis assessment.
- **Evaluate policy:** Resolve entitlement, personal-data permissions, confidentiality conditions and any justified safety restriction before creating the response.
- **Issue limited credentials:** Where OAuth is chosen, follow current security guidance, including Proof Key for Code Exchange (PKCE), appropriate redirect validation and restricted token privileges. (rfc-editor.org)
- **Deliver and terminate:** Record delivery outcomes, provide the agreed stopping mechanism, and enforce expiry or withdrawal in the authorization service.

OAuth handles technical delegation; it does not establish every legal condition for health-data sharing. Bundesnetzagentur identifies the separate legal-basis question where the user and data subject differ. (bundesnetzagentur.de)

For an OAuth implementation, require exact matching of preregistered redirect addresses subject to the specification's native-application exception. Use audience restrictions and sender-constrained tokens where appropriate to the deployment. (rfc-editor.org) Scope tokens to the approved resources and operation, and make revocation testable rather than merely describing it in a contract.

Separate measurements, timestamps and records of access

Name observation, upload and export times separately. FHIR's version-pinned Observation model includes a clinically relevant time or period. (hl7.org)

Use a separate security event record for access activity. FHIR AuditEvent is designed for security logging and can represent the outcome of an event. (hl7.org) Logging should support reconstruction of the access decision without copying all disclosed clinical data into another store. Apply privacy minimization to the log itself, including the information retained and who can retrieve it. Audit design should have its own necessity and retention assessment. (edpb.europa.eu)

Privacy, Medical-Device Safety and Confidentiality Controls

Treat GDPR permissions as an independent gate

CNIL explains that GDPR prevails if the Data Act conflicts with personal-data protection. (cnil.fr) Existing GDPR rights can also coexist with Data Act access rights. (bundesnetzagentur.de)

Identify controller and processor relationships for each disclosure. Where user and data subject differ, assess a valid GDPR legal basis and additional health-data conditions. Bundesnetzagentur identifies Article 6 and, where applicable, Article 9 and ePrivacy requirements; Ireland's regulator explains health data's special-category status. (bundesnetzagentur.de) (dataprotection.ie)

Recommended privacy review questions include:

- **Purpose:** What precise service or activity will the recipient perform?
- **Necessity:** Which personal fields are needed for that purpose?
- **Authority:** Who can instruct the transfer, and what permissions remain independently necessary?
- **Retention:** How long should the recipient and the access service retain their respective records?
- **Risk:** Does the processing require a data protection impact assessment (DPIA)?

The European Data Protection Board (EDPB) explains that privacy by default limits processing to what is necessary for each specific purpose and that likely high-risk processing requires a DPIA. (edpb.europa.eu) Spain's Agencia Española de Protección de Datos (AEPD) separately recommends defining strict retention limits. (aepd.es)

Integrate access changes with device risk management

Medical Device Coordination Group (MDCG) guidance links security controls affecting safety or effectiveness to the safety-risk assessment, and identifies testing as the primary means of security verification and validation. (health.ec.europa.eu)

Assess access changes under applicable Medical Device Regulation (MDR) and In Vitro Diagnostic Medical Devices Regulation (IVDR) duties. MDCG connects software development, information security, verification and validation to these frameworks. (health.ec.europa.eu)

The recommended design separates the data-delivery workload from functions whose availability or timing is clinically important. Test authorization failures, concurrent export requests, malformed requests and interruptions against the applicable device risk analysis. NIST's capability catalog supports protecting stored and transmitted data and restricting logical access to authorized entities. These are useful engineering references, not EU Data Act mandates. (pages.nist.gov)

International manufacturers can reuse suitable evidence across programs while retaining the jurisdictional distinction. The United States Food and Drug Administration's (FDA) cybersecurity guidance addresses design, labeling and premarket documentation; it does not establish the EU access requirement. ([fda.gov](https://www.fda.gov)) The UK Information Commissioner's Office (ICO) addresses lifecycle privacy design, as comparative guidance. (ico.org.uk)

Apply exceptions through a documented decision

The Data Act's security restriction concerns legally established requirements and serious effects on people; a generic security preference does not express that statutory test. (digital-strategy.ec.europa.eu)

- **Personal-data permission gap:** Establish the missing legal condition or limit the response to data that can lawfully be supplied. A user's commercial entitlement does not establish a legal basis for another person's data. (bundesnetzagentur.de)
- **Safety restriction:** Document the applicable security requirement, the serious health, safety or security effect, the agreed restriction and any required authority notification. (publications.europa.eu)
- **Trade-secret safeguards:** Identify the protected data and proportionate confidentiality measures before determining the disclosure route. (publications.europa.eu)
- **Exceptional refusal:** Distinguish missing or ineffective safeguards from the stricter, case-specific serious-economic-damage test for refusal despite safeguards. Document reasons and required notifications. (publications.europa.eu)

Record affected fields, evidence, owner, reconsideration conditions and complaint route. National responsibilities can differ; Germany identifies a distinct role for its federal data-protection authority in overseeing personal-data processing. (bundesregierung.de)

Contract Disclosures, Testing and the Evidence Pack

Maintain a controlled relationship between the data catalog, customer-facing disclosure and deployed access capability. Traficom's detailed guidance includes pre-sale information on generated data volume, generation characteristics, storage and retention. (traficom.fi) Related-service information requires additional attention to collection frequency and the service relationship. (publications.europa.eu)

Table 2 maps selected requirements to proposed controls and evidence. The control choices are recommendations; the cited sources establish their underlying requirements or relevant technical patterns.

Requirement or objective	Proposed control	Review evidence
Accessible data and metadata	Test local and service access against approved catalog entries.	Output samples, schemas and a documented direct-access decision. (ccpc.ie)
Comprehensible pre-contract information	Generate disclosures from approved catalog content.	Versioned customer document and comparison with released behavior. (acm.nl)
User-requested third-party sharing	Bind recipient grants to the recorded user instruction.	Recipient record, authorization decision and transfer outcome. (traficom.fi)

Requirement or objective	Proposed control	Review evidence
Purpose-limited authorization	Restrict credential privileges to approved resources and operations.	Authorization configuration and negative test results. (rfc-editor.org)
Machine-readable interface description	Maintain a versioned interface contract and schema.	OpenAPI document and operation-level security definitions. (spec.openapis.org)
Proportionate identity checks	Define acceptable evidence according to access risk.	Verification policy and minimal decision record. (dataprotection.ie)
Security and delivery audit	Record requester, decision, operation, time and outcome.	Protected event records with a defined retention policy. (hl7.org)

The evidence should connect the customer's experience to a specific released configuration. A contract template alone cannot show whether a requested field arrives with usable units and timing. Conversely, an export test cannot show what the buyer was told before contracting. Read the two records together.

The Commission's model contractual terms can inform drafting, but their use is voluntary and users can amend them. (digital-strategy.ec.europa.eu) The recommended contract review should preserve the distinction between data access, personal-data permissions, recipient obligations and compensation, rather than compress them into one undifferentiated acceptance box.

A practical release evidence pack should contain:

- **Scope record:** Product, service, territorial and enterprise assessments with responsible owners.
- **Catalog baseline:** Approved field classifications, metadata and access characteristics.
- **Permission record:** User entitlement, recipient eligibility and personal-data assessments.
- **Delivery evidence:** Successful requests, denied unauthorized requests and termination behavior.
- **Lifecycle record:** Disclosure versions, retention decisions and review triggers.

The European Union Agency for Cybersecurity's (ENISA) healthcare procurement guidance covers the procurement lifecycle and identifies information suppliers should provide. (enisa.europa.eu) This supports organizing the pack so a hospital's technical and privacy reviewers can find evidence without relying on a sales description. Documenting design decisions also follows AEPD's privacy-engineering guidance. (aepd.es)

Data Analysis and Evidence

Use the relevant dates, without inventing a market benchmark

The quantitative core for this implementation decision is statutory timing and measured product coverage. This report does not establish a medtech-wide compliance rate, a typical API implementation cost or a sector adoption benchmark. Its coverage metric below is a proposed internal calculation, not an empirical finding or regulator-approved score.

Table 3 separates legal application dates from the status of supporting guidance and legislative proposals.

Date	Verified event	Practical interpretation
12 September 2025	General Data Act application began. (acm.nl)	Assess existing access and disclosure obligations independently of the later design milestone.
After 12 September 2026	Article 3(1) applies to the specified products and related services placed on the market after this date. (publications.europa.eu)	Record placement facts and include access architecture in release evidence. Traficom uses the same after-date distinction. (traficom.fi)
15 May 2026	ACM published its provisional Data Sharing Guidelines. (acm.nl)	Use the guidance with its stated status, rather than treating it as final legislation.
21 October 2026	The Council agreed its negotiating position on digital legislative simplification. (consilium.europa.eu)	Track the legislative procedure; a negotiating position is not completed enactment. (consilium.europa.eu)

The design date should not be turned into a statement that all older products are outside the Data Act. Equally, a product-family development date is not the regulation's definition of placement: the statute refers to the first making available of a connected product on the Union market. ([publications.europa.eu](#))

Calculate field coverage from reader-supplied inputs

For internal measurement, define **S** as the approved set of in-scope field entries for one released configuration and access scenario. Count an entry as implemented only when its applicable access, metadata, permission and disclosure controls have passed the team's review. These are proposed measurement rules.

Calculate **coverage = 100 × implemented entries / entries in S**. If S is empty, report "not applicable" with the scope rationale rather than dividing by zero. Count a field once in the headline ratio, and retain separate views by device configuration, user role and delivery route. The percentage multiplier is arithmetic, not a statutory threshold.

Use the following reporting controls:

- **Denominator stability:** Version the field set and preserve reasons for additions, exclusions and reclassification.
- **Control intersection:** Count a field only when all applicable controls are evidenced, rather than averaging unrelated completion percentages.
- **Quality visibility:** Report unavailable history, timing limitations and unresolved permission questions alongside the ratio.
- **Operational evidence:** Measure actual request and delivery behavior against the approved catalog; keep the event outcome available for review. ([hl7.org](#))

A high ratio can coexist with a missing important field or an incorrect scope decision. The proposed metric is therefore useful for finding incomplete work and showing changes over releases, while legal and safety reviews remain independent acceptance conditions.

Implications and Future Directions

Keep standards modular and legal assumptions reviewable

The recommended architecture uses interchangeable components: catalog, policy evaluation, extraction, delivery and audit. A common catalog can support several transport choices without implying that every customer must adopt the same API. DCAT addresses catalog interoperability, while OpenAPI describes HTTP interfaces; neither source establishes that its specification is mandatory under the Data Act. ([w3.org](https://www.w3.org/)) (spec.openapis.org)

Regulatory tracking should identify what changed, its legal status and which product assumptions it affects. The Commission's FAQ landing page identifies its published version, and the Data Act Legal Helpdesk offers direct assistance to organizations. (digital-strategy.ec.europa.eu) The Digital Omnibus should remain a tracked change item: the Council described a negotiating mandate, and Parliament's procedure file remained awaiting a committee decision when checked. (consilium.europa.eu) (oeil.europarl.europa.eu) Do not redesign against a proposed exception as though it were already operative.

Use a staged remediation plan

The following **30/60/90-day plan** is an author-proposed work sequence. These durations are planning choices, not statutory grace periods.

- **Days 1 to 30, ownership:** Name accountable product, engineering, privacy, security and legal owners.
- **Days 1 to 30, scope:** Review product configurations, related services, placement evidence and qualified enterprise exceptions.
- **Days 1 to 30, inventory:** Classify fields, transformations and metadata, then map current disclosures to actual retrieval behavior.
- **Days 31 to 60, access:** Implement the approved direct or request-based path and recipient authorization workflow.
- **Days 31 to 60, permissions:** Resolve personal-data conditions and document the handling of confidentiality or safety questions.
- **Days 31 to 60, evidence:** Test schemas, timestamps, scope enforcement, delivery outcomes and termination.
- **Days 61 to 90, integration:** Exercise the complete workflow with representative user and recipient roles.
- **Days 61 to 90, publication:** Release accurate disclosures with the corresponding product configuration and support process.
- **Days 61 to 90, review:** Calculate field coverage, assign unresolved work and schedule reassessment of legal assumptions.

Keep this work within the product lifecycle. NIST's IoT guidance explicitly spans conception, design, testing, sale and support, offering a useful international engineering reference for maintaining the resulting controls. (nist.gov) Privacy review should likewise extend beyond launch; the ICO's lifecycle guidance is a comparative UK reference for that operational approach. (ico.org.uk)

Conclusion

For connected medical devices, a defensible Data Act implementation connects legal scope to specific fields and working access capabilities. The design obligation applies to the relevant products and related services placed on the market after the statutory milestone, while the broader access framework has an earlier general application date. ([traficom.fi](https://www.traficom.fi)) ([acm.nl](https://www.acm.nl)) Product teams should preserve that distinction in release decisions and remediation plans.

The recommended operating model starts with a controlled catalog: what the product and service generate, how transformations affect classification, what metadata make the output usable, who can request access, and which delivery path fulfills the approved design. It then connects each catalog entry to permissions, disclosures, tests and evidence.

The most consequential review questions sit at the boundaries. A device user can differ from the patient whose data are represented. A technically successful transfer can still need a separate privacy assessment. An inferred score can require different treatment from its source measurements. Those distinctions should be recorded explicitly, with counsel assessing the relevant legal conclusions.

The proposed coverage calculation and remediation plan help organize the work; neither replaces that assessment. The practical outcome is a release process in which teams can demonstrate an authorized request, usable data and metadata, an accurate customer explanation, and a documented response to exceptional cases. That evidence gives product leaders a concrete basis for deciding what is ready and what still needs resolution.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>
2. <https://www.traficom.fi/fi/datatalous-ja-datan-valittaminen/datan-haltijan-velvollisuudet>
3. <https://www.acm.nl/en/publications/data-sharing-guidelines-sharing-data-connected-products-and-related-services>
4. <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/DataAct/Hintergrund/1-Daten/artikel.html>
5. <https://www.ccpic.ie/enforcement-and-regulation/data-regulation/eu-data-act>
6. <https://www.acm.nl/en/online-platforms/data/data-smart-devices>
7. <https://dataprotection.ie/en/dpc-guidance/case-studies/transparency/processing-health-data>
8. <https://spec.openapis.org/oas/v3.1.1.html>
9. <https://hl7.org/fhir/R4/observation.html>
10. <https://www.consilium.europa.eu/en/press/press-releases/2026/10/21/digital-rulebook-council-agrees-position-to-simplify-data-protection-privacy-and-cyber-reporting-rules>
11. <https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025/0360%28COD%29>
12. <https://www.acm.nl/en/publications/publishing-guidelines-acm-offers-businesses-clarity-regarding-sharing-data>
13. https://publications.europa.eu/resource/cellar/ef51c6ab-a06c-11ee-b164-01aa75ed71a1.0006.03/DOC_1
14. <https://traficom.fi/en/digital-services-act/obligations-data-holders>

15. <https://www.cnil.fr/fr/reglement-donnees-data-act-nouveau-cadre-europeen-pour-partage-utilisation-donnees>
16. <https://www.w3.org/TR/vocab-dcat-3>
17. <https://www.w3.org/TR/prov-overview>
18. <https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/technical>
19. <https://www.dataprotection.ie/en/dpc-guidance/case-studies/access-request-complaints/requests-identification-when-responding-access-requests-amicable-resolution>
20. <https://www.rfc-editor.org/rfc/rfc9700.html>
21. <https://hl7.org/fhir/R4/auditevent.html>
22. https://www.edpb.europa.eu/sme/be-compliant/be-compliant_en
23. <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/DataAct/Datenschutz/start.html>
24. <https://www.aepd.es/guides/guide-to-privacy-by-design.pdf>
25. https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf
26. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket>
27. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default>
28. <https://www.bundesregierung.de/breg-de/suche/umsetzung-eu-data-act-2391374>
29. <https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding>
30. <https://www.enisa.europa.eu/publications/procurement-guidelines-for-the-cybersecurity-of-hospitals-and-healthcare-providers>
31. <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>
32. <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series>

THE PUBLISHER

About IntuitionLabs

IntuitionLabs is an AI consulting, custom software development and data engineering firm serving pharmaceutical, biotechnology, medical-device and other life-science organizations. We work with clinical, regulatory, medical-affairs, commercial, quality and IT teams to connect technology decisions with the work people need to accomplish.

AI consulting and adoption

Our AI enablement services cover readiness assessments, use-case selection, governance and policies, team workshops, adoption measurement and ongoing advisory support. We help organizations structure the information layer behind AI: source material, context, permissions and maintained knowledge that make generated answers useful and reviewable. Private LLM inference and hosted AI options support teams evaluating how to operate AI with appropriate control over their data and infrastructure.

Software, data and life-science workflows

IntuitionLabs develops custom software for pharma and biotech, integrates enterprise systems, and builds data engineering and business intelligence solutions. Areas of focus include AI agents, regulatory research, medical writing, medical affairs, CMC information, competitive intelligence and clinical-document workflows. Our eTMF intelligence work includes cross-system reconciliation and inspection-readiness support.

Enterprise platforms and regulated delivery

We provide Veeva services, application support, managed services, integrations and custom applications, alongside enterprise content work involving platforms such as Egnyte. For regulated workflows, our services include GxP enablement, computer-system validation and software development addressing 21 CFR Part 11 requirements. The applicable controls, validation responsibilities and acceptance criteria are defined for each engagement.

Work with IntuitionLabs

Explore [AI enablement](#), [pharma and biotech software development](#), [data engineering and BI](#), and [Veeva services](#). [Contact IntuitionLabs](#) to discuss your workflow, information sources and implementation needs.

IntuitionLabs publishes educational research to help life-science teams make informed technology decisions. Coverage of a product or organization does not imply a client relationship, endorsement or partnership.

Website: <https://intuitionlabs.ai>

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.