One way I keep myself up to date with developments within laboratories and related areas is by reviewing draft standards.  This keeps me appraised of the current state of affairs, keeps my documentation audit skills fresh and potentially allows me to contribute to the content of standards.  For this draft standard, I have some knowledge of IT and IT security so am able to critically review the draft standard and offer comment.

Notes: refer to the conditions for comment stated towards the beginning of the draft standard.

**DR AS 2828.2 Health records, Part 2: Digitized health records**

Here I step through the draft standard making comments.  Where a comment is answered later in the standard, I go back to my original comment and make notes.  An uncommented comment is potentially worthy of becoming an official comment on the standard.

I decided to review this draft standard as I currently work with IT security software and have an idea of the needs for secure electronic documentation.

**Preface**

The standard appears to specifically apply to the digitization of health records, not to the creation of “raw data” aka Electronic Heath Records (EHR).  Here the standard is called AS 2828.2 Health records, Part 2: Digitized (scanned) health records.  Whatever the name, it needs to be stated consistently.

This is a “new” AS based on AS 2828.2 (int) 2012. Int informs the reader of the interim nature of the standard. An interim standard is used for a period of time before review and submission for consideration for issuing as a formal Australian Standard.

**Scope**

Specifies the requirements for digitization, storage, security, conformance and reproducibility of scanned record(s).  Specifies the requirements when scanned records accessed from within context of EHR.

**Section 1 Scope and General**

**1.3 Terms and definitions**

**1.3.2 born digital**

This is also known as raw (or original) data (at least in laboratory circles).

**1.3.11 electronic health record (EHR)**

Note that this is a record that computer calculations can be performed on.  Photos of paper records will not be able to manipulated without text conversion or complex image analysing software.

**1.3.21 individual healthcare identifier (IHI)**

Is this Medicare number?  Perhaps clarify this.  It could be a number assigned by a clinic, a hospital or someone else.

**1.3.28 personal health record (PHR)**

States this is controlled by the person.  This should ultimately be the same as an EHR and all access to such records should only be allowed when authorised by the person.  Ideally there would be a central repository for such data (eg the MyHealth record).  In other words, the person, not the doctor or organisation should own their data, regardless of who captured it, controls it or where it is stored.  I acknowledge that could get tricky unless the storage and security is overseen by the Government.

Perhaps provision should be given to a person being able to request their full EHR from any organisation and perhaps they should be able to request the record’s deletion from locals storage once transferred to the person.

**Section 2 Digitization of health records**

No comments.

**Section 3 Processes for digitization of health records**

No comments.

**3.1.2 Metadata and value domains**

About the only transactional  meta data that could be captured here is scan date and scannee (or when using a camera, camera settings and time stamp).  I am not sure as to the value of such data.  This is covered in 3.3 Design of paper health records, documents and forms which details OCR readable identifiers so patient details and test specifics can be automatically added to the file upon scanning.

**3.2 Clinical relevance**

“[b] Documents captured in a digitized health record shall – (iii) be subjected to quality control checkes…to reduce likelihood of errors or omissions arising from digitisation…”

Here the scanned document should be visually compared to the original and signed off (once meta data is confirmed as correct) indicating a full and complete transfer.  The scanned document, including meta data should be then be hashed.  This will reveal any change to the document following initial conversion and approval.  Any changes should be captured by an audit trail (and for scanned images, unless there is an error in the meta data, I do not see why changes would be required).  3.4 Support for legal obligations (c) states the captured record cannot be altered, though does not details how that can be determined. 3.5 Quality Processes (e) NOTE addresses visual inspection and more.  4.4.2.1 Required metadata functionality describes capturing device meta data

“[d] [iv] minimise the need for clinical personal to re-enter data that already exists in other clinical and administrative systems.”

How would clinical personnel know what has and has not be scanned into an existing system?  Shouldn’t 3.1.1 General and 3.1.3 Planning for implementation cover this?

**3.3 Design of paper health records, documents and forms**

Very good.

**3.4 Support for legal obligations**

(c) States the record cannot be altered

(d) States alterations need to be authorised and captured with an audit trail.  Which is it?  (c) or (d)?

(f) Which states the original data should be maintained until QA checks on the scanned document are complete. This should be a standard QA practice regardless of legal obligations.

(h) Audit trails for records access – very good.

(i) Privacy consents from patient to be recorded.  Here perhaps have an expiry period for consent.

(j) Mentions up to date privacy consents, so perhaps this includes an expiry period.

**3.5 Quality Processes**

I agree with everything here with the exception of 3.5.4 Key performance indicators as such stats should have been captured during operational and performance qualification of the capturing system.  KPIs are only of use to determine how much money is spent/lost reprocessing failed scans.  Periodic system revalidation would/should capture performance metrics and such data should be compared to initial system qualification.

**3.6 Cybersecurity and access control**

Suggested: Add “(c) safeguard of data from malicious actors and unauthorised access.”  Add malicious actor definition to relevant section of standard.

**3.6.2 Unique access credentials**

Only single factor authentication is required.  Given the sensitive nature of the DHR, at a minimum, 2 factor authorisation should be mandated.  Ideally, multi factor authentication would be mandated.

**3.7 Retention and Disposal**

Suggested: “(d) Digital records should be backed up across at least two physically distinct locations and employ some form of error checking to ensure the data remains consistent across the sites.  Backups should be incremental and for a sufficient time period so data recovery in the event of a disaster can be accomplished.”

The above statement would be just at home in 3.8 Maintenance and operation of a digitizing health record system.

**3.8 Maintenance and operation of a digitizing health record system**

Suggested: “If for any reason, it is envisioned decommissioned (scanning) equipment might be needed during the DHR’s legal retention period, said equipment should be retained”.

**Section 4 Digitizing health record system (DHRS)**

**4.1 Key characteristics**

(a) states to capture at highest resolution of capturing device.  (b) states a loss of resolution is allowed (if permitted or required).  Which is it?

(e) (ii) states DHR cannot contain embedded objects.  This precludes the use of PDF files or other documents containing text and images or clickable hyperlinks.

**4.3 Image processing**

**4.3.1 Required image processing functions**

(f) (ii) and (h) States there should be an ability to crop and scale images.  Cropping and scaling images effectively reduces the resolution and thus is lossy.  This is NOT recommended.

**4.3.2 Desirable image processing functions**

States that poor contrast, high contrast etc images can be post processed to improve the look.  This technically means the original data has been altered.

Suggestion: “All image manipulations including post processing during conversion an original document into a DHR mist be logged as part of the document’s audit trail.

4.4.2.1 Required metadata functionality (c) mentions the capture, acceptance and processing of image-level metadata so that might be sufficient.

4..7 Storage of digitized health records

**4.7.1 General**

“Digitized …records…shall be” (a) Maintained on media which is stored securely in formats that are readily readable and periodically refreshed to ensure that they remain current.”

What is classed as secure?  Encrypted?  Physically inaccessible (I assume password protected for LAN or WAN access).  What does refresh mean?  Hardware replacement?  Format update?

(b) implies secure facilities.

(d) Reference to backup and disaster recovery plans = very good.

Also a note that backups needs to be tested to ensure they work as intended.  Very good.  Expanded in 4.7.3 (d)(iii).

**4.7.2 Requirements for storage of digitized health records**

(b) Keep the primary copy and any secondary or backup copies…on devices physically located within Australia.

Ideally the company providing backup services should also be Australian owned and operated.  Why?  No conflict of interest related to foreign powers (not that that is really an issue, but I cannot say what foreign intelligence agencies or powers will be able to do with such data with or without the aid of advancements in medical technology).  It will also generate Australian jobs.

**4.7.3 Desirable measures for storage of digitized health records**

Question?  Lossless encryption?  Lossless applies to compression, not encryption.

Suggestion: remove section (a).

“(d)(vi) Apply timely updates to operating systems, application software, and network operating systems, devices and firmware.”.

Suggestion: Add the following, “Any update should first be tested before being applied to a live system.”  This reduces the risk of a loss of data integrity or the introduction of undocumented security holes.

**4.8 Reproduction of digitized health records**

Comment: How is the dissemination of reproduced records to be managed?  Should a password be required to access digitally reproduced records?  What steps should be in place to ensure physical copies of reproduced digital records remain private or unseen by unauthorised persons?  Will the viewing of reproductions (digital or physical)  be logged, and if so, how will this be added to the EHR’s audit log?.   Section (c) requires the logging of printing or other reproduction.  Should a metadata point be included in the EHR to log the destruction of the duplicated digital record?