Australian Government

Department of Health

Online Validator user guide

Version 1.00

As at 29 October, 2025

Getting help

A dedicated **Help Desk** is available for technical user support in relation to the use of the Online Validator. All technical enquiries should be directed to: support@validator.com.au

Table of Contents

1. Introduction

1.1. Overview

The Online Validator is an extensible, web-based application for determining the validity of large data sets. It ensures that large data sets passed between *Submitters* and *Reviewers* are valid and consistent, according to a set of rules. These rules ensure that data is

1. Formatted correctly, as per a specification;
2. Internally consistent (that is, the data appears to be logical and coherent).

The value of the Online Validator is that very large data sets – such as health records – can be efficiently and effectively examined for validity prior to acceptance.

This reduces errors, lowers costs, and improves the accuracy and effectiveness of subsequent reporting and decision making.

The Online Validator is developed and operated by Logicly Pty Ltd under contract to the Department of Health, Disability and Ageing, in support of data sets sponsored by the Department. Its current users include the Australian Institute of Health and Welfare (AIHW) and the Australian Mental Health Outcomes and Classification Network (AMHOCN).

1.2. Purpose of this document

This document covers general information about the application and the end-to-end process.

This project is evolving, and changes to the application are implemented periodically. As such, this is intended to be a working document, and will be updated according to subsequent releases.

2. Overview of submission process

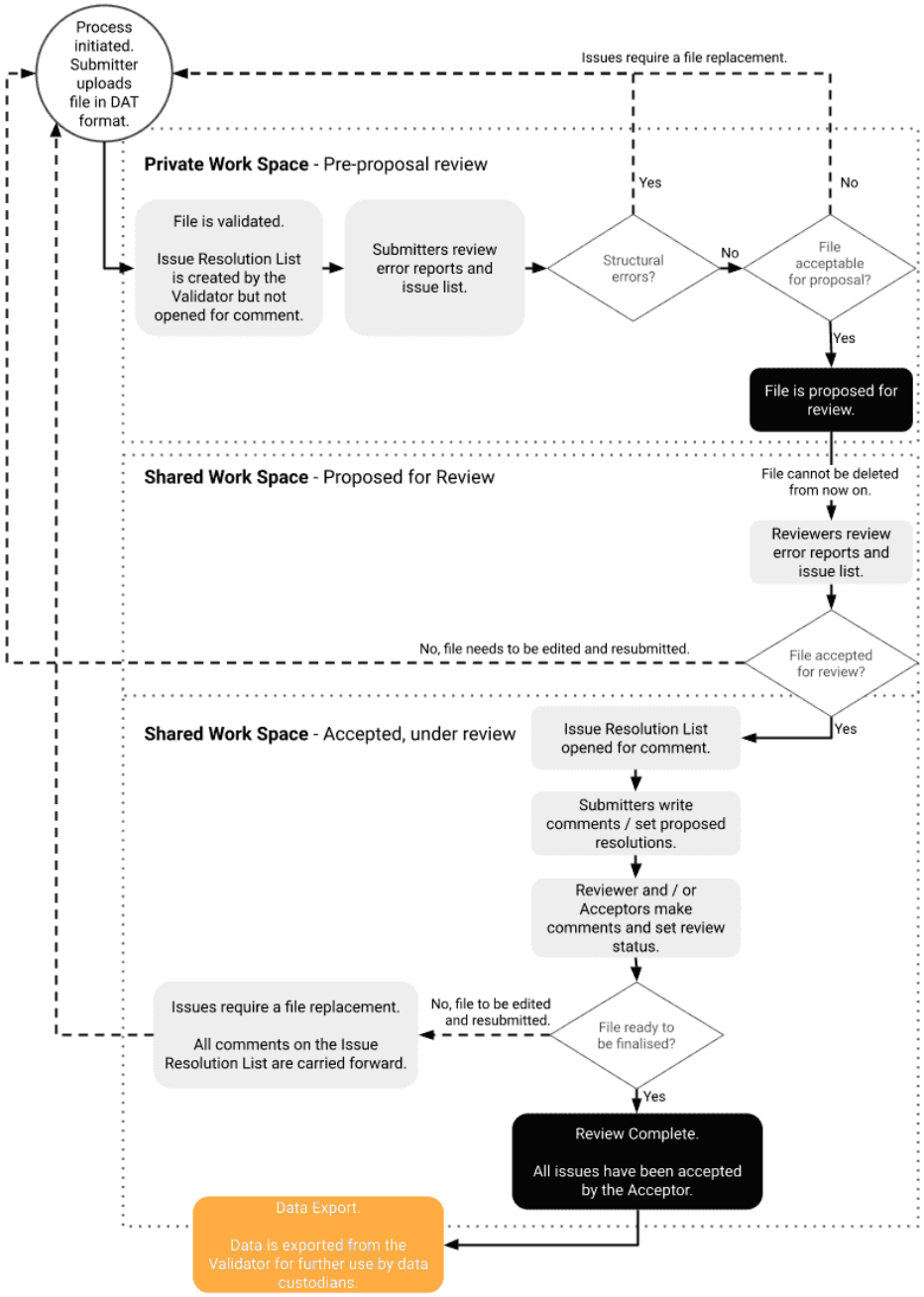


Fig. 2.1 *Overview of the Validator Submission Process*

2.1. Summary of workflow

See Fig. 2.1 for a more detailed overview of the submission process summarised below:

1. Submitter uploads **in** private workspace **for pre-submission validation checks**

Pre-submission checks, such as structural and consistency validations, allow Submitters to easily identify and correct data anomalies before submitting the data for assessment by Reviewers. Structural validations ensure the data is structured correctly and satisfies its specification, while consistency validations ensure the data is reasonable and consistent, including comparison to data submitted in previous reporting periods.

The validator can be configured to prevent a file being proposed for review based on the existence of any type of issue. Typically files with structural issues cannot be submitted, however in some cases exceptions may exist to allow for incorrect data to be supplied where the impact is low and it is unlikely that a Submitter could correct the data. For example, diagnosis codes that don't match the officially accepted ICD code list do not prevent a file from being proposed.

2. Submitter proposes file for review **in a shared workspace**

Submitters 'propose' files for acceptance by Reviewers. Once proposed, Reviewers can assess the quality of the datafile via the consistency validations and a series of issue and rule reports.

3. Reviewer accepts **or** rejects **the file**

Reviewers can either accept the file for further review, or reject it if they believe the remaining issues need to be rectified before the file is reviewed in full. In this situation, Submitters prepare and upload a new file in their private workspace (Step 1).

4. Reviewer and submitter collaborate on data

The Online Validator provides a collaborative platform for reviewers to work with Submitters to ensure that data meets the standards required by the Reviewer. Issues are tracked and discussions between Submitters and Reviewers are retained.

This process may result in a shared decision to resupply the data; again, Submitters prepare and upload a new file in their private workspace (Step 1).

5. Reviewer finalises submission

Once the Reviewer is satisfied that the submission is adequate, the submission process is considered complete. The data is now considered to be suitable for reporting and can be manually or automatically transferred to an external data warehouse or reporting system.

2.2. Private v Shared workspace

When first uploaded, files remain in the Submitter's private workspace. This allows Submitters to review their potential submissions before choosing to formally propose the file for review. Submitters may share the file with other users if they wish.

Once a file has been proposed for review, it is automatically viewable by other users **who have been given access to that data set**. This 'sharing' of the file is not user customisable. Additionally, the other users with identical access privileges will have the identical file rights, e.g. other users with submit privileges can leave comments, delete the file and submit for review.

3. Access and authentication

3.1. Logging in

Login: https://validator.net.au/

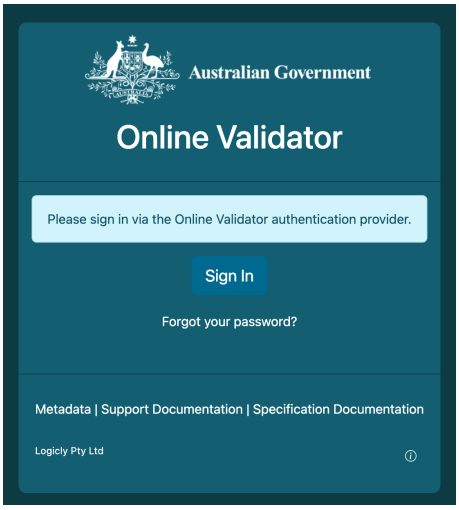


Fig. 3.1 *Sign in screen*

3.2. Requesting and managing access to the Online Validator

Logicly's application authentication procedure is designed to align with the Australian Signals Directorate's Protective Security Policy Framework (https://www.protectivesecurity.gov.au/) at OFFICIAL:Sensitive level and requires Multi-Factor Authentication to register and log-in to the application.

In order for Logicly to register you for an account, Logicly requires your work email address. Your email address will be used as your login identifier and to communicate with you regarding important events associated with the application such as updates and scheduled outages.

Once you have been registered, you will need to set-up Multi-Factor Authentication in order to use the Online Validator. We have a user guide to help step you through different set-up options: https://docs.logicly.com.au/en/latest/mfa-user-guide/index.html.

We take data security very seriously. For more information about Logicly's approach to security, please visit https://www.logicly.com.au/about/oursecurity/.

3.2.1. Registering for user access

1. The new user's manager will need to email support@validator.com.au requesting that the new user be registered for an account and confirming which datasets the new user should have access to. If you are unsure who your manager is, please contact support@validator.com.au.
2. If not already provided, Logicly will request an email address associated with an appropriate Australian jurisdiction (i.e. one of the Australian States or Territories or the Australian Government) for the new user.
3. An email containing a link to verify the account will be sent to the new user.
4. The new user will need to follow the instructions in the verification email to begin their registration (please be aware that the access link is only viable for a short period of time). After registration new users will have access to our Authentication System, but they will not have any functional attributes.
5. The administrators will be notified that the new user has registered and will grant them the correct attributes to access, upload or review the correct file types. A confirmation email will be sent to new the user informing them that they now have access to the Online Validator.

3.2.2. Managing user details

All users may update their personal details via the ***Manage Details*** tab in the Menu Bar via https://auth.logicly.com.au/.

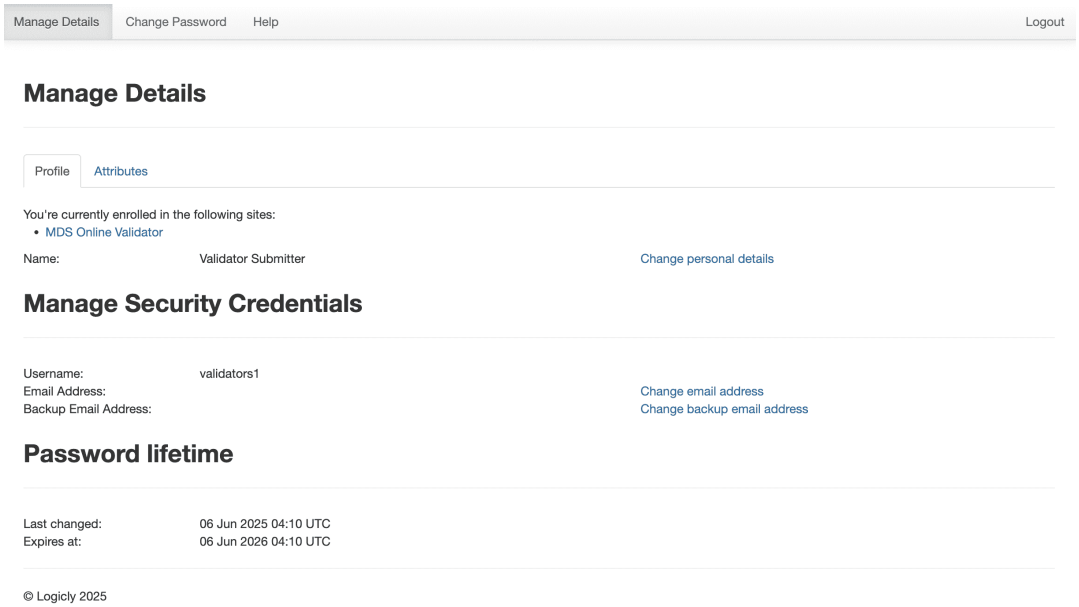


Fig. 3.2 *Account Details Management page*

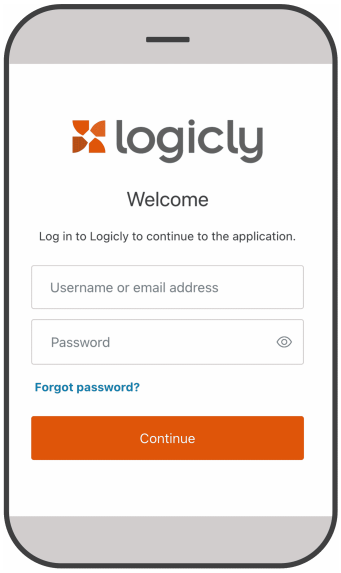
3.2.3. Removing a user's access

Please contact an Administrator via support@validator.com.au to request that user access be removed from the application.

3.3. Authentication

Role-based access is managed by Logicly's existing Authentication and Authorisation Service (Streuth). Streuth manages the roles a user has, and restricts access accordingly. It also provides for self service user details maintenance, password changing and enforces password complexity and password expiration.

Logicly's authentication system now supports Multi Factor Authentication (MFA).



MFA is an additional layer of authentication that works by requiring users to provide verification information (via a device they have) in addition to their email address/password (which they know) when logging in. Taken together these multiple "factors" are used to verify the user. Logicly's authentication system supports a variety of additional factors, including:

- Push notifications
- One-time passwords
- Security Keys

MFA is required each time a user logs into a Logicly application for enrolled users.
While there are a variety of MFA apps compatible with our system, instructions are available to guide you through setting up MFA push notifications on your mobile device using either the *Auth0 Guardian* app OR *Microsoft Authenticator*, as these can be responded to on a mobile device without having to enter a code manually.

For those that would prefer to not use an application on their mobile device, hardware security keys such as the yubico Security Key may be used as an additional factor.

3.4. Roles

Online Validator supports five levels of access. They are Submitter, Reviewer, Acceptor, Exporter and Administrator.

3.4.1. Submitters

Submitters are usually based in the jurisdiction. Submitters can:

- Upload and review potential submissions
- Share files with users in their jurisdiction, who have access to the dataset
- View file contents and check validation issues
- View resolution codes and comments assigned to individual issues
- **If the Submitter has control, they can also:** assign issue resolution codes and / or comments to individual issues;
    - assign control of the issue resolution log to the Reviewer; and
    - propose a replacement for the file under review.

3.4.2. Reviewers

Reviewers, Acceptors and Exporters are usually based in the Commonwealth. Reviewers can:

- View file contents and check for validation issues
- View resolution codes and comments assigned to individual issues
- Record comments against individual issues
- **If the Reviewer has control, they can also:** attribute the ***Accept*** or ***Reject*** status to individual issues; and
    - assign control of the issue resolution log to the Submitter.

3.4.3. Acceptors

Acceptors can:

- View file contents and check for validation issues
- View resolution codes and comments assigned to individual issues
- Record comments against individual issues
- Attribute the ***Accept*** or ***Reject*** status to individual issues
- Assign control of the issue resolution log to the Submitter
- Accept the file

3.4.4. Exporters

An Exporter is able to export files; the role is usually given to Reviewers or Acceptors.

3.4.5. Administrators

Administrators manage the application on behalf of the Department of Health.

4. Submitter workflow

4.1. Submitter dashboard

The ***Submitter Dashboard*** provides access to files that the Submitter has recently worked on, or that have upcoming deadlines for action, along with a summary of their status.

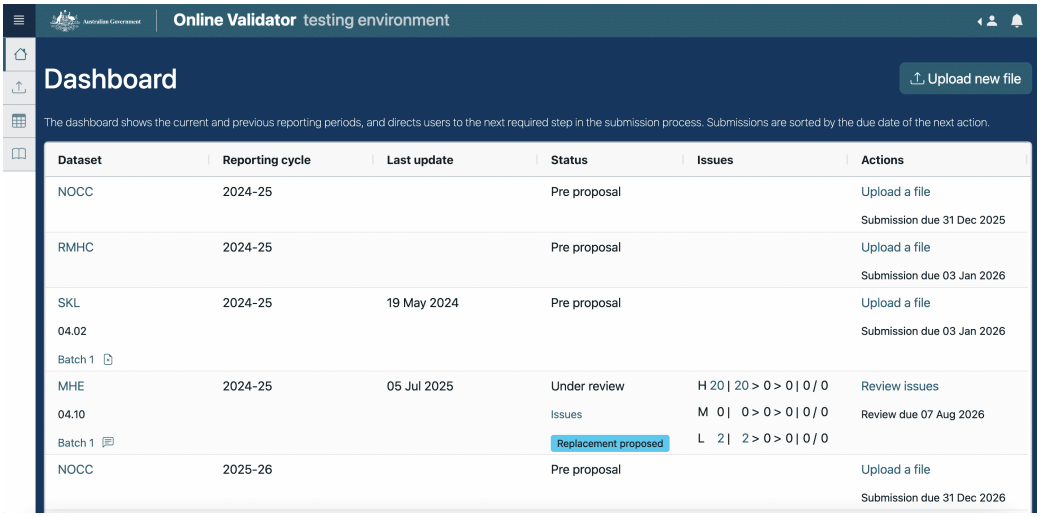


Fig. 4.1 *Submitter Dashboard*

4.2. Uploading files

Files must adhere to the correct format and file naming convention to be successfully uploaded.

Files are automatically checked for record integrity validation and consistency validations as they are uploaded.

After the file is uploaded and the validation process is complete, an email is sent to the Submitter informing them of the file's status and providing a link to the online validation reports.

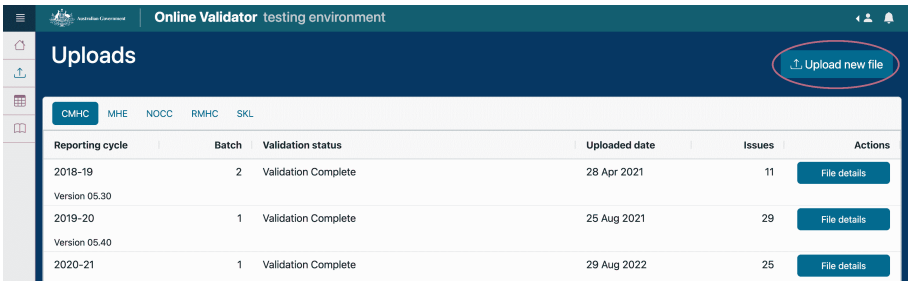


Fig. 4.2 *Uploads page*

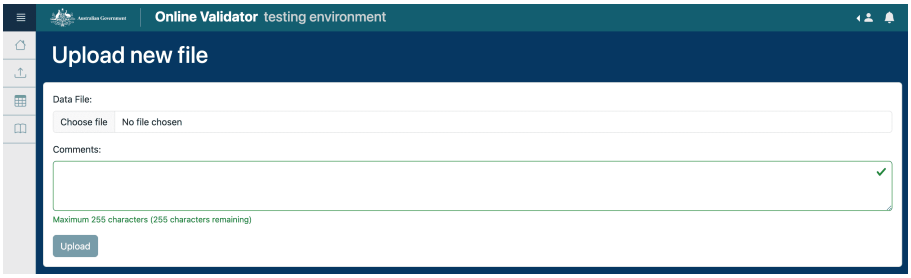


Fig. 4.3 *Upload a new file page*

4.2.1. File format

Files are uploaded in .DAT format. Files can also be uploaded in .ZIP format, however these files can not be password protected. The upload link is encrypted, protecting information in the file throughout the submission process.

4.2.2. Data file naming convention

The data file must have a formal name consistent with the format of Tsssyyyybbbbb.DAT. Note that the filename is case sensitive. The *T*, *sss*, *yyyy*, and *bbbbb* components are defined as:

`T` - File type (CMHC, MHE, NOCC, RMHC, or SKL)

`sss` - Jurisdiction code (ACT, NSW, NTE, QLD, SAU, TAS, VIC, or WAU)

`yyyy` - Year of the end of the financial year for the batch submission

`bbbbb` - Yearly incremental batch number (leading zeros present) indicating the sequence number of the submission. Note that successive quarterly files and any resubmitted files must have a batch number greater than all preceding files for that year.

Example

Suppose that the ACT submitted quarterly data files to AMHOCN in respect of the 2020-21 financial year, then submitted a final submission; their first NOCC data file would be named `NOCCACT2021000001.DAT`, whilst the second would be named `NOCCACT202100002.DAT`, and so on. If no resubmissions were made the final submission for that year would be named `NOCCACT202100005.DAT`. If that file then had to be resubmitted for some reason, then it would be named `NOCCACT202100006.DAT`. Their first submission for the 2021-22 financial year would then be named `NOCCACT202200001.DAT`.

4.3. Pre-proposal review

Submitters can access detailed reports on the validity of their submissions before proposing the files for review.

During this stage, Submitters can:

- View file contents and check validation status
- Review record integrity validation issues
- Review consistency validation issues
- Review issues reports
- Share files if desired
- View, but not use, Entity Mapping Tool (SKL files only)
- Propose a file for review

The Online Validator provides two types of validation: record integrity validation and consistency validation. Record integrity validation issues may prevent a file from being proposed; please see Record integrity report for more information.

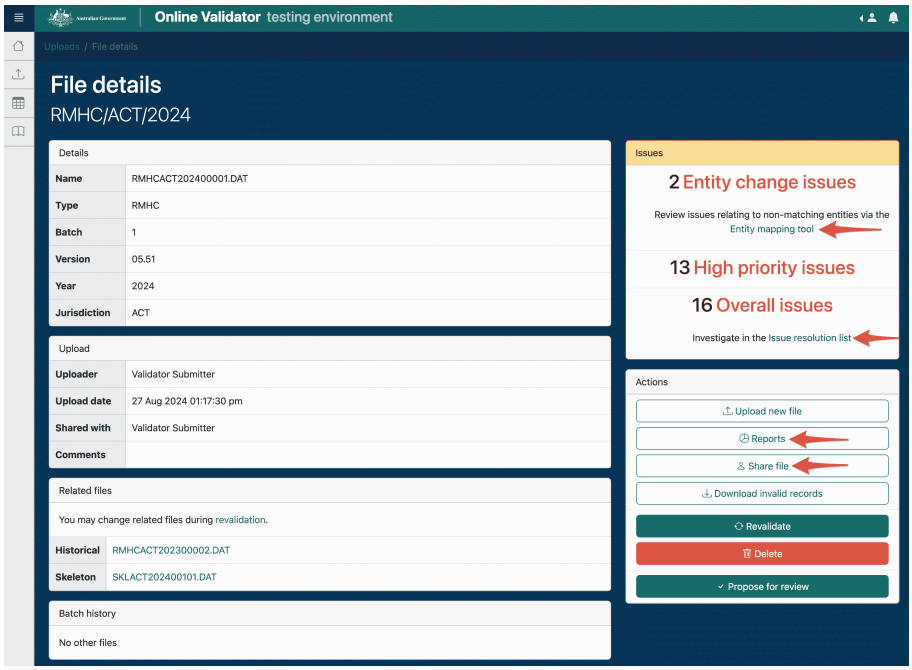


Fig. 4.4 *File details page; pre-submission*

4.3.1. File cannot be proposed for review?

If Structural errors are present, the Submitter must replace the file with a corrected version. Structural validations ensure:

- that records have the correct number of fields, as well as valid data within those fields.
- that records specify valid hierarchical entities. For example, an organisation with a region specifies a valid corresponding region record.
- that organisations have valid identifiers.

The Record Integrity Summary Table and Line Status report indicates if there are ***Malformed***, ***Barren***, ***Duplicate***, ***Orphaned*** or ***Miscoded*** error types.

4.3.2. File cannot be deleted?

The most common reasons you will be unable to delete a file are:

- File has already been deleted (refresh your page to ensure you are seeing the most recent information)
- File is still validating
- File has already been proposed for review (you will need to follow the instructions in propose a replacement file instead)
- File has been proposed as a replacement (will need to wait on file to be accepted or reject for review)
- Filename has been used as part of a submission at any time

4.3.3. Sharing

A Submitter may choose to share access to an uploaded file, that they own, with other users at any time. Recipients of shared files must be registered in the system, and be either from the Submitter's jurisdiction or from the Commonwealth (DoH or AIHW). Sharing options are accessed via the ***File Details*** page.

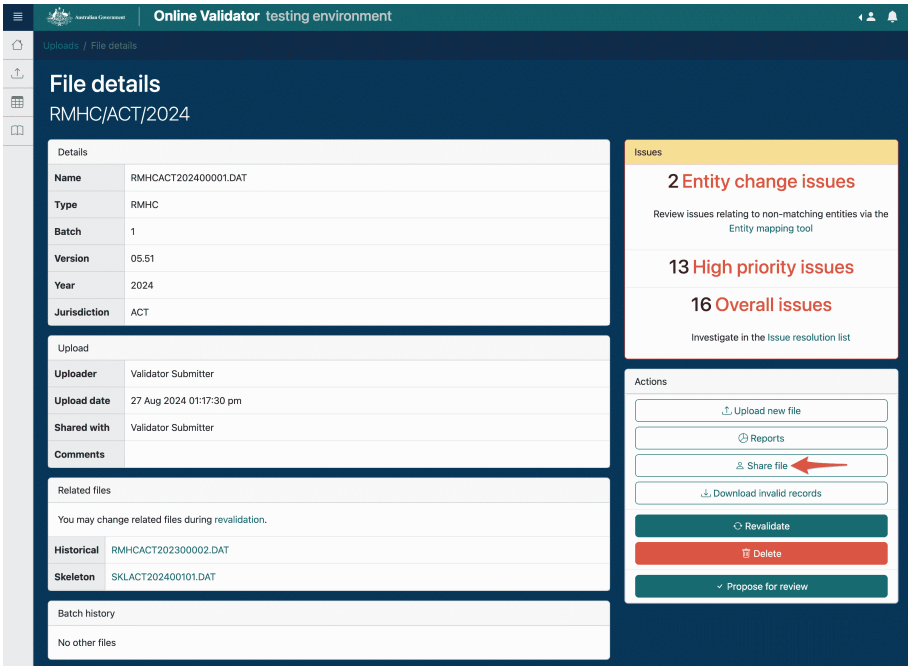


Fig. 4.5 *File details page; share*

4.3.4. Post-validation

At this stage, the Submitter can either:

- leave the upload in the private workspace (which may contain multiple files);
- delete the upload, completely removing it from the system; or
- propose the file for review.

When a file is proposed for review, the relevant Acceptors and Reviewers are notified, and the file cannot be deleted.

4.4. Proposing a file for review

The proposal of files for review is analogous to posting a physical file; it is a formal activity that can only be undone with assistance from the intended recipient.

After a file is proposed for review, it can automatically be viewed by other jurisdictional users with access to the same dataset. Users with identical access privileges as the file's Submitter can comment, delete and propose new files for review.

Reviewers are notified of file submissions via email. Reviewers will then undertake a 'pre-acceptance review'.

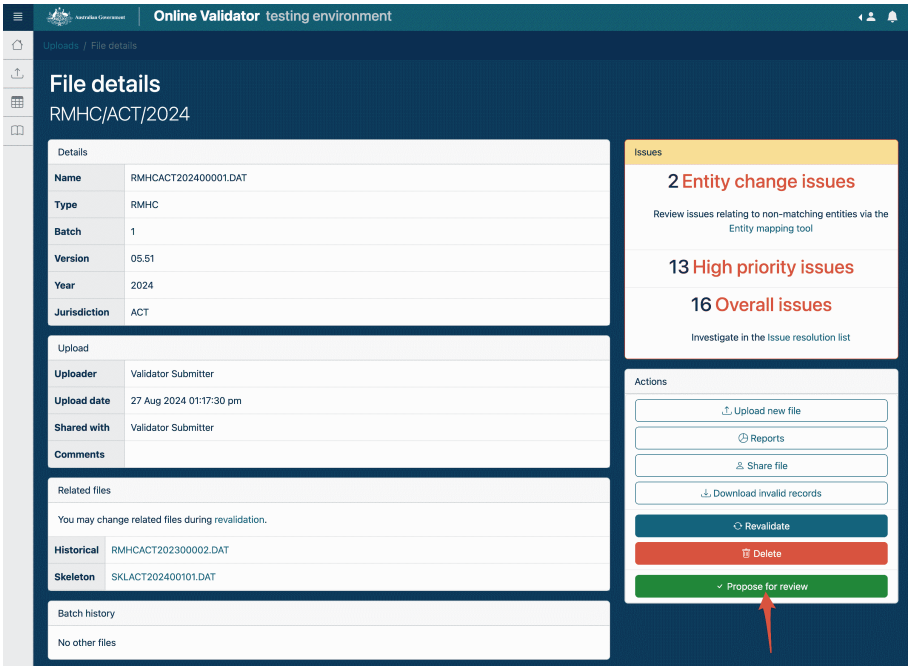


Fig. 4.6 *File details page*

4.5. Pre-acceptance checks by Reviewer/Acceptor

Once a file is proposed for review, Reviewers and Acceptors conduct pre-acceptance checks. These checks aim to ensure the supplied information doesn't contain obvious and significant errors that necessitate a re-submission of the file. Examples of these errors include:

- Incorrect number of variables
- Mismatch between data and variable types
- Incorrect formatting of date fields
- Incomplete information
- Duplication of key fields
- Missing link(s) to parent records

During this phase, the Submitter can:

- View file contents and check validation issues;
- View resolution codes previously assigned to individual issues.

Files with the status of ***Proposed for Review*** are effectively in control of the Reviewer(s), and can not be un-proposed by the Submitter. If the Submitter needs to replace the file, they must contact the Reviewer(s), advising them to cease work on the file, and request that the Reviewer rejects the file.

4.6. Accepted for review

If the file is accepted, submitters are notified via email. Control over issue resolution coding transfers to the Submitter, and the Review process is started.

4.7. Rejected for review

When a file is rejected by the Acceptor the Submitter will be notified and must follow the steps outlined in this document to upload a replacement file.

If a file is rejected, control reverts to the Submitter, who is notified that a new file upload is required. Rejection of a file recommences the submission process. Submitters are unable to upload a file that has previously been proposed for review.

4.8. Replacing a file

Submitters may propose a replacement for a file that was previously proposed for review and either accepted or rejected, if it becomes apparent that updated information should be supplied.

When a replacement submission is accepted, all matching issue resolution statuses and comments are copied to the new submission, preserving the information pertaining to each generation of files.

If a replacement submission is rejected, the proposal review process will revert back to the file with the highest batch number that has already been accepted.

The replacement file must meet the following criteria:

- Successfully uploaded and validated
- Batch number must be higher than the current proposed file
- No other file can be pending as a replacement. If you have already proposed a file, you will need to have it accepted or rejected before you can propose another.

- Step 1 - Successfully upload and validate your replacement file
- Step 2 - On the replacement File Details page click *Propose for Review*
- Step 3 - Reviewers have now been notified of the proposed replacement file

---

Step 1 - Successfully upload and validate your replacement file

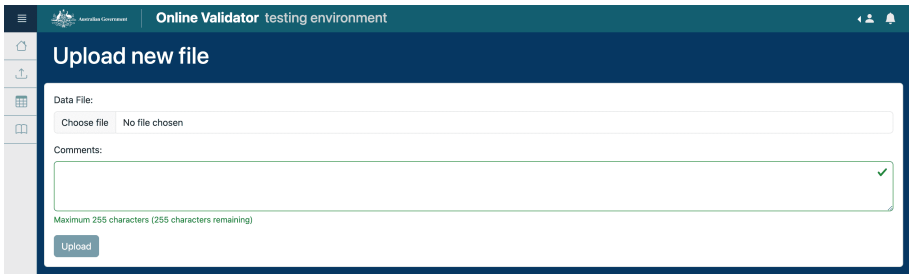


Fig. 4.7 *Submission Workspace - Upload Files*

Step 2 - On the replacement files *Details* page click *Propose for review* button

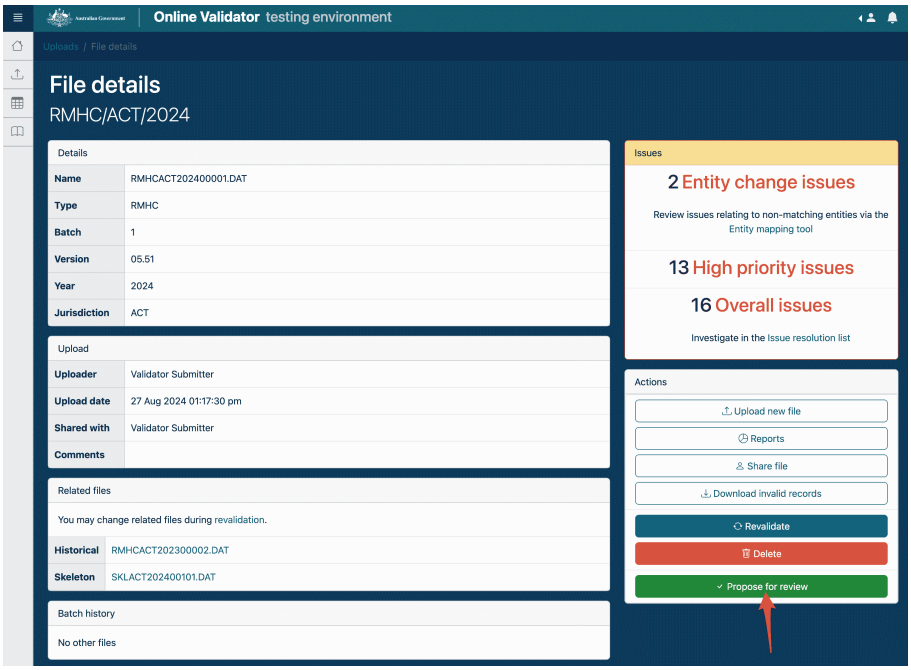


Fig. 4.8 *Submission Workspace - File Details*

Step 3 - Reviewers have now been notified of the proposed replacement file.

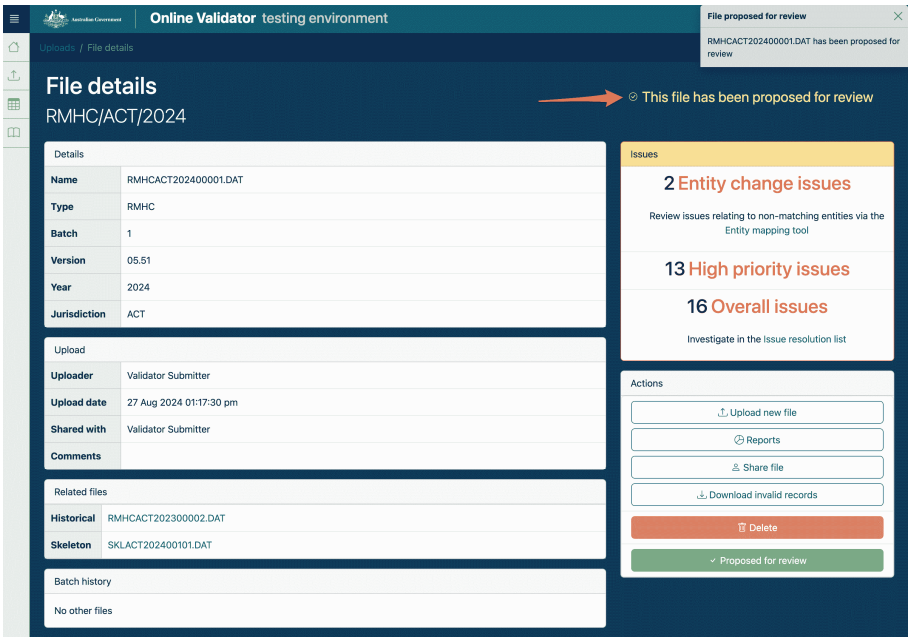


Fig. 4.9 *File Details - File under review*

4.9. Review and issue resolution for Submitters

The purpose of the Review is to identify, and explain or rectify inconsistent, anomalous and exceptional issues. During this process the Submitter and Reviewer may assign control over the list of issues to each other as many times as necessary. Assigning control in this manner prevents the Reviewer and Submitter from having write access simultaneously, maintaining the integrity of notes throughout the issue resolution process.

During this phase, the Submitter can:

- View file contents and check validation issues
- Map entity changes across time (SKL files only)
- View resolution codes and comments assigned to individual issues
- If the Submitter has control they can also:
    - assign issue resolution codes and / or comments to individual issues;
    - assign control of the issue resolution log to the Reviewer; and
    - propose a replacement for the file under review.

4.9.1. Issue resolution list (Submitters)

The Issue resolution list identifies and explains all inconsistent, anomalous and exceptional issues.

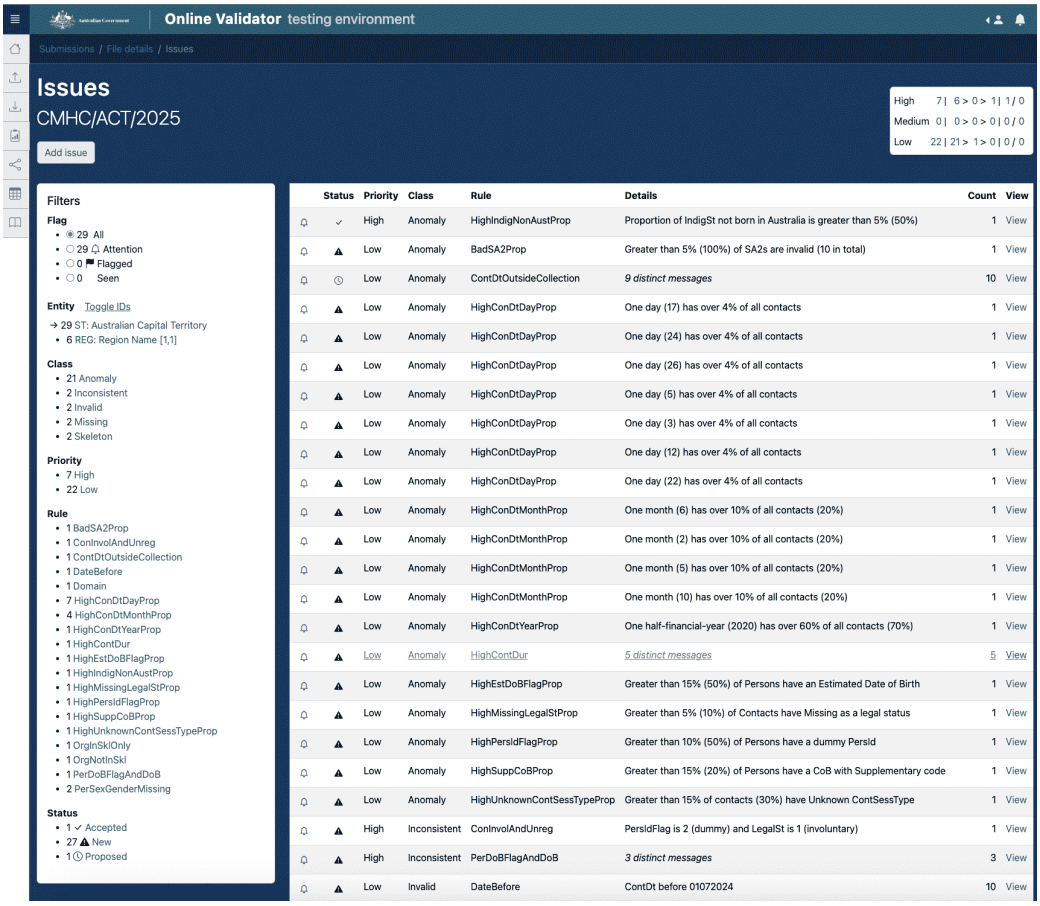


Fig. 4.10 *Issue resolution list*

Clicking on an issue brings up the Issue details modal, via which Submitters assign control over issues to the Reviewer, and vice versa, as many times as necessary. Assigning control in this manner prevents the Reviewer and Submitter from having write access simultaneously, maintaining the integrity of notes throughout the issue resolution process.

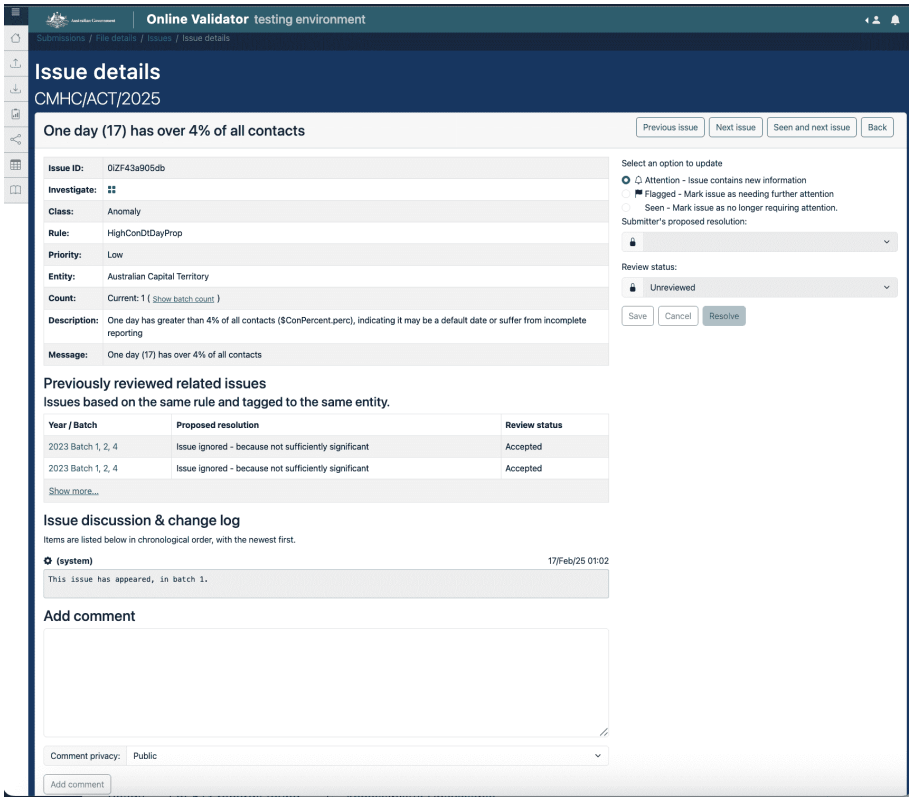


Fig. 4.11 *Issue details modal*

4.10. Entity mapping tool - SKL only

The Entity Mapping Tool enables entities to be mapped across time in the SKL files. This in turn enables the Online Validator to suppress 'child' issues that are caused by entity changes. For example, a change to an organisation's name and ID will generate an issue for that change, and for each of that organisation's 'children', whose parent ID has now also changed. Mapping the organisation to its historical name and ID will then suppress the issues against the organisation's children.

4.10.1. Using the entity mapping tool

1. Select *Entity Mapping* **report for the relevant SKL file:**

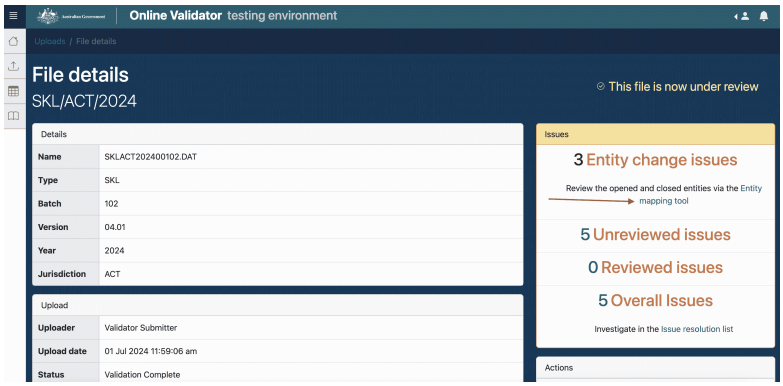


Fig. 4.12 *Submissions Workspace File Details page*

2. Select entities that map directly across the submission years (currently, only 1:1 mappings are possible). Click *Connect two entities*:

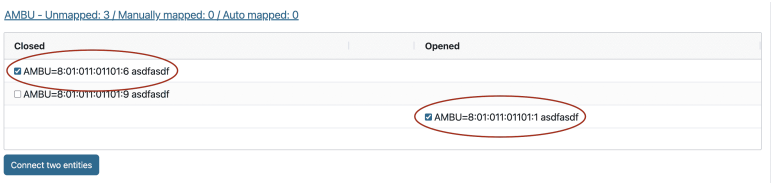


Fig. 4.13 *Submissions Workspace Entity Mapping for Org Record Type*

3. The display will indicate that the entities have been mapped, and provide the option to *Unmap* the entities:

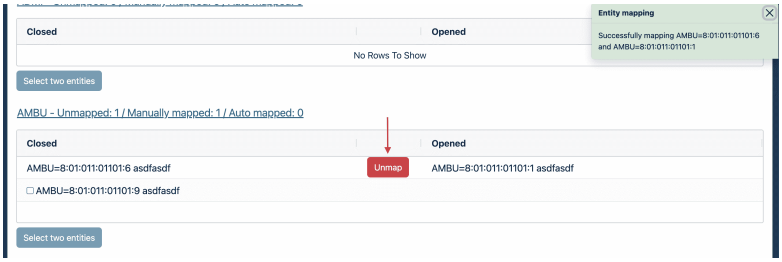


Fig. 4.14 *Submissions Workspace Entity Mapping 'Unmap' button*

4. Continue connecting entities. Note that in the screenshot below the number of unmapped AMBU entities is now 1, rather than 3:

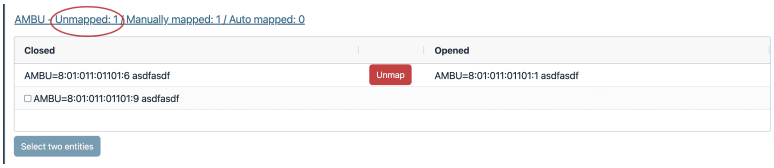


Fig. 4.15 *Submissions Workspace Entity Mapping Summary of Record Types Mapped*

5. The HOSP display shows that some entities have been auto-mapped when ORG entities were manually mapped:

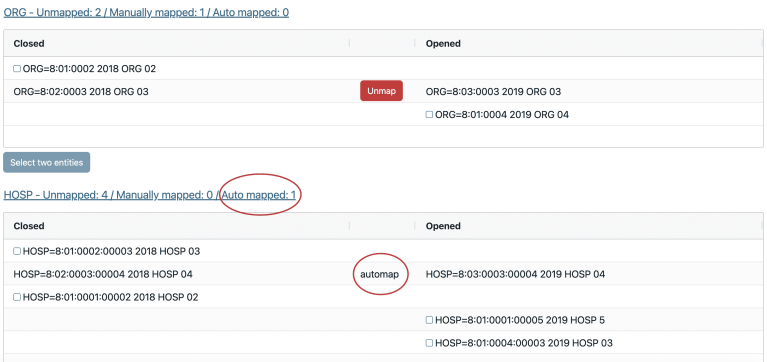


Fig. 4.16 *Submissions Workspace Entity Mapping Auto-mapped entities*

4.11. Completion of the submission process

The submission process is considered complete when all issues have been corrected and/or clarified, and comments and proposed resolutions against each issue are accepted. At this stage, data is marked by an Acceptor as Finalised and is regarded as being suitable for reporting. The data can be manually or automatically transferred to an external data warehouse or reporting system.

Acceptors are able to **Finalise** a submission at any point after accepting a file for review. Generally, any issues requiring resolution are addressed first, as once finalised, no further file versions will be accepted as replacements, and issue resolution is locked.

If required, a finalised submission can be re-opened by an Acceptor, allowing for issues to be edited again, and replacement files can be proposed.

4.11.1. File revalidation

Generally results remain static when a file has been uploaded and validated, however an exception to this is when ALL of the following occur in relation to a file:

- the MDS Rules for the file type use historical data;
- a historical file was not found at the time of the original upload; and
- a historical file was uploaded at a later date.

In those circumstances, a facility exists to revalidate the file.

Users will see a warning explaining that historical checks have not yet been performed, and a button will be present offering revalidation now.

4.11.1.1. Revalidation after software updates

Software updates may also necessitate revalidation. These are usually performed as part of the upgrade, however they can be manually initiated by administrative staff.

5. Rules and V-Fields

- Rules
- VFields

5.1. Rules

Rules are validations that have been created with the aim of improving data accuracy.

Each submitted file will be evaluated against a set of rules. These rules are generated from both the dataset specifications, as well as rules identified by the Commonwealth and jurisdictions to draw focus to common unusual trends that have been found over the history of the project.

Rules for datasets can be found via the metadata site. Each rule has a set of elements, some of which are used in reporting. These include:

- **Name** - Unique shortname used to identify a rule.
- **Class**
  - Anomaly: A field or combination of fields contain data that is likely to be incorrect
  - Barren: The record is expected to have child records but there are none present. This can occur if the child record exists but has irredeemable errors
  - Exceptional: Identifies indicators derived from data combinations that are exceptional on statistical (normative) criteria. Exceptional indicators may point to errors with one or more of the component data elements, or be based on correct data
  - Historical: Information from previous years is used to find changes between years. Examples include: establishments opening, closing or being renamed, significant changes in items that are expected to be stable. The value provided may be correct but should be checked
  - Inconsistent: There is a logical inconsistency between two fields or derived data items
  - Invalid: A field contains incorrect data, misformatted or out of Domain
  - Missing: A field contains no meaningful data. Depending on the entry involved, it may be all spaces, all zeroes, or a Missing value in the Domain (eg. “9”) if applicable to the data-set.
  - Skeleton: Structural comparisons to the SKL file to check the same set of entities is used, or that there is a statistical match between files
- **Priority** - The priority of rules has been determined by the jurisdictions and Commonwealth to enable users to focus on data issues with the greatest impact on the accuracy of reporting.
  - Low
  - Medium
  - High
- **Bulk** - Simple rules that result in a high number of similar issues, such as spaces being used to indicate missing data rather than the appropriate missing value, are reported in bulk, that is, as a total count of the times the issue exists in the submission file.
- **Message** - Short message that briefly describes the issue. The following list indicates rules for formatting:
  - $xxx.perc - this extension formats the numbers as percentages
  - $xxx.commas - this extension formats the numbers with commas
  - $xxx.dmy and $xxx.ddmmyyyy - these extensions format the numbers as dates
- **Mark** - Indicates on which field or record the error is marked.

- **Description** - Detailed description of the issue.
- **SQL** - Outlines the SQL implementation of the rule.

5.2. VFields

Some rules use **Virtual Elements** (*VFields*): fields that have not been directly supplied in your data, instead they are calculated from a variety of fields in the submitted data file. VFields and their SQL can be found via the metadata site.

- **Name** - Unique shortname used to identify a V-Field.
- **Base** - Indicates on which record type the calculation is based.
- **Title** - Descriptive title of VField.
- **SQL** - Outlines the SQL implementation of the virtual field calculation.

6. Reports

6.1. Accessing reports

Users can access reports via the Reports page, accessible from the File Details page.

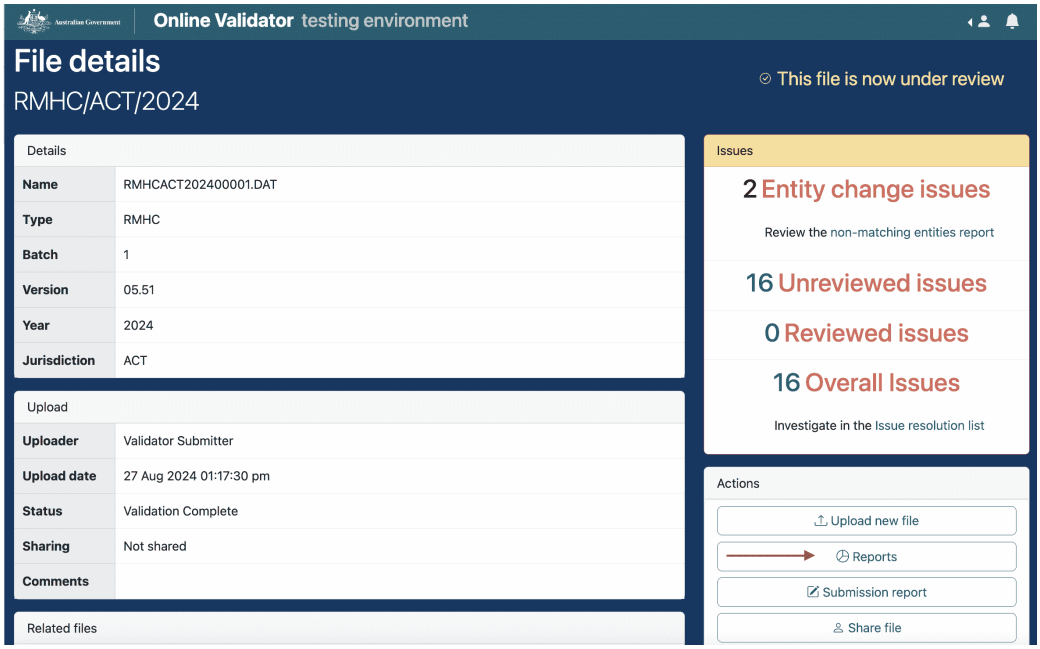


Fig. 6.1 *Reports available from File Details page*

6.2. Record integrity report

The **record integrity report** provides a summary of all records, and presents as a tabluar breakdown by record type of detected issues within the file being validated. This report can be used report to identify records that have structural issues, preventing the file from being proposed for review.

Note that it reports in real time so it can be viewed while the validation run is in progress. Doing so can save you from validating an entire file for which it is already evident a rebuild is required.

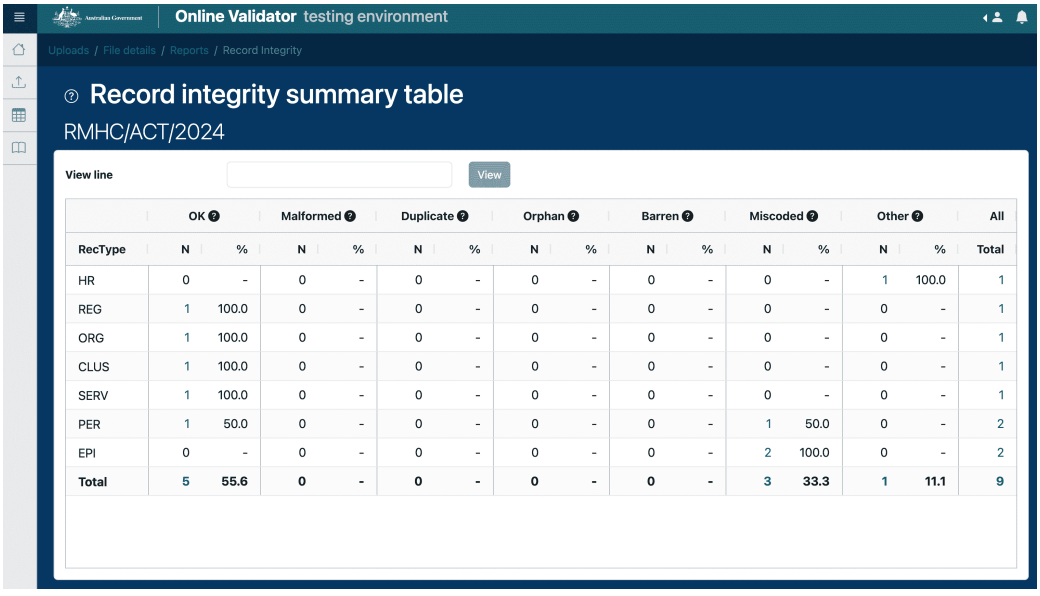


Fig. 6.2 *Record Integrity Summary Table*

A count and percentage is displayed for all items flagged as ***OK***, ***Malformed***, ***Duplicate***, ***Orphan***, ***Barren***, ***Miscoded*** and ***Other***, along with a total count for each record type and for each flag category.

Record integrity validations ensure:

- that records have the correct number of fields, as well as valid data within those fields.
- that records specify valid hierarchical entities. For example, an organisation with a region specifies a valid corresponding region record.
- that organisations have valid identifiers.

These rules are internal (that is, there is no SQL associated with them) as they are applied while processing the raw uploaded file before the data is extracted into the database.

6.2.1. Types of record integrity issues

Table 6.1 Types of record integrity issues

Malformed	The record has at least one issue that renders it undecipherable. Examples include: short lines, bad record types or invalid key fields. The dataset specifications dictate the requirements for each row in detail.
Duplicate	There are two or more records with the same key fields.
Orphan	The record does not have a parent in the submitted file. This can occur if the parent record exists but has irredeemable errors.
Barren	The record is expected to have child records but there are none present. This can occur if the child record exists but has irredeemable errors.
Miscoded	The record has at least one incorrectly supplied non-key field. Examples include: illegal characters, incorrectly formatted numbers, out of domain values and invalid dates.
Excluded	Applies only to NOCC. The record has errors which lead to it being excluded from analysis, for example, a Sequence error Incomplete status.
Other	These are non-structural errors that can be investigated further via the Data integrity reports.

6.3. Data integrity reports

Consistency validations ensure that data appears to be reasonable and consistent, both within the current reporting periods and when compared to data submitted in previous reporting periods. Many of these validations have emerged over time in response to errors in past-year data.

The Data integrity reports report on data that is invalid or appears to contain anomalies, for example:

- a male client should not have a female-only diagnosis
- services should serve a reasonable number of clients
- contact durations should be of reasonable length

There are a number of common terms used in the reports, they include;

- ***Record type***: Fields under this heading will change depending on the file type being reported. Information on a file's expected record types is available in the metadata.
- ***Rule***: Rules are validations that have been created with the aim of improving data accuracy.
- ***Issue***: Highlights uploaded data that triggers a 'Rule' that requires further attention.

Each submitted file is evaluated against a set of rules. These rules are generated from both the dataset specifications, as well as rules identified by the Commonwealth and jurisdictions to draw focus to common unusual trends that have been found over the history of the project.

Some rules use Virtual Elements (VFields). These are fields that have not been directly supplied in the data; instead they are calculated from a variety of fields in the submitted data file. VFields and their SQL can be found via the metadata site.

6.3.1. Dataset reports

Data integrity reports available for all datasets:

- Summary of issues
- Issues by field
- Issues by priority
- Issues by record type
- Rule by record type
- Rule by class
- Organisation by rule (not available to NOCC)
- Region by class
- Organisation level issues list

Data integrity reports available only to **NOCC**

- Hospital cluster
- Organisation by age group and setting
- Sequence errors: Organisation by rule and setting
- Measure frequency distribution
- Person sequence frequency

6.3.2. Invalid records download

The 'Download Invalid Records' link generates a CSV download of all of the invalid records in the datafile. Each row represents a single error; records with multiple errors are repeated with one row per error. This enables users to filter the download as required.

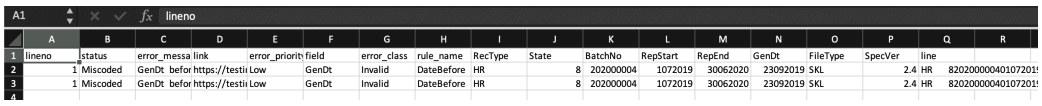


Fig. 6.3 *Example export of Invalid HR Level Records report*

6.4. Cross-file comparison reports

6.4.1. Ad-hoc data explorer

This report allows users to select data elements, such as the number of clients and the number of contacts, for comparison between submissions.

For example, when comparing the number of clients and contacts between MHE and CMHC, the output provides the difference in clients and contacts between each group both as a number and a percentage. Totals are also provided.

6.4.2. Non-matching entities

When uploading a new file (MHE/CMHC/RMHC), users have the option to validate the file against that year's accepted SKL submission. If any entities in the newly uploaded file do not match what is in the SKL file, the Non-matching entities report will helps to identify the unmatched entities.

The Non-matching entities report displays the entities that cannot be matched and lists them in either the ***Not in SKL*** column or the ***In SKL Only*** column, along with the corresponding rule. Clicking on an entity's name takes the user directly to the related issue.

6.4.3. MHE-CMHC Clients & Contacts

This report summarises the difference (absolute and percentage) in **number of clients** and **number of contacts** across MHE and CMHC files.

6.4.4. MHE-RMHC Episode & Accrued MHC Days

This report summarises the difference (absolute and percentage) in **number of clients** and **number of contacts** across MHE and RMHC files.

6.4.5. NOCC-CMHC/RMHC PersId Comparison Reports

This report shows the amount of overlap between the patient identifiers in the NOCC and the CMHC, and NOCC and the RMHC. It has been designed to assist jurisdictions in understanding the integrity of these identifiers for the purposes of subsequent linkage when reporting coverage estimates as is the case with Mental Health Services Performance Indicator (MHS PI) 14, Outcomes readiness.

The NOCC and CMHC/RMHC Total columns indicate the total number of unique person identifiers found in the respective file for the given entity (i.e., at a jurisdiction, region and organisational level).

The Shared Total column indicates the number of unique identifiers found in both files. The NOCC and CMHC Shared columns indicate the percentage of their dataset's identifiers that were shared with the other dataset.

There are several important considerations when interpreting this report:

1. The meaning of this report depends on the consistency of region and organisational code sets. This consistency should be assessed initially via validation of the NOCC & CMHC submissions with the MHE Skeleton. If different code sets are used between these collections, there can be no matches with the patient identifiers.
2. Linkage between the NOCC and CMHC is reported only with those NOCC patient identifiers used for NOCC Collection Occasions in NOCC Ambulatory Mental Health Services Settings and those CMHC patient identifiers where the CMHC person identifier flag indicates a “genuine” unique individual.
3. The report is generated at the time of initial file validation and compares the current submission of the NOCC/CMHC with the available CMHC/NOCC submission for the given reporting period. With the NOCC data it should be noted that there are additional validation processes applied after acceptance that filter only those data that meet the requirements of the NOCC “business rules” (i.e., one episode at a time, change of setting triggers a new NOCC episode of mental health care).

By way of guidance, we can reasonably expect that “all” consumers recorded on the NOCC in ambulatory settings will have service contacts recording on the CMHC. While there are some differences between jurisdictions, previously we have found that approximately 90-95% of NOCC patient identifiers exist in the corresponding CMHC for that reporting period.

On the other hand, the proportion of CMHC patient identifiers that have NOCC clinical ratings is likely to be in the range 35-40%. This is not surprising given that we have consistently found that approximately 30% of all unique CMHC patient identifiers, in a given reporting period, have service contacts recorded on only one or two service contact days.

It may be useful to generate these reports with previous submissions of the NOCC and CMHC/RMHC to check whether there are in fact new issues being identified in the current submission process (e.g., there may be “known” issues regarding “low” completion rates of NOCC measures by some organisations reporting CMHC service activity).

6.5. Trend reports

6.5.1. CMHC/RMHC Activity and Client Level Statistics

This CMHC- and RMHC-specific report provides breakdowns of client and activity data, comparing the current and previous year’s CMHC/RMHC data.

Client reports present contact and client counts broken down by client demographic information (age, sex, etc.).

Activity reports present contact, client, contact hours and treatment days broken down by registration status (is the client registered on the system or is the person generated by the presence of a contact).

6.5.2. MHE: Historical trend report

This report allows users to select and compare information in recently submitted files with that in files that had been submitted previously. Output provided includes current and previous figures and their difference, along with a percentage figure to represent growth for directly apportioned and indirectly apportioned expenditure. Totals are also provided.

6.5.3. NOCC: Protocol adherence

The aim of the **Protocol Adherence Report** is to improve data quality by flagging potential issues of adherence to the NOCC reporting requirements as summarised in Fig 9.1. of the specification: https://docs.validator.com.au/nocc/04.00/collection-protocol.html#figure-data-ep-setting-age-group

The colour coding of the **Protocol Adherence Report** is as follows:

- Green - close to 100% conformance on a mandatory measure.
- Yellow - some conformance, but many items missing from a mandatory measure.
- Red - low or no conformance on a mandatory measure.
- Blue - measures received when no reporting requirements apply. These measures will not be included in the standard NOCC reporting, but may be used by the Jurisdiction for its own reporting purposes.

6.5.4. NOCC: Measure trend

Adherence to NOCC reporting requirements in current submission is compared with historical trend data to determine whether the current submission is credible and valid.

The colour coding of the **Measure Trend Report** is as follows:

- Green - close to 100% conformance on a mandatory measure.
- Yellow - some conformance, but many items missing from a mandatory measure.
- Red - low or no conformance on a mandatory measure.
- Blue - measures received when no reporting requirements apply. These measures will not be included in the standard NOCC reporting, but may be used by the Jurisdiction for its own reporting purposes.

6.6. Reporting principles

Person at organisation, cluster and service unit levels

The person identifiers are defined at ORG level but are reported below SERV on PER records. This leads to various complications. Inconsistent values at a PER level is caught by the *Differs* rules, but it's still possible to have one valid value and some number of Missing values (or all Missing). Counted differently at different SERV and ORG entity levels:

- Same person (orgid+persid) in two units of the same org
- Same person (orgid+persid) in two units of the same org on same day

Both could be counted as 2 at reports below ORG and 1 above.

Variable person attributes

The general principle is to use the most recent valid value. In situations where multiple values can be taken by a person, either different values on PER records in different SERVs or over time on CON attributes, then the most recent (ContDt) valid value should be consistently used in all reports. “Valid” depends on the particular variable, but generally just means non-missing and mappable.

Variable person DxPrinc same-day

Find most-recent contact diagnosis prefix for each person. In the case of a multiple, last-day CONs, the RecordId is taken as a stable, albeit arbitrary, tie-breaker.

Country of birth priority

CoB codes in priority order:

1. Valid: 0001,1000,1100-9999(not 1603)
2. Not Stated: 0003
3. Inadequately Described: 0000
4. Other: ‘ ‘ or out of valid 1603,0002,0004-0999,1001-1099

These priority classes are used by the most recent, valid value rule. Some are more valid than others.

Date of birth priority

More accurate values of DoBFlag are preferred (if present).

Person age

This is calculated at the RepEnd reporting period end date and used in AgeGroup reports.

Treatment day calculation

“Treatment Days” are calculated separately at SERV, CLUS and ORG levels with the result that one ORG person seeing two units on the same day will count as 2 at the lower level and 1 at the higher level.

7. Specifications

7.1. 2025-26

- CMHC v07.00
- MHE v05.00
- NOCC v04.00
- RMHC v07.00
- SKL v05.00

7.2. 2024-25

- CMHC v06.00
- MHE v04.10
- NOCC v03.00
- RMHC v06.00
- SKL v04.02

7.3. 2023-24

- CMHC v05.51
- MHE v04.01
- NOCC v02.11
- RMHC v05.51
- SKL v04.01

7.4. 2022-23

- CMHC v05.50
- MHE v04.00
- NOCC v02.10
- RMHC v05.50
- SKL v04.00

7.5. 2021-22

- CMHC v05.42
- MHE v03.01
- NOCC v02.03
- RMHC v05.42
- SKL v03.01

7.6. 2020-21

- CMHC v05.41
- MHE v03.00
- NOCC v02.02
- RMHC v05.41
- SKL v03.00

7.7. 2019-20

- CMHC v05.40
- MHE v02.40
- NOCC v02.02
- RMHC v05.40
- SKL v02.40

7.8. 2018-19

- CMHC v05.30
- MHE v02.30
- NOCC v02.01
- RMHC v05.30
- SKL v02.30

7.9. 2017-18

- CMHC v05.20
- MHE v02.20
- NOCC v02.00 | v02.01
- RMHC v05.20
- SKL v02.20

The complete list of NMDS specifications is available at https://validator.net.au/webval/metadata

8. MHE NMDS Data Entry Tool

The MHE Data Entry Tool is a Microsoft Access Application that assists Jurisdictions to properly format and submit an MHE Data File into the Online Validator. A release of this tool is made available for each submission period (2021/22, 2022/23, 2023/24 etc).

Instructions:

1. Download the ‘back end’ database mhe-nmds-20xx-20xx-empty-data.zip
2. Download the ‘interface’ mhe-nmds-20xx-20xx-interface.zip

These files are distributed in zipped form. Extract them both to the same folder on your computer and open the MHE-NMDS-20xx-20x-Interface.mdb file with Microsoft Access.

NOTE: If you have entered any data **DO NOT** extract the mhe-nmds-20xx-20xx-empty-data.zip file into the same directory as your old MHE NMDS database or you will lose your data.

8.1. MHE Data Entry Tool releases

MHE NMDS Data Entry Tool for 2024-2025 (Current release) MHE NMDS Data Entry Tool - Data (Empty) 2024-2025, zip format, 57 kB

- MHE NMDS Data Entry Tool - Interface , zip format, 702 kB
- MHE NMDS Data Entry Tool User Guide , pdf format, 1.2 MB

MHE NMDS Data Entry Tool for 2023-2024 MHE NMDS Data Entry Tool - Data (Empty) 2023-2024, zip format, 58 kB

- MHE NMDS Data Entry Tool - Interface , zip format, 733 kB
- MHE NMDS Data Entry Tool User Guide , pdf format, 1.2 MB

MHE NMDS Data Entry Tool for 2022-2023 MHE NMDS Data Entry Tool - Data (Empty) 2022-2023, zip format, 59 kB

- MHE NMDS Data Entry Tool - Interface , zip format, 750 kB
- MHE NMDS Data Entry Tool User Guide , pdf format, 1.2 MB

MHE NMDS Data Entry Tool for 2021-2022 MHE NMDS Data Entry Tool - Data (Empty) 2021-2022, zip format, 55 kB

- MHE NMDS Data Entry Tool - Interface , zip format, 581 kB
- MHE NMDS Data Entry Tool User Guide , pdf format, 1.2 MB