


Review Date: July 2024
Date Developed: July 2021
Principal Responsibility: AOA Board
Endorsed: 3/7/2021 Board Meeting

Approved by:	Title: CEO	Name: Adrian Cosenza	Signature/date  7 July 2021
--------------	---------------	-------------------------	--

OUTCOME:

AOA members will be informed that orthopaedic and patient data generated and/or stored by external stakeholders other than the AOANJRR may not be protected under qualified privilege.

AOA advises that members should proceed with caution when providing any sensitive patient related data to external bodies and ensure that they are familiar with and agree with the privacy policy of the external stakeholder.

It is advised that members discuss the storage of data, notify them that the data will not necessarily be protected by qualified privilege (if applicable) and seek patient consent to store their data with an external body and if applicable.

AOA will not enter into any arrangements, commercial or otherwise when it involves an external party collating or holding member orthopaedic or patient data which is not protected by qualified privilege.

BACKGROUND:

AOA already has specific policies in place to guide industry and surgeons in the use of AOANJRR data, this policy relates to use of orthopaedic and patient data by all other stakeholders.

Orthopaedic and patient data may be generated in many ways by many including, but not limited to, patient records held by orthopaedic surgeons in relation to treatment, data held in practice management software databases, data held in sponsor software packages relating pre and postoperative patient care and data utilised in research projects/clinical trials undertaken by surgeons in conjunction with external bodies eg: hospitals, sponsors, insurers and the like.

AOA members should be aware that databases have a value and could be subject to commercial transactions in exchange for particular data. AOA members are therefore cautioned to ensure any data relating to them or their patients is protected and not liable to on-selling or used for commercial purposes

This policy aims to provide guidance to AOA members and external stakeholders as to the appropriate use and security of orthopaedic and patient data.

DEFINITIONS:

- AOA - Australian Orthopaedic Association
- AOA Members – AOA members of any categories including trainees.
- AOANJRR - Australian Orthopaedic Association National Joint Replacement Registry
- Industry /External Stakeholders - medical device companies, sponsors or manufacturers; medical indemnity or health insurers, includes IT companies, data collection companies, data collection software vendors companies.
- Qualified Privilege - Qualified privilege aims to encourage hospitals and health professionals to conduct quality improvement activities and investigate the causes and contributing factors of clinical incidents by protecting certain information from disclosure.

POLICY

- AOA will not enter into any agreements with industry partners where AOA believes member orthopaedic or patient data may be compromised by not being protected legally.
- AOA will not provide external parties with the names and contact details of any members attending AOA events or educational sessions.
- AOA members must be aware of the possible uses of the patient data held by them, or databases related to the patient management activities where the data is held by external stakeholders.
- AOA members must be cognisant of the privacy issues and potential legal issues around data held by external stakeholders and the potential use of that data.
- AOA advises members not to provide copies of their AOANJRR reports to any external body for any reason as this information is held in the AOANJRR under Qualified Privilege.
- AOA Members who collect and holds data on their own patients without assistance from a software vendor are not subject to this policy.

STRATEGIES:

1. Clinical data
2. Qualified privilege
3. Externally held data

1. CLINICAL DATA

- Orthopaedic and patient data is generated by AOA members, the medical device industry and other stakeholders such as private health insurers on a regular basis particularly in relation to surgical intervention and prostheses use.
- This data may be held by the surgeon, the surgeon's practice, the medical device company, the private health insurer and a database/data warehouse attached to any or all of these entities.
- The data may also be data collected from patients via any method including wearable patient devices or smart phones.

2. QUALIFIED PRIVILEGE

- The Quality Assurance Confidentiality Framework (the Qualified privilege) embrace a wide range of activities, such as academic studies of incidents, some registries, and information involved in the performance evaluation of the relevant services rendered by health care professionals.

- Quality assurance is the process of measuring, evaluating and studying the quality of health care services provided by a person. A quality assurance activity involves measuring the effectiveness of a procedure or process carried out by health professionals and making evidence-based improvements in relation to the particular health care services.
- All States have their own qualified privilege legislation within the Commonwealth overarching qualified privilege arrangements provided under Part VC of the Health Insurance Act 1973 which are intended to address concerns by clinicians that information or data they provide may be attributed directly to them.
- The AOANJRR has Clinical Privilege under the Commonwealth Quality Assurance legislation as outlined in the above dot points.
- Members must be aware that once their data (AOANJRR surgeon reports) are provided to a third party that data are no longer protected under Qualified Privilege and may be subject to subpoena.

3. EXTERNALLY HELD DATA

- AOA member should be aware that data held in external commercially owned databases may not be protected under qualified privilege arrangements. This could potentially leave the surgeon legally exposed in certain circumstances.
- As data has an intrinsic value, members should aware that clinical data may be used by the database owner for commercial purposes.