HealthManagement
Promoting Management and Leadership

Best Practices for Sharing Patient Imaging Data

A recent report, published in the *Journal of the American College of Radiology*, describes the top concerns and best practices for preparing and sharing the health data needed to develop artificial intelligence tools. In 2019, the American College of Radiology organised a Data Sharing Workgroup to develop philosophies around best practices in sharing health information. This report details the workgroup's effect in exploring these issues.

1. Privacy

Sharing health data must be secure, reliable, and available only to the intended recipients. There are five key parameters in the information flow: sender, recipient, subject, information type, and transmission principle. The information itself may be dynamic, but not the recipients.

In the U.S., data protection rules are outlined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and establish the concept of protected health information (PHI), which is any information that identifies or can be used to identify an individual. The Safe Harbor method of de-identification removes 18 categories of information, including names, relatives, geographic locales, dates, contact information, and unique identifying numbers. In the EU, the General Data Protection Regulation (GDPR) requires explicit consent to use "sensitive personal data" like health and genomic data and non-health data like financial and employment information. Consent should be easy to withdraw. Some of the stricter portions of GPDR have come to U.S. For example, the California Consumer Privacy Act allows consumers to know when their data are being processed, to opt-out of that process, and to request deletion of personal data, except when already covered by HIPAA. It is important to note that the California regulation does not apply to non-profit entities.

2. Consent

According to the U.S. Department of Health and Human Services, researchers must obtain legally effective informed consent from research subjects under the bioethical principle of respect for persons as autonomous agents. Institutional review boards (IRBs) may waive consent requirements for de-identified data used in retrospective studies under the following conditions:

- The only record linking the subject to the research would be the informed consent form. Thus a breach of confidentiality represents the principal risk to cause harm.
- The research presents minimal risk of harm to subjects.

Thus, de-identified PHI doesn't require a subject's permission for use in studies, quality improvement projects, or commercial purposes. Research cases do require informed consent agreements. For overseeing data sharing agreements outside the purview of the U.S. Code of Federal Regulations or IRBs, parallel frameworks may be needed to govern data sharing. These should cover the patients to authorise the time-span of consent, episode of care, ability to opt-out at any time, and removal of data points. Integrating obtaining consent into the workflow may require digital forms or having staff brief patients before or during imaging procedures.

3. Anonymisation of Radiology Data

Anonymisation of radiology data removes PHI from a data set and destroys any link to the patient's original identity. This differs from de-identification, where a pseudo-identity replaces the patient's identity. A securely held mapping set can relink the data. The decision to anonymise or de-identify data depends on the individual use case, the data’s nature, and whether or not it will leave the radiology practice.

De-identifying image data requires replacing DICOM image headers that contain the Safe Harbor identifiers. Software that can achieve this include DICOM Library, RSNA Clinical Trial Processor, GDCM, PixelMed DICOMCleaner, Tudordicom, and YAKAMI DICOM tools. Some commercially available tools are integrated directly into the PACS. Dates of service are most common in radiological reports; patient names and medical record numbers occur infrequently. Since headers and formats across documents lack consistency, tools specific to radiology are needed for report de-identification.

Conclusions

- Data sharing requires an understanding of the relevant ethical and legal frameworks.
- Data sharing complexities requires careful preparation and annotation of data sets.
- Addressing anonymisation and privacy concerns can be challenging.

Source: Journal of the American College of Radiology

Published on : Wed, 29 Dec 2021