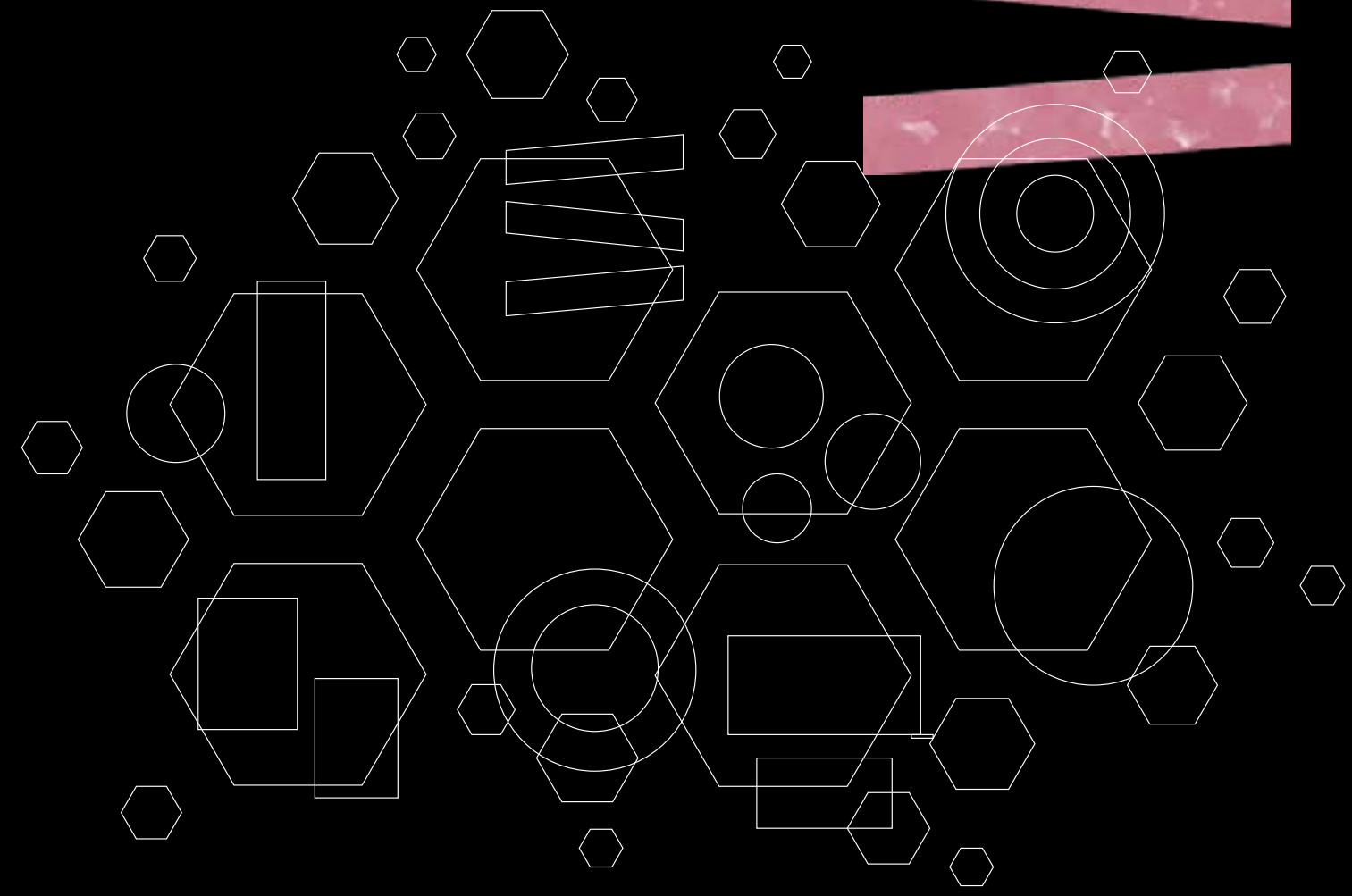
SCTO PLATFORMS

Guidance for Electronic Health Record (EHR) System Requirements in Switzerland



Publisher
Swiss Clinical Trial Organisation (SCTO)
Bern, Switzerland

Authors
Regulatory Affairs Platform of the SCTO

Recommended form of citation
Regulatory Affairs Platform of the Swiss Clinical Trial Organisation (SCTO) (2021). Guidance for Electronic Health Record (EHR) System Requirements in Switzerland. Edited by the SCTO.
doi: 10.54920/SCTO.2021.03

Copyright
This publication is licensed under CC BY-NC 4.0. The content of this publication may be shared and adapted as long as you follow the terms of the license. To view a copy of the license, visit http://creativecommons.org/licenses/by-nc/4.0/. Please attribute this resource to “Swiss Clinical Trial Organisation (Regulatory Affairs Platform)” and link to the following website: www.sctoplatforms.ch.

Contact
To give feedback on this publication or obtain further information, you can contact platforms@scto.ch.
For more information on SCTO Platforms, please visit: www.sctoplatforms.ch.

Content

1. Background 4
2. Requirements 5
2.1.1. Attributability 5
2.1.2. Audit trail 5
2.1.3. Medical oversight 6
2.1.4. Security 7
2.1.5. Access, roles and rights (authorisation) 8
2.1.6. Quality assurance 9
2.1.7. Archiving 10
2.1.8. General study administration 11
2.1.9. Scanning and electronic certified copies 11
3. General recommendations 12
3.1. For sponsors and sponsor-investigators 12
3.2. For study sites 12
3.2.1. Contact person at the IT department for technical and functional questions. 12
3.2.2. Documentation and records 12
4. Certified copies 13
5. References 15
6. Reading recommendations 15

1. Background

Electronic medical records are continuously replacing paper based health records of patients. These electronic medical records are recorded and hosted by electronic platforms, so-called electronic health record (EHR) systems, which are maintained by health care providers and institutions. Although there is a variety of EHR systems currently in use in Switzerland, these are slowly updated or replaced with newer versions or systems, as the requirements to handle data complexity and quality standards are rising.
With respect to clinical research, EHR systems are generally used to host the source data (ICH GCP[1] 1.51, 1.52) of a clinical trial. Thus, special regulatory requirements have to be fulfilled by the EHR systems to be compliant with ICH-GCP[1], Human Research Act[2] and its Ordinance on Clinical Trials (ClinO[3], ClinO-Med[4]), cantonal data protection laws and international recognised standards[5,6].

Purpose
Data integrity is paramount for the credibility and reliability of clinical research comprising both clinical trials (ClinO, linO-Med) and research projects (HRO). Thus, it is essential to ensure that health related data are assessed and recorded by a robust and high quality standard electronic system which provides adequate measures of data control and data protection and allows data reconstruction.
As was shown by a survey that we conducted among Swiss clinical researchers and research staff in January 2019[7], uncertainty is broadly present regarding the compliance of EHR systems with respect to the technical and functional requirements to be fulfilled by such a system in the setting of clinical trials[7].
This guidance is intended to provide an overview of the system requirements which an EHR system is required to fulfil in order to guarantee that data recorded in the EHR system are valid and reliable to be further used for clinical trials and research projects and that such a system allows source data verification compliant to data protection laws.
This guidance is addressed to sponsor-investigators and investigators to support them to fulfil their obligations in accordance to ICH-GCP[1] (4.1.3, 4.2.5, 4.2.6, 4.2.6, 5.0, 5.5.3, 5.15, 5.18.3, 5.20.1). Hence, it shall be of help for monitors to support the study sites and to evaluate source data assessment at the study site if necessary or required.

2. Requirements

2.1.1. Attributability

Health related data which are stored in EHR systems and retrieved from EHR systems have to be attributable to individual trial subjects.

ICH GCP 2.10, 4.9.0 and EMA eSource reflection paper topic 2.

2.1.2. Audit trail

The audit trail allows complete reconstruction of any changes made to health-related data in the EHR system and as a consequence to study data.

a) The EHR system should have an integrated audit trail logging the following items regarding the access of patient health records:
   - date and time stamp of any login, access and action
   - The time and date format of the audit trail records should be specified.
   - user ID of accessing person
   - hospital patient ID, patient's name and date of birth
   - type of record accessed
   - any action (e.g. open, write, edit, release, delete) must be traceable. Thus, recording of any action should be logged at the lowest level or as far as possible (e.g. at the level of data fields).
   - with special regard to document the medical oversight of the investigator, the audit trail should record the investigator's review of electronic test and assessment results (e.g. laboratory tests, x-rays, ECGs, etc.).
   - recording details of modification by displaying what has changed, either by coloured highlighting of a modified text/data entry, modification or deletion or by displaying the modified data field with the new and the old value (numbers or text)
   - version history of e.g. reports.
   - possibility to document the reason for any changes made to the source data.

b) The EHR system does not allow overwriting of the audit trail.

c) The EHR system does not allow any alteration of the audit trail.

d) The audit trail has to be easily and readily accessible to the investigator, monitor, auditor or inspector to allow for medical oversight and monitoring, auditing or inspection purposes.

e) The retention and availability of the audit trail has to be warranted as long as required for medical records. This needs to be in compliance with the archiving requirements as set out in the study protocol and at least legally required as per local regulations.

Recommendations

- The items of the audit trail should be displayed in chronological order to enable a clear reconstruction and traceability of changes.
- The system should allow an export of the audit trail in a human readable and common data format e.g. .xls, .csv and/ or printing.

ICH GCP 2.10, 2.13, 4.9.0, 5.5.3 and 5.5.4, EMA eSource reflection paper topic 2, ClinO art. 18

Suggestions for mitigation in the absence of an appropriate audit trail
In case an appropriate audit trail is not available, the study site has to ensure processes to allow data reconstruction by means of e.g.:

- Printing of medical records in defined intervals. Hard copies printed from the medical records derived from the EHR system have to be complete, dated (date of printing), paginated, and confirmed by the investigator with his/her dated signature (initialled) that the printouts are the true copy ("certified copy") of the electronic records (see also section 4).
- Maintenance of a change log to document any changes made in the source data.
- Marking of new entries/corrections in the system by date and name of modifier. Hard copy printouts have to be made as described above.

Note

- Mitigation strategies (extent and strategy should be recorded to warrant traceability) to be implemented should be based on applicable and individual risk assessment and may vary from study to study. For clinical trials where a formal risk assessment has to be done, applicable descriptions and justifications may be recorded there.
- Hard copies have to be kept as part of the Investigator Site File (ISF).
- All mitigation processes should ideally be described in a SOP.

ICH GCP 1.63, 8.1 Addendum, EMA eSource reflection paper 6.3.3 and topic 4

2.1.3. Medical oversight

As entries in the medical records of patients are made by various medical staff,

a) the traceability has to be warranted regarding the user identity and time of data entry/modification;

b) the investigator has to demonstrate medical oversight about the records of his/her trial participant(s), as entries in the medical records of a patient may also be done by others, i.e. the study coordinator and non-study staff. This can be achieved by an audit trail (see section 2 of this Guideline) and a differentiated role and authorisation structure (see section 5 of this Guideline). A confirmation (e.g. in written or by an audit trail log) or a final release of the records may only be performed by the investigator or sub-investigator.

In addition to demonstrating that the investigator (and sub-investigator involved in trial specific decisions) has appropriate oversight, any access, opening, and reading of any relevant supporting electronic documentation e.g. laboratory results, reports of radiological assessments, pharmacy records, etc.) should be logged by an audit trail.

ICH GCP 4.9.1, 4.9.3, 4.9.5 and chapter 8 addendum, EMA eSource reflection paper 6.3

Mitigation in the absence of a directly electronically documented medical oversight
In case electronic medical oversight cannot be directly demonstrated by the EHR system, processes should be in place like e.g.:

- By adding appropriate notes by the investigator in the electronic progress documentation stating that medical results were reviewed and evaluated. Those entries must be clearly attributable to the investigator or authorised sub-investigator as well as to a date and under circumstances the time the data were collected.

- By means which were applicable at times of paper medical records, e.g. relevant electronic reports/results are printed and verified by the investigator's (or authorised sub-investigator's) dated signature or on study-specific paper source documents.
- Those hard copies belong to the essential documents and, according to ICH GCP and ISO14155 (as applicable), have to be filed in the ISF.
- In general, an audit trail or in its absence e.g. a version history of the documents or a hardcopy change log providing an overview of all changes made should be available to provide a chronological overview demonstrating what was known at all time points when relevant decisions were made for the trial.

ICH GCP[1] 1.63, 8.1 Addendum, EMA eSource reflection paper[5] 6.3.3 and topic 4

2.1.4. Security

a) Password protection

Access controls need to be in place with regard to controlling any access to the EHR system via individual user accounts (i.e. user name and password).
At the institution, a policy has to be in place that all password protected logins are personal and must not be shared. A documented training should be available.

Recommendation
The system should:
- provide an automated logoff after a certain time of inactivity;
- support regular changes of login passwords at defined intervals.

ICH GCP[1] 5.5.3 Addendum, EMA eSource reflection paper[5] topic 3, applicable cantonal data protection laws, Good practices for computerised systems in regulated "GxP" environments[6] 19

b) Backups

The EHR system provides appropriate system control measures for data backup and data recovery to prevent data loss.

Recommendation
The following should be in place:

- a documentation about the data backup, recovery processes, and applied systems;
- a risk-based disaster recovery plan together with emergency procedures in case of data and/or data entry unavailability.

ICH GCP 4.9.4 and chapter 8, EMA eSource reflection paper [5] topic 5, Good practices for computerised systems in regulated "GxP" environments[6] 19, applicable cantonal data protection laws.

c) Access and authorisations
The system allows the allocation of access rights - which are assigned to the appropriate and correct organisational level/function/role of the user - and permits a differentiated panel of authorisations within the system. For further details see section 5.

Mitigation/recommendation in the absence of security measures as described
Paper-based documentation and filing of source data is recommended. In case of retrospective data (including but not limited to data of the medical history), the data should be evaluated and confirmed regarding completeness and accuracy before printing to obtain certified copies (see also section 4).

2.1.5. Access, roles and rights (authorisation)

The EHR system has to provide a differentiated authorisation concept depending on the organisational structure of the institution and system.

Rights (i.e. write, edit, release, read) are attributed to individual roles and allocated to internal staff of the institution, but also to external players (e.g. inspectors, auditors, monitors of clinical trials).
Rights are allocated depending on the role and function but also depending on the organisational unit the person belongs to.

A documentation must be available with the records of users and their authorisations being valid at all times. Any changes in roles and rights shall be recorded e.g. in an access log depending on the job responsibility by the institution.

For monitors, auditors, and inspectors of clinical trials
Monitors, auditors, and inspectors should have access to the health-related data of trial participants as well as to the associated data of the audit trail. This access should be granted under the following prerequisites:

a) Individual password-restricted access to health related data is limited to:
   - study participants who gave appropriate consent;
   - participants of a certain clinical trial for which the monitor, auditor, or inspector has to fulfil his/her regulatory tasks at a given time point;
   - read-only access

   Thus, the access is restricted to trial participants of a specific clinical trial, for which the auditor, monitor, or inspector has the authorisation to view the data only. This means that monitors etc. may NOT have access to health-related data of all clinical trial participants recorded in the EHR system. Access is only allowed for specific trials and where informed consent has been verified.

b) The access has to be limited in time and should expire after the monitoring visit (or audit/inspection).

ICH GCP[1] 2.13, 4.9.7, 5.1.2, 5.15.1, 5.18.5 (k), (m(i)), 6.10, EMA eSource reflection paper[5] topic 3, 4, 5

Mitigation in the absence of restricted access for monitors, auditors and inspectors
In case **no restricted access** (as described above) **for monitors, auditors, and inspectors is possible**, the following alternatives are possible:

- Paper printouts from the electronic source data, analogous to section 2. Attention should be paid that printouts are current, complete, dated on each page with the date of the printing, pages numbered, and signed by the (sub-)investigator with the date of signature. Accompanied (in the presence of site staff) spot cross checks of the paper records against the electronic source data in the EHR system to check for completeness performed by the monitor (or auditor, inspector) should be allowed. Paper copies of the source data have to be filed together with the essential documents in the ISF.
- Accompanied monitoring (source data verification). In the presence of site staff, the monitor (or auditor, inspector) may have direct access to the source data in the EHR system. Site staff warrants that no other patient data is accessed by the monitor. This should only be allowed if an audit trail is in place to record if any changes were made and if it is guaranteed that the audit trail is checked after the monitoring visit.
- Data protection declaration and access control via audit trail.
- Direct access to the EHR system may be allowed in case where the monitor (or auditor, inspector) can be provided with an individual password-protected login with reading rights only.
- Further, a declaration has to be signed to confirm that data insight is limited to trial participants of the monitored trial. In addition, access has to be logged by an audit trail which has to be reviewed and checked after the monitoring visit to confirm that data protection was not violated.

Note: For all alternative measures, appropriate procedures have to be put in place and control measures have to be implemented. Furthermore, the defined and documented approaches have to be accepted by the investigator and the sponsor.

2.1.6. Quality assurance

a) System validation and change control
The EHR system has to be controlled as such that it has to be validated with respect to its purpose, the fulfilment of regulatory and user requirements, and operational testing.
For the entire life cycle of the EHR system, a change management system should be in place with change control procedures documenting the reason, impacts, and release of the changes made to the EHR system.

Recommendation
In case data are transferred from other electronic systems via interfaces to the EHR system, tests should be performed to check for data transfer completeness, correct allocation, and to exclude any alterations during data migration. Appropriate documentation should be in place to ensure that migrated data was not changed. These records should be kept to be provided to the monitor, auditors, and inspectors upon request.

ICH GCP 1.65, 2.13, EMA eSource reflection paper topic 1, Good practices for computerized systems[6] 14, 17, 18

b) Training
All persons working with the EHR system should receive a basic training in the computerised systems of the EHR system and specifically in the tasks assigned to them.
Appropriate documented processes and records for the training how to use end employ the EHR system should be available. Training lies within the responsibility of the health care institution hosting the health-related data by the EHR system.

EMA eSource reflection paper topic 2, Good practices for computerized systems[6] 22

2.1.7. Archiving

There have to be processes and system prerequisites in place to ensure that health related data recorded in the EHR system is adequately archived. This should include the retention of audit trails and associated metadata throughout the legally and per study protocol required archiving period. It is essential that all archived data remain retrievable upon request and readable by human beings.
Suitable archiving systems and processes have to be implemented to protect data integrity from unintended manipulation or deletion.
Regular backups should be made.
Appropriate quality checks should be in place to confirm that archived data (including metadata) are available, complete and readable by humans.

- *ICH GCP 2.10, 4.9.0, 4.9.4, 4.9.5, 5.18.4, 8.1 Addendum, EMA eSource reflection paper topic 5, applicable data protection laws, applicable cantonal health and cantonal patient laws, ClinO art. 18, 35, 35, 45*

Mitigation/recommendation in the absence of suitable archiving measures
It is recommended to ensure that printed certified copies (see also section 4) from the electronic source data can be made at the end of the trial, which can then be archived in accordance to ICH-GCP and the prerequisites made in the study protocol and contractual agreements.

2.1.8. General study administration

a) Flagging of patients participating in a clinical trial

It is recommended that the EHR system allows to allocate patients to a clinical trial or a research project. Amongst others, this facilitates the search and retrieval of records relevant for clinical trials within the EHR system.
In case the EHR system provides only a minimal administration structure for clinical trials (e.g. study title, study number, start, and end date of trial, names of investigator and any relevant contact person, patient identification of trial participants etc.), the following should be considered:
Rights for the individual study administration should be restricted to authorised staff of the study site and protected by individual password login and predefined authorisations (i.e. write, edit, release, read). Access control shall be allocated as defined in section 5 of this guideline.

b) Recording and flagging of patients providing general consent to the further use of health-related data and biological samples (HRO chapter 3)

Any consent-related information should be centrally recorded in the EHR system. This allows to easily identify patients who agreed and patients who refused to provide general consent for the reuse of their health-related data and biological samples for research projects. This central recording is essential in order to prevent any breach of the patient's personal rights.

Mitigation action in case of lacking functional or technical feature

Relevant information has to be recorded on paper and appropriately stored to allow for rapid access, prevent misuse, unintended modification and disclosure to unauthorised personnel.

2.1.9. Scanning and electronic certified copies

In order to file paper records in the EHR system, e.g. written reports from referring institutions, or previous paper-based documentation, certified copies of the original documents have to be made (see also section 4). For this purpose, special validated procedures for paper record scanning, digitalisation, and electronic filing along with risk-based quality checks, should be implemented:

- A written procedure should be available to describe the workflow, responsibilities and quality checks to warrant scan quality, legibility, and completeness.
- Attention should be paid to ensure that the electronic copy is an accurate copy of the paper source (e.g. with regard to scan resolution, colour, font, congruency of information between the paper and the electronic document, especially concerning front and back pages or page margins).
- Further, it has to be guaranteed that the electronic copy is allocated to the correct patient and to the correct file. Bulk pdf files without any order and temporal assignment with respect to date of origin would hamper the reconstruction of study data. Data in the EHR system should be identifiable and searchable by date and keywords.
- Appropriate metadata have to be recorded for the certified copy (as e.g. type of document, format, date and time of scanning and name of person scanning the document).
- In addition, the file format of the electronic copy generated may not allow any modification (e.g. pdf/A).

Recommendation

Strong adherence to a formalised procedure (in terms of a description of the whole process by e.g. a working instruction or SOP) of scanning, uploading and accompanying quality checks is required before any destruction of the original paper records to ensure the certified copy (see

also section 4) as reliable and complete. Where possible, paper records should be retained during the archiving period.
With respect to documents with wet ink signature (e.g. informed consents), the original paper documents should be kept to ensure legal evidential value[8].

ICH GCP[1] 1.6.3, 8.1 Addendum, EMA eSource reflection paper[5] 6.3.3, topic 4, EMA guideline on the content, management, and archiving of the clinical trial master file (paper and/or electronic) section 5.1 and 5.2

3. General recommendations

3.1. For sponsors and sponsor-investigators

It is highly recommended for sponsors and sponsor-investigators to make an evaluation of the data integrity prior to the conduct of a study at each of their study sites.

For this purpose, they can use the EHR System Study Site Assessment Template that we provide on the SCTO Platforms website and issue the evaluation form to their study sites for completion.

3.2. For study sites

In order to answer to questions regarding the EHR system assessment for the evaluation by the sponsor/sponsor-investigator or in case of audits and inspections the following recommendations are made:

3.2.1. Contact person at the IT department for technical and functional questions

It is highly recommended to have a central contact person at the IT department:

- to contact in case of any audit and inspection;
- to address questions from sponsors and regulatory authorities (e.g. Swissmedic) regarding structure and organisation as well as technical and functional requirements of the EHR system either at site selection, site initiation or at audits or inspections;
- to request e.g. an export of an audit trail, or directory of users and authorisations or any other documentation for monitoring, audit or inspection purposes;
- to request information regarding the validation, maintenance and change control of the system.

3.2.2. Documentation and records

A detailed documentation of the EHR system organisation (e.g. connection to other systems), structure, maintenance, and quality assurance is required by the institution to comply with *Good practices for computerized systems in regulated "GxP"[6] environments*.

Examples of documentation to be maintained and made available in case of an audit or an inspection:

- details about the organisation and structure of the EHR system, including interaction with other (sub-)systems and modules, data flows;
- tasks outsourced to third parties;
- list of hardware and software, associated systems and modules, etc.

- procedures (SOPs or any other documentation) should be in place, which cover all processes to ensure data reliability and integrity (life cycle management, change control, validation, training, access control, etc.);
- validation plans, protocols and reports;
- records of the EHR system's life cycle management, change management, and validation;
- statement on qualifications of staff engaged in the EHR system maintenance;
- user handbooks.

ICH GCP[1] 2.11, EMA eSource reflection paper [5] topic 3, ClinO [3] art. 18, applicable cantonal data protection laws and applicable cantonal patient laws

4. Certified copies

According to ICH GCP E6 R(2), certified copies are defined as "a copy (paper or electronic) of original information that has been verified, as indicated by a dated signature, as an exact copy, having all of the same attributes and information as the original".

The original information may be electronic data or paper documents.

EMA is a little bit more precise and says, a certified copy is either a paper or an electronic copy that has been verified (e.g. by a dated signature) and generated through a validated process to produce an exact copy having all the same information, including data that describe the context, content and structure, as the original.[8]

The Food and Drug Administration (FDA) defines a certified copy as a "copy of original information that has been verified, as indicated by a dated signature, as an exact copy having all of the same attributes and information as the original." [9]

As an example, if a medical report is using a colour code system, the certified copy thereof should exactly display the colours and the attributed information of the original.

How to implement a validated process and what does it entail?
There are no concrete regulatory provisions thereof. ICH-GCP does not provide any information nor do the Swiss legislation (HRA and its ordinances) and Swissmedic.
According to EMA (independent of the original information (whether paper or electronic), **risk-based QC checks of certified copies**, should be made regarding the completeness, correctness, legibility, any correct allocation of information in order to ensure that no information is lost or altered and thus the copy is an exact copy of the original.
Finally, the verification is confirmed by dated signature either in written in case of paper certified copies or in case of electronic certified copies by dated electronic signatures or stamps (date and user ID).
In case of digitisation, a validated system (e.g. scanner) should be used, which means that the system was tested if it worked as supposed to do and testing has been documented along with the test results.

It is self-evident that there is a broad range of quality checks and validation measures depending on the purpose and the source and system used.

So, for monitoring purposes, regarding the printouts of the electronic health record system covering a certain time span, it may be sufficient to check if the printouts are accurate and complete.
From the printout it shall become obvious when and by whom the different health records were made. The printed pages should be dated (date of printing), and numbered and signed off by the investigator or sub-investigator.

For digitisation purposes of medical records, when the electronic copy is irreversibly replacing the original, stricter quality checks and validation measures become necessary, which should be documented and defined accordingly.
The system used for scanning and data storage has to be validated.
With regard to quality checks, attention should be paid to ensure that the electronic copy is an accurate copy of the paper source e.g. with regard to scan resolution, colour, font, congruency of information between the paper and the electronic document, especially concerning front and back pages or page margins.
Special attention should be paid regarding the data format of the electronic copy which should be static (e.g. pdf scan) and allows long-term archiving, but which does not allow any changes of the content.
In addition, it has to be guaranteed that the electronic document is assigned to the right patient, the right examination and may be retrieved easily upon request. Further, it has to be guaranteed that the copy itself is protected from any alteration or deletion.

It is recommended that written processes/SOPs are available and site staff should be trained appropriately.

ICH GCP R6 (2) 1.63, EMA guideline on the content, management, and archiving of the clinical trial master file (paper and/or electronic) section 5.1, FDA Guidance for Industry on Computerized Systems Used in Clinical Investigations

5. References

1. E6(R2), Good Clinical Practice. In: Harmonization ICo, editor. https://www.ich.org/page/efficacy-guidelines; 2016.
2. Federal Act on Research involving Human Beings (Human Research Act, HRA). In: Confederation TFAotS, editor. https://www.admin.ch/opc/en/classified-compilation/20061313/index.html; 2011.
3. Ordinance on Clinical Trials in Human Research, ClinO. In: Council SF, editor. 20 September 2013 ed; 20 September 2013 (Status as of 24 April 2018).
4. Ordinance on Clinical Trials with Medical Devices (ClinO-MD). In: Council SF, editor.; 2020.
5. Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials. EMA: European Medicines Agency; 2010.
6. Good practices for computerized systems in regulated "GxP" environments. 2007.
7. Sandra Unfer MP, Elke Hiendlmeyer. Electronic health record systems at Swiss clinical trials sites: Usage, experience and needs. 2020.
8. Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic). In: Agency EM, editor. EMA; 2018.
9. Services USDoHaH, (FDA) FaDA. Guidance for Industry Computerized Systems Used in Clinical Investigations 2007.

6. Reading recommendations

GCP requirements

- https://mhrainspectorate.blog.gov.uk/2019/07/23/electronic-health-records/
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470228/Electronic_Health_Records_MHRA_Position_Statement.pdf
- https://www.fda.gov/regulatory-information/search-fda-guidance-documents/use-electronic-health-record-data-clinical-investigations-guidance-industry
- GCP-compliant digital archiving of paper-based patient records of clinical trial subjects: a key issues paper (2013)
- TMF Reference Model: Guidance for the management of e-mail communications in clinical studies (31.07.2020)

Electronic signature, validation and beyond

- https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application
- https://ispe.org/publications/guidance-documents