TT Tracker Data Security and Compliance

The TT Surgery Tracker utilizes two platforms for data collection and data visualization. CommCare Enterprise level software, developed by Dimagi, is used to collect and manage data, while Metabase is a data visualization tool used for reporting de-identified summary data. While using both of these systems to support the efficient tracking and reporting of surgical activities security of patient data is of the utmost importance.

Data Security

CommCare

Data are collected with the android-enabled mobile device using a password-protected data collection app. Data are stored within CommCare - to which only designated users have access via individual username and password - and will remain on their HIPAA-compliant servers throughout the use of the TT Tracker. HIPAA, or the Health Insurance Portability and Accountability Act of 1996, is the United States legislation that provides data privacy and security provisions for safeguarding medical information. The HIPAA Security Rule establishes standards for protecting health information that is held and/or transferred in electronic form. Compliance means that technical and physical safeguards ensuring the integrity and confidentiality of electronic patient data have been taken to protect against impermissible uses or disclosures. It also ensures that data are backed up offsite and may be recovered accurately and intact in the event of disaster.

When in transit, data are encrypted to ensure data security and patient privacy. The cloud-based system is compliant with ISO 27001, which is the best-known standard in providing requirements for information security management systems. Data housed within CommCare will be stored in one of two data centers within the US, Rackspace or Softlayer. Rackspace adheres to ISO 27001, ISO 27002, PCI-DSS, SSAE16, SOC1, SOC2, SOC3, Safe Harbor, and CPS. Similar to Rackspace, Softlayer's security management is aligned with US government standards based on NIST 800-53 framework, and is compliant with SOC1, SOC2, CSA, PCI-DSS, HIPAA, and HITECH.

Metabase

Metabase is a password-protected platform used for data visualization and reporting. All information uploaded into Metabase will be de-identified and displayed in the aggregate. Though data are de-identified, it is still paramount that data be kept secure. Data viewed in Metabase will be housed on a secure server, hosted by Amazon. Amazon Web Service (AWS) has network firewalls and data encryption for data while in transit. The cloud-based system is compliant with ISO 27001, which is the best-known standard in providing requirements for information security management systems. It also adheres to ISO 900, SOC1, SOC2, SOC3, CSA, and PCI-DSS. AWS is also HIPAA compliant.

Administrator

The Administrator, as designated by the Ministry, has access to all elements of the application, from users to locations to data. The Administrator can also limit the access to records and data editing capabilities within the country. In the Letter of Cooperation, country programs will also grant permission to the TT Tracker Development Team to provide Administrator assistance.

Partners

Ministries will have access to all data entered by various partner programs entering surgical activity information. Partner programs, however, will have a limited view of the data, only seeing the information from their own programs.

Mobile workers

When utilizing the phone application, CommCare controls access to patient records by issuing usernames and passwords for each phone. Users working in the area are given a username and password for the phone in use so that patient information can be reviewed and/or updated. The access to patient records is also managed using coverage areas, limiting access of users to only the records within the coverage area(s) where he/she works. The web-based version of the TT Tracker for mobile workers utilizes the same data access controls as the mobile phone, ensuring the security of patient records by limiting access to individuals with a username and password and following the same coverage area designations for patient records.

Identifiable Data

Most summary reporting is done on the aggregate, summarizing data to the district, regional, or national levels and does not include individual patient data.

CommCare

Reports and exports created from CommCare can include identifiable patient data, if desired, so that users may locate a specific patient record if an issue arises. Follow-up lists do include patient names as it is required for planning follow-up and audit activities for those patients. At the request of the Ministry, follow-up lists can be sent via email to designated supervisors who are responsible for follow-up outreach planning.

Metabase

Reports created from Metabase include de-identified information only, providing summary analyses and reports in the aggregate. Information stored will not include patient or surgeon names or identifiable information. Though individual surgeries can be queried, the identifiable information will be redacted, as it will never be stored in Metabase and is only available within the CommCare system. Unique surgeon IDs are included in the Metabase reporting, but partners will have to ask the Administrator or those with the highest levels of access in CommCare to reference the surgeon list and access the name of the surgeon.