# Research with Digital Data Collection Tools

The purpose of this guidance is to assist researchers navigate review processes for research utilizing **digital data collection tools (“DDCT”)**, such as wearable devices or software **applications (“apps”)** downloaded on a research subject’s device. Historically, clinical research data has been generated and collected using standard collection methods and verifiable source documents. As technology becomes more prevalent in society and healthcare, DDCTs are becoming increasingly common in human subjects research. Some studies develop, test, or validate the DDCTs themselves, while others use DDCTs solely to collect data. Questions regarding DDCTs can be directed to Medical Center Information Technology (MCIT) at [#NovelTechnologyReviewTeam@nyulangone.org](mailto:#NovelTechnologyReviewTeam@nyulangone.org).

DDCTs collect, transmit, and/or disseminate private, or non-private, actively or passively collected data or private information using software or technology on mobile or wirelessly communicating devices such as smartphones, free- standing monitors or sensors, or wearable devices that collect information at a point in time or over a period of time. All DDCTs being developed, tested, validated, or used in human subjects research are subject to NYU Langone Health’s review, including DDCTs developed in-house and DDCTs provided by a sponsor or other third party. NYU Langone Health’s review will include a review of any **Terms of Service (“TOS”)** or **End-User Agreements (“EUA”**) associated with a DDCT.

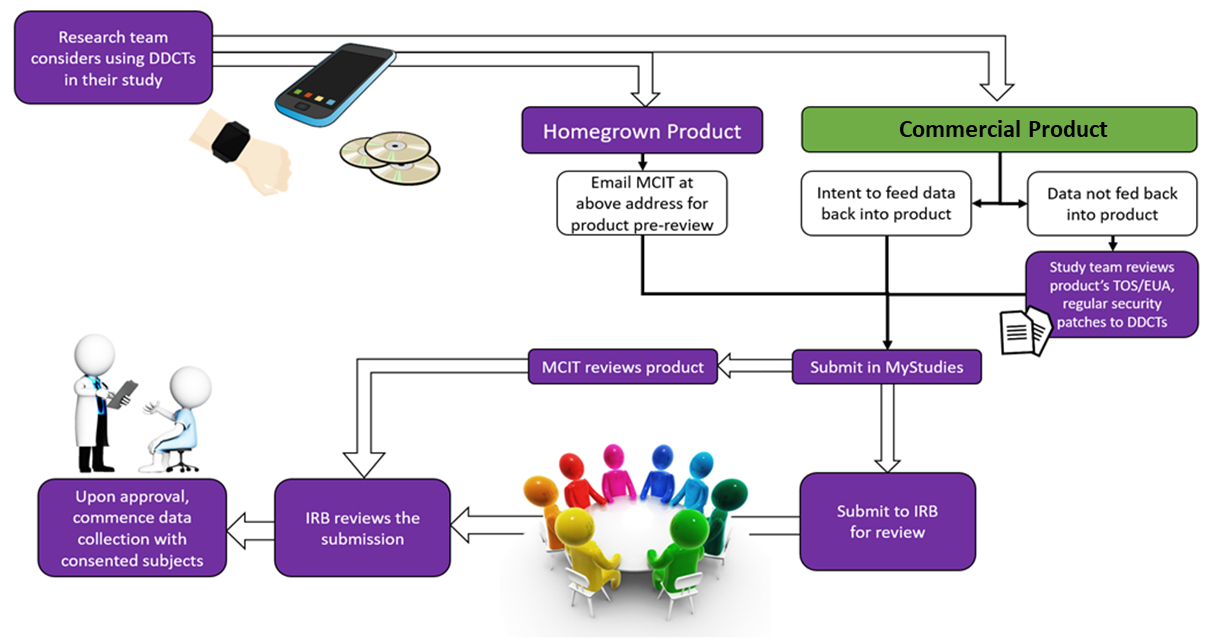
Topics covered in this guidance include:

* Institutional review process of DDCTs in research
* Considerations for ensuring protection of privacy and confidentiality
* Review of TOS and EUA by researchers
* Data security plans, incident response, and mitigation tips

The following topics are not covered in this guidance:

* Use of applications/software other than DDCTs in research
* FDA requirements for investigational devices and their applicability to DDCTs used in research

## Institutional Review



**Note:** *IRB is not the only review body required for projects involving a DDCT at NYU Langone Health. MCIT may need to conduct an “ancillary review” of*

*the technology, similar to radiation safety or pharmacy ancillary reviews. In other cases, the study team will assess the use of the digital data tool.*

As illustrated in the diagram above, several points must be considered when designing and/or employing DDCTs. The origin of the DDCT, and the way in which the data will be used, also affects the pathway to approval of the DDCT:

| **Type of DDCT** | **MCIT Review of DDCT** | **Researcher Review of EUA/TOS** | **OSR Contracts Review of EUA/TOS** |
| --- | --- | --- | --- |
| Homegrown application or software  (requires contracts review in order to create the EUA/TOS prior to review of created EUA/TOS by the IRB) | **✓** |  | **✓** |
| Commercially available wearable device, including free products  (used as marketed, where data not fed back into the product) |  | **✓** |  |
| Sponsor provided application or software | **✓** | **✓** | **✓** |
| Free, commercially available application or software |  | **✓** |  |
| Licensed, commercially available application/software (purchased by NYU Langone, if data will be fed back into the product) | **✓** |  | **✓** |

Commercial or sponsored DDCTs may collect and store data from research subjects and provide that to researchers at NYU Langone for use. If the DDCT requires additional data from NYU Langone, further MCIT review is required.

## Researcher Review of Terms of Service and End-User Agreements

### Why Is Review of Terms of Service (TOS) and End-User Agreements (EUA) Important?

When using third-party product as a DDCT, the provider may ask research subjects to agree to certain terms of service. DDCTs have documents, referred to as the EUA or TOS, which require subject agreement prior to access and use. Researchers must review EUAs/TOS as part of their assessment of whether the tool is appropriate for the study and whether the tool has measures in place that protect the privacy, security, and confidentiality of the subject’s information. Researchers should **confirm their review of the EUA/TOS in the** **protocol**, that no unacceptable terms were found, and that the EUA/TOS will serve as the subjects’ notification of risks related to use of the DDCT when participating in the study. Third-party services and related DDCTs licensed by NYU Langone Health also require review of the EUA/TOS by MCIT.

### What Should Researchers Look for When Reviewing the EUA/TOS?

Look for who owns the data collected via the service, what might be done with the data in the future, and the user’s rights regarding their data. The EUA/TOS are contracts between the user/research subject and the product provider. Review the EUA/TOS for:

* Protection for private information that only subjects who have consented to participate in the research can access. The research team should only access data required for the research.
* Mechanisms for developing, testing, publishing, and deploying updates so that discovered vulnerabilities are mitigated, even on devices on which the DDCT was previously installed.
* Who developed/hosts the DDCT and data and the level of security they will provide.
* How the DDCT will be installed on research participants’ devices.
* A plan for removing the DDCT when it has reached the end of its lifecycle, including whether the DDCT will be disabled or removed from devices when the study ends, if the tool instructs installers to remove it upon completion of the research, and what will happen to the collected data. DDCTs that have temporary or limited utility should recommend removal from the user’s device when the utility of the DDCT expires.
* If researchers will be entering data on/into a commercial DDCT service, the EUA/TOS must not conflict with NYU Langone Health policy, or governmental contracts/grants in regards to data ownership. ***Note that ownership of institutional data must remain with NYU Langone Health.***
* The level of control the host allows the study team torecords relating to NYU Langone Health business, such as email, instant messages, files, etc.
* If the DDCT service is free, or if the EUA/TOS are not subject to negotiation. Researchers should be aware that such scenarios leave them with no recourse against the vendor if there is an incident or if the host changes their privacy or security practices.
* If minors may access the app, and if the parent needs to agree to the child’s access.
* Language that would not be allowable in a research context, such as a waiver of legal rights, or indication that developers may own the data collected by their products and that they retain the right to use the data for any purpose later on.

## Data Security Plans, Incident Response, and Mitigation Tips

Data collected via DDCTs is subject to the same data security principles that apply to human subject research data. Researchers must consider if data collected as part of the DDCT function is necessary to the study and if they should strip such data from the research data set. Avoiding collection or storage of data is an effective way to protect sensitive data.

Protocols developing, validating, testing, or using a DDCT must include a data security plan that contains a review of the DDCT and reflects a genuine effort to ensure that only the minimum necessary sensitive data is collected and stored. When sensitive data is collected or stored, the plan must indicate how researchers will protect the data and any copies or extracts of the data through its lifespan. The plan must include provisions for the destruction or de-identification of any sensitive data using current best industry practices. Researchers may be required by NYU Langone Health to produce such data and records at any time, regardless of whether it is stored on institutional or non-institutional systems/services.

Researchers must:

* Retain contact information of research subjects, internal and external collaborators, study team members, and participating sites in the event that research data (including but not limited to data collected by a DDCT) is compromised, lost, stolen, or subjected to unauthorized use
* Review with NYU Langone Health’s incident response policy
* Contact the IRB (see footer), the Office of Internal Audit, Compliance & Enterprise Risk Management (24/7 anonymous compliance helpline: 866-698-1212), and other relevant offices in the event of an incident
* Train study staff on incident response and mitigation measure