TEACHERS COLLEGE IRB
INSTITUTIONAL REVIEW BOARD

SOP-M-004: TC IRB Standard Operation Procedures (SOP) on Business Continuity for IRB Operations

Purpose

To outline the procedures for ensuring the continuity of Teachers College IRB (TC IRB) operations during emergencies or disasters to protect research participants and facilitate recovery of research activities.

Scope

This SOP applies to all IRB staff, IRB members, researchers, and other institutional stakeholders involved in IRB-related processes during emergencies or disasters.

Definitions

- Business Continuity Plan (BCP): A plan to ensure critical business functions continue during and after a disaster.
- Emergency or Disaster: Any event that disrupts normal IRB operations, including natural disasters, pandemics, infrastructure failures, or cybersecurity incidents.

Policy

Although relatively infrequent, emergencies and disasters of all types can occur and have a devastating effect on institutional operations that also affect research operations. In any emergency, there are both individual department and institutional responsibilities to ensure timely and efficient resumption of research activities after the emergency or disaster. Organizations should have a Business Continuity Plan (BCP) that encompass the entire organization, and an IRB BCP should fit within the larger organizational BCP, but must be specific for how research operations will continue after, for example:

- A hurricane destroys infrastructure and communication and prevents access for an extended period
- Major flooding causes damage to research facilities
- A tornado causes structural damage to organizational and research buildings
- An earthquake that destroys infrastructure and disrupts communication
- A blizzard causes power loss and prevents access to research facilities
- A pandemic causes closure of the research facilities and impacts a large percentage of research staff for an extended period
- Organizational and/or IRB electronic systems are compromised
- Some other event that causes long-term disruption of operations

To ensure that research participants are protected from research-related harms during an emergency or disaster, it is essential that the IRB be able to function in its protective capacity throughout the disruption. For example, subjects in research may need to continue their investigational interventions (drug, device, behavioral) or receive an alternative intervention to assure their safety and well-being or research plans may require cessation of enrollment and/or changing to remote interactions or locations rather than having subjects come to the research site to complete research required activities (e.g., follow up exams, receipt of investigational products, etc.).

The IRB at Teachers College is committed to protection the rights and welfare of research participants during both normal and emergency operations. The procedures described in this section are intended to assist in:

- maximizing the effectiveness of the IRB's response to emergencies and disasters;
- ensuring IRB operational continuity to the extent possible throughout the emergency or disaster; and
- protecting research subjects and efficiently recovering from disruptions from emergency situations.

Procedures

1) Preparedness

The Research Compliance Director, in collaboration with the IRB Chair, is responsible for developing and maintaining the IRB emergency preparedness, continuity and recovery plan. The overall plan is intended to cover a worse-case scenario, however, only the components of the plan that are required for the specific emergency will be implemented. The IRB plan will coincide and coordinate with the existing Teachers College policies below:

- Teachers College Information Services Business Continuity and Disaster Recovery Policy
- Teachers College Clery Crime Alerts, Emergency Notifications, and Campus Safety Advisories Policy
- Teachers College's Emergency Response Protocols
- Teachers College's Emergency Evacuation Procedure

2) Key Contact List

Perhaps the most important component of a BCP is knowing who to contact during an emergency or disaster and how to contact them assuming communication disruptions. Therefore, the Research Compliance Director will develop a list of key IRB emergency contacts and their contact information to aid in communication and coordination during an emergency, as well as the emergency contact list for the organization. These lists will include cell phone numbers assuming that the contacts may not be able to be on-site during the emergency. The list will include IRB and IRB staff and the Institutional Official and may also include specific researchers and staff.

- Organizational emergency contact lists will include:
- Information technology staff that support the IRB systems
- Facilities management and critical infrastructure support (power, water, heat, etc.)

- Organizational security
- Human resources and payroll
- Organizational leaders
- Federal agencies/funding sources

The Research Compliance Director will keep a written copy of the contact list below in a location that can be readily accessed assuming that normal internet and intranet services will be lost:

Contact Name	Phone number
Emergency	911
TC Public Safety	(212) 678-3333
Vice President for Academic Affairs, Provost and Dean of the College (Institutional Official)	(212) 678-3050
Research Compliance Director	(212) 678-4105
TC IT	(212) 678-3300
Mentor IRB (Sitero)	(888) 275-2462

3) Establish an emergency communication plan, test it periodically and revise as necessary

a. Communication Methods

To ensure effective and timely communication during an emergency or disaster, the Research Compliance Director will develop a "call tree" that is a hierarchy or "tree" of people in which each person calls and forwards a message to the next person down the tree. For example, the Institutional Official or IRB Chair are listed at the top of the call tree and calls the person below them on the tree, and so on. The "tree" can be branched for efficiency and expediency to reduce the number of calls any single person is required to make and assist in getting everyone notified as quickly as possible. If a person on the list does not answer, the caller skips to the next person on the tree to ensure that as many people as possible are contacted. The last person(s) on the call tree contacts the first person on the call tree to confirm that the calls/messages went through the entire call tree. This assures that all individuals on the tree receive the communication. For example: Assuming that cell phone coverage is intact, communications will be conducted using cell phone service and the call tree. Anticipating that the volume of cell phone calls will increase during an emergency, for less emergent calls, the plan may also include specified call times to attempt to communicate at times where call volumes are expected to be lower (e.g., early or late in the day).

i. Assuming that cell phone coverage and internet service will be disrupted, the plan will also include other methods of making contact with IRB and key organizational staff. These methods might include meeting in-person at off-site locations at specified times. If possible, procedures for utilizing local radio and television services to communicate messages to institutional personnel should be established. If this can be established, the BCP should provide information on the stations that should be monitored.

ii. The BCP should also include methods for communicating the procedures and/or adjustment to procedures that will be implemented during an emergency or disaster.

iii. The Research Compliance Director is responsible for assuring that the call "tree" is constantly up to date. Individuals can be added or removed as necessary to represent the most current staffing. The Research Compliance Director should test the call tree at least annually to assure that all individuals are available at the numbers listed. In order to assure a more realistic assessment of the call tree, tests should not be announced. All individuals on the tree should carry or have immediately available to them, a copy of tree in the event a test is initiated, or an actual emergency occurs.

iv. The Research Compliance Director, in collaboration with the IRB Chair, will ensure that input from all IRB components and applicable organizational units is sought, considered and discussed. Facilities Management should be involved to describe when a building or office is not safe or operational, who will make that determination, how to contact that person(s), if/when relocation of IRB operations will be required and how the relocation will be communicated and accomplished. This part of the plan should describe who is responsible for and how paper-based files will be relocated, stored, secured and maintained, when necessary.

v. Information Technology (IT) should provide a description of the organizational priorities that will impact the level of support that can be expected for IRB electronic systems. Other organizational offices should contribute if they have the potential to affect IRB operations. A critical factor in developing the IRB BCP will be having individuals who are responsible for the organizational BCP be part of the IRB planning process to assure that the organizational and IRB BCPs can be carried out without significantly impacting either plan.

4) Management of IRB operations during emergencies.

a) It is likely that normal operations will not be possible during an emergency and adjustments to IRB submissions, COI disclosures, sponsored program activities, etc. will need to be made. The IRB BCP should inform stakeholders (staff, organizational officials, researchers, etc.) as to what the adjustments will or might be, how emergency operations will be conducted during an emergency or disaster and the potential impact of implementing the BCP. As much as possible, the emergency or disaster should be "triaged" to determine the types and extent of adjustments that must be made. There can be many possibilities. For example:

i. In a severe emergency with significant infrastructure loss or disruption, suspension of new protocol submissions and/or review and execution of new contracts, except in extraordinary circumstances, will likely be required, however, continuing review and amendment requests, unanticipated problem reports and other time-sensitive reviews will have to accepted and processed to assure that protection of research subjects is not interrupted. The IRB BCP must describe:

- How to contact the Institutional Official, IRB Chair and the IRB Director
- How the time-sensitive submissions will be accomplished and processed

- How results of IRB review will be communicated to researchers
- Assuming disruption of electronic system operation, how records will be maintained for the duration of the emergency

b) To be as efficient as possible, a new IRB, with the regulatory minimum number of members (5) and make-up (one non-scientist, one scientist, one non- affiliated) may need to be established to review the time-sensitive submissions, assure subject safety and well-being and prevent lapses in IRB approval. In this situation, applicable regulatory agencies should be notified, as soon as possible.

i. IRB meetings may be conducted face-to-face, by tele- or videoconference or by a combination or all three but may change from meeting-to-meeting due to loss or restoration of internet and phone service.

c) In the event of infrastructure destruction or loss of operational capability or in the interest of staff safety, IRB and other IRB activities may need to be relocated to sites in other areas of the institutional facilities or remote from institutional facilities. Advance arrangements must be in place that assures site availability so several contingent sites may need to be identified. The sites should have appropriate security, HVAC, electrical power, water, internet service (if possible) and be easily accessible, if in-person operations are required.

i. For paper-based systems, relocation must be to a secure location to assure file integrity throughout the emergency or disaster. Appropriate utilities must be in place to control temperature and humidity.
ii. The electronic IRB files at Teachers College are stored on a server (Mentor IRB) used for day-to- day operations that is not at the organization's physical location (cloud service) and are backed up at least daily.
iii. All TC IRB staff members are provided with a laptop for business purposes. These laptops include access to telecommunication systems, email systems, and a Virtual Private Network (VPN) for all business-related purposes. TC
iv. IRB's IT systems may be utilized remotely in a disaster situation. Note that TC IT is available to assist in configuring IT systems for offsite access, and in addressing technical questions of the staff. Also refer to TC's Information Technology Network and Email Accounts Policy for further discussion regarding IT policy.

5) Communication of the BCP prior to having to use it in an emergency or disaster

All IRB components and applicable organization officials and departments should have access to a copy of the IRB BCP. At least annually, the BCP should be reviewed to assure that all information in the plan is accurate and up to date. If necessary, the Research Compliance Director, in collaboration with the IRB Chair, will make revisions to and update the BCP. After each review, a pdf copy of the BCP will be electronically available to all IRB components, applicable organizational officials and those responsible for carrying out the organization's BCP in the event of an emergency or disaster.

6) Periodic verification of the BCP

It is essential that the BCP plan is accurate and can actually be implemented in an emergency or disaster. To verify that the BCP will be able to support IRB operations, the Research Compliance Director should periodically:

a. Test the communication system(s) to assure that those that need to be contacted can be contacted;

b. Conduct on-site audits of locations to which operations may be relocated;

c. Verify how servers and their back-up procedures respond to power outages and other types of disruption that might occur;

d. Evaluate access to buildings, paper-based and electronic files and relocation sites that may be required during an emergency or disaster.

7) Training of IRB staff on the BCP

To assure that all IRB staff are aware of might be required of them during an emergency or disaster, situational training will be provided and may be required for specific individuals. Training will include how normal operations could be affected, the adjustments that may have to be made and specifically how operations may have to be carried out during the emergency or disaster. The training will be developed and conducted by the Research Compliance Director in collaboration with the IRB Chair, as needed.

8) Continuity

To assure continuity of operations as much as possible, the plan will be followed to the extent required to assure continued IRB operations and assure that subjects remain protected. Modifications to the BCP and/or implementation of temporary IRB Standard Operating Procedures may be required as emerging conditions develop.

IRB continuing reviews, amendments and unanticipated problem reports will be processed and reviewed so that approval for research studies does not lapse and that subject protections remain in place. Reviews may be conducted through an expedited process, when applicable, or through review at a convened meeting of the IRB. Depending on the specific situation, a newly established IRB with the minimum required membership may review the submissions for the duration of the emergency or disaster.

Other IRB components will likely make adjustments to their operational procedures, and these should be described in the BCP.

9) Recovery

Upon recovery from the emergency situation, resumption of normal operational SOPs will proceed at the fastest possible rate, but complete recovery will be dependent on the extent of procedural changes that were made for the emergency. If the IRB offices and files were relocated, arrangements will need to be made to return staff and files to the on-site location. The BCP should include important steps to take, required resources, and key contacts needed to complete the task. An effective recovery strategy and recovery tasks should be easily understood by all involved with the recovery.