Storage of your information

Dr. Brooks stores your demographic and medical information in 3 HIPAA (Health Insurance Portability and Accountability Act) compliant, secure (firewall and password protected) sites:

- Dr. Brooks' computers and external hard drives
- Microsoft Office 365 Cloud
- U of AZ REDCap https://www.project-redcap.org

Dr. Brooks has written confirmation that the Microsoft Office 365 Cloud is HIPAA compliant and secure. A copy of that document is available from Dr. Brooks upon request.

Dr. Brooks has written confirmation from the U of AZ that the U of AZ REDCap is HIPAA compliant, that all of your information will be held in confidence, and that the U of AZ assumes responsibility for any data breach of the U of AZ REDCap that compromises the privacy of your medical and demographic information. A copy of that document is available from Dr. Brooks upon request.

All business and medicolegal information is **only** stored on Dr. Brooks' computers and the Microsoft Office 365 cloud.

Use of your information

Dr. Brooks and his office manager/research assistant, James Brooks are Designated Campus Colleagues (non-paid but contracted, thus voluntary, positions) with the U of AZ Department of Orthopedic Surgery—Dr. Brooks' former employer. Dr. Brooks and James Brooks hold those positions to engage resources intended to enhance **your** health care as well as that of other patients.

In addition to information derived from traditional history taking, physical examination and the results of any lab, imaging, or other studies, Dr. Brooks also collects standardized "Patient Reported Outcome Measures" (PROMs): the current "gold standard" for which is only available through the REDCap project (which is not available to commercial entities such as a private medical practice). As data capture technology is put into place, Dr. Brooks intends to also collect pain location and severity information as well as "Functional Outcome Measures" about motion and balance using "wearable sensor" technology.

There are two categories for analysis of **pooled** patient information:

- Quality data
- Research data

“Quality" information about you may be pooled and analyzed by Dr. Brooks, at his discretion, to improve the quality of care provided to his patients; to conduct quality improvement activities; to obtain audit, accounting, or legal services; or to conduct business management and planning. The results of any such analysis must be held in confidence by Dr. Brooks. The results are not publishable.

In contrast, **“research”** is performed to enhance the care of **all patients everywhere**. In that spirit, Dr. Brooks is collaborating with researchers in the U of AZ Department of Orthopedic Surgery to perform **“outcomes research”**: in other words, assessment of the effectiveness, safety, and efficiency of an established medical intervention. “Outcomes research” does not require your explicit informed consent as it only analyzes data collected in the usual course of medical care. No interventions that would be considered “experimental” are provided.

By signing Dr. Brooks Medical Care Agreement, you agree that all of your demographic and medical information may be stored on the U of AZ REDCap and that, unless you expressly “opt out” (refuse permission), all of your **deidentified** information may (upon approval of the U of AZ “Internal Review Board” charged with protecting human subjects in research protocols) be pooled and analyzed for the purpose of outcomes research. The results of such analyses may be published.

Deidentification is performed by removing the following 18 classical personal identifiers prior to pooling and analysis of data:

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers (not applicable for Dr. Brooks’ patients)
9. Health plan beneficiary numbers
10. Account numbers (not applicable for Dr. Brooks’ patients)
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images

18. Any other unique identifying number, characteristic, or code (Note: this does not mean the unique code assigned by the investigator to code the data.)

There are also additional standards and criteria to protect individual's privacy from re-identification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, a subject's initials cannot be used to code their data because the initials are derived from their name. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study nor can the method to derive the codes be disclosed. In other words, the information would still be considered identifiable, if there was a way to identify the individual even though all of the 18 identifiers were removed.