Disaster and Contingency Planning for Scientific Shared Resource Cores

Sheenah Mische¹ and Amy Wilkerson²

¹Office of Collaborative Science, New York University School of Medicine, New York, New York 10016, USA; and

²Research Support, The Rockefeller University, New York, New York 10065, USA

Progress in biomedical research is largely driven by improvements, innovations, and breakthroughs in technology, accelerating the research process, and an increasingly complex collaboration of both clinical and basic science. This increasing sophistication has driven the need for centralized shared resource cores ("cores") to serve the scientific community. From a biomedical research enterprise perspective, centralized resource cores are essential to increased scientific, operational, and cost effectiveness; however, the concentration of instrumentation and resources in the cores may render them highly vulnerable to damage from severe weather and other disasters. As such, protection of these assets and the ability to recover from a disaster is increasingly critical to the mission and success of the institution. Therefore, cores should develop and implement both disaster and business continuity plans and be an integral part of the institution's overall plans. Here we provide an overview of key elements required for core disaster and business continuity plans, guidance, and tools for developing these plans, and real-life lessons learned at a large research institution in the aftermath of Superstorm Sandy.

KEY WORDS: core facility, business continuity, emergency management, emergency preparedness

INTRODUCTION

"Plans are worthless, but planning is everything. There is a very great distinction because when you are planning for an emergency you must start with this one thing: the very definition of 'emergency' is that it is unexpected, therefore it is not going to happen the way you are planning." — Dwight D. Eisenhower¹

On October 29, 2012, the posttropical cyclone remnants of Superstorm Sandy made landfall along the coastal areas of New Jersey and New York. The storm is widely considered by experts to be the most powerful in the Northeast in recorded history. An unusual combination of weather phenomena (warm Caribbean air, a high pressure system over Greenland, and a disturbance in the jet stream), combined with a full moon, caused a storm surge, with the East River water levels rising more than 14 feet. New York University Langone Medical Center (NYULMC) and associated hospitals, Bellevue and Manhattan Veterans Administration, were inundated with more than 15 million gallons of water flooding the lowest floors of every building on the main campus in mere minutes. Shortly thereafter, at approximately 9:00 PM Eastern time, a major electrical substation in lower Manhattan had flooded and exploded dramatically, plunging most of the island below 34th Street

into darkness (Fig. 1). NYULMC and Bellevue Hospital, just blocks apart, were thrown onto backup generators.² Despite facility precautions that included locating generators on higher floors and installing flood barriers in basements, both lost their backup power at the height of the storm water surge and could not restore it.³ The flood waters directly and indirectly caused irreparable damage to medical equipment and research materials on the ground floor and the basement and caused ancillary damage to operations and loss of research materials throughout the institution, including the NYULMC-shared resource cores. On October 30th, President Obama declared a major disaster for the State of New York [Federal Emergency Management Agency (FEMA)-4085-DR-NY], authorizing the Department of Homeland Security's (DHS) FEMA to provide federal assistance in designated areas of New York.

These events created impetus for significant changes in emergency preparedness, business continuity, and disaster response at NYULMC. Sandy was one of the most devastating superstorms ever to hit the East Coast and a stark reminder of the fragility of life in all aspects. From a public perspective, Sandy left approximately 8 million homes and businesses without power. In New York City alone, the effects were devastating, with estimated economic losses in the vicinity of \$42 billion from the flooding of the city's subway system and several road tunnels entering Manhattan, the loss of electricity for days, evacuations, network outages, and the closure of the New York Stock Exchange for 2 consecutive days.

ADDRESS CORRESPONDING TO: Sheenah Mische, Office of Collaborative Science, NYU School of Medicine, New York, NY 10016, USA (Phone: 212-263-0859; E-mail: sheenah.mische@nyumc.org)
doi: 10.17171/jbt.16-2701-003

FIGURE 1

Aerial photograph of lower Manhattan on October 29, 2012. NYULMC is located in the dark area. Photographer: Iwan Baan, Getty Images News/Getty Images.

Because the business of research increasingly relies on centralized cores, Sandy's impact on the NYULMC cores' ability to conduct normal business operations could have had far-reaching consequences. Having business continuity plans in place allowed the cores to carry on the business of research and to start providing services within 2 weeks of Sandy, despite the fact that two-thirds of the NYULMC cores was forced to shut down.

While no one plan can address all possible risks, each institution must take its unique characteristics into account when developing disaster and business continuity plans, existing industry standards and review of best practices can assist core administrators, directors, and staff as they develop their own plans. We provide a brief overview of industry standards and suggestions for the development of core-specific plans, drawing upon real-life lessons learned from the response and recovery of cores at NYULMC in the aftermath of Superstorm Sandy.

DISASTER PLANNING

Best practices for disaster planning include conducting thorough risk assessments, undertaking mitigation activities, such as relocation of research assets from high-risk areas, and developing and testing response strategies and recovery plans, including preparing for extended disruption of critical infrastructure. As an aftermath to the sustained damage academic institutions have suffered following severe weather events such as Katrina and Sandy, it is now commonplace for institutions to have emergency planning and business continuity offices.

For a number of regulatory and business reasons, colleges and universities have developed and maintained disaster plans for decades.^{4–7} After 9/11, the college and university community embraced comprehensive emergency

management planning approaches, and following issuance of Presidential Directive 5 in 2003, colleges and universities seeking federal funding for preparedness activities are required to adopt FEMA National Incident Management System (NIMS)-based approaches to disaster planning.^{8, 9} Most larger institutions now have dedicated emergency management departments whose primary role is ensuring that the institutions are best situated to minimize the negative consequences of emergency and disaster challenges. All institutions have staff members that, even if not involved in formal disaster planning, are responsible for emergency response on some level.

In summary, disasters are events that prevent the organization from carrying on normal business operations. Disaster planning is needed to help ensure that damages and losses are minimized. Business continuity planning is needed to address extended disruptions of normal business operations. Disaster and business continuity planning are based on four of the following key steps: preparedness, mitigation, response, and recovery (Fig. 2). There are similarities and a predictable need for overlap and transition between disaster and business continuity plans. However, the plans serve different purposes, do not necessarily require activation of one for activation of the other, and are not substitutes for each other.

Below we discuss the basic approach to and elements of an "all-hazards" institutional disaster plan. We strongly encourage the reader to avail themselves of the extensive literature and government and public and private agency guidance and assistance available (see Table 1) and to consult with their institution's emergency management department or committee to familiarize themselves with the plans and procedures already in place at their institution.

DISASTER PLAN PRIMER

The primary purpose of a disaster plan is protection of life, health, and institutional assets and enabling an effective and efficient return to normal operations. No single plan can predict and account for all the possible emergency and disaster scenarios, but an all-hazards plan, coupled with effective risk assessment (also referred to as hazard vulnerability assessment or HVA), should equip an institution to respond to any emergency/disaster.

The group or committee that develops a new or enhances an existing disaster plan should include representation from senior leadership, security/public safety, physical facilities, environmental health and safety, human resources, student administration, finance, materials management, and faculty. A key first and periodically repeated step is assessing risks that the institution may face. This process helps identify gaps in current preparedness, mitigation, and response capabilities and allows the

FIGURE 2

Phases of emergency preparedness and business continuity.

institution to set priorities for closing gaps and strengthening its capabilities. There are a number of approaches that the committee can use to evaluate and weigh the types of hazards that the institution is most likely to face, how disruptive the event could be, and how well the institution is prepared to address them. The Kaiser Permanente HVA is commonly used and is easily modified to align with the needs and characteristics of your institution.¹⁰ A sample of the HVA template is available for download as a planning resource. Because the HVA is a subjective process, it is important that the committee conducting the assessment include individuals with broad institutional knowledge and functional expertise.

During the process of developing and/or reviewing the disaster plan, the committee should remember and convey to the community that the goal is not to have multiple long, detailed incident-specific plans but rather to identify and rely upon the institution's existing leadership and decision-making capabilities and resources to address any emergency or disaster. The plan should contain the following major elements:

Notification and communication—Robust and reliable communications systems and processes are essential to effectively managing in any disaster situation. For the purposes of this plan, communications include the following three primary components: 1) telecommunications, which refers to the physical technology to be used; 2) emergency communications, which refers to the methods and protocols for coordinating disaster operations and disseminating life safety alerts; and 3) informational messaging, which includes all processes used to convey important information to a wide range of stakeholders and audiences. Making sure that the right

information gets to the right people in time is essential to avoiding, responding to, and recovering from disasters. This section of your plan should describe the methods and means by which institutional leadership and emergency response personnel would alert the community to an emergency or disaster and how they would provide and maintain ongoing communication. Institutions should and do use multiple communication tools (e.g., life safety systems such as fire alarms, public address systems, phone, web-based, email-based, radio broadcast, sirens, and social media). Institutions that must comply with the Clery Act,¹¹ as well as many others, use internal and third-party emergency notification systems that allow for simultaneous notification of all members of the institution on multiple devices and carriers.¹² Electronic methods provide obvious advantages, but it is key to remember that these systems may be unavailable as a result of the emergency/disaster. As a consequence, the notification and communication section should also describe how the institution would use more basic tools such as phone trees, two-way radios, paper postings, and messengers. During and following the events of Superstorm Sandy, all ultra high frequency (UHF) systems supporting NYULMC failed because of catastrophic power loss and water damage. As a result, NYULMC was without all telecommunications, power, and lighting. On the institutional level, texting and cell phones were indispensable for establishing communications for those first few days until telecommunication systems were restored. In addition, an NYULMC Twitterfeed was established, allowing rapid deployment of volunteers for Sandy recovery efforts, and a twice daily incident command

TABLE 1

Resources and links related to disaster planning, business continuity and development of standard operating procedures for colleges, universities, and research institutions

Focus	Source	Title	URL
Emergency management	FEMA	Building a Disaster-Resistant University Handbook	https://www.fema.gov/media-library/assets/documents/2288
	FEMA	Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education	http://www.fema.gov/media-library/assets/documents/33597
	U.S. Department of Education	Action Guide for Emergency Management at Institutions of Higher Learning	http://rem.s.ed.gov/docs/rem.s_ActionGuide.pdf
	American Red Cross	ReadyRating	http://www.readyrating.org/
	National Fire Protection Association	NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs	http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600
	National Association of College and University Business Officers (NACUBO)	Emergency Preparedness	http://www.nacubo.org/Business_and_Policy_Areas/Risk_Management/Campus_Security/Emergency_Preparedness.html
	Disaster Resilient Universities (DRU) Network	DRU Network Listserve	https://lists.uoregon.edu/mailman/listinfo/dru
Business Continuity	Department of Homeland Security National Protection and Programs Directorate and FEMA	Business Continuity Planning Suite	http://www.ready.gov/business-continuity-planning-suite
	KualiCo	Kuali Ready Continuity Planning	https://www.kuali.co/products/continuity-planning/
Standard Operating Procedures	Regents of the University of California	EH&S Directors Leadership Council "Standard Operating Procedures"	http://ucanr.edu/sites/ucehs/Lab_Safety_Training/Administrative_Controls/SOP/
	U.S. Environmental Protection Agency	Frequent Questions—Standard Operating Procedures (SOPs) and Guidance for Preparing Standard Operating Procedures (SOPs) EPA QA/G-6	http://www.epa.gov/quality/faq7.html ; http://www.epa.gov/quality/qs-docs/g6-final.pdf
	Food and Drug Administration	Good Laboratory Practice for Non-Clinical Laboratory Studies. Title 21, Part 58	http://www.ecfr.gov/cgi-bin/text-idx?SID=0f90bdc6a2a75757c0d7e6a0f7a2da24&mc=true&node=pt21.1.58&rgn=div5

session was held for the NYULMC research community. In the early days after Sandy, incident command meetings were conducted by bullhorn in a windowed corridor for lack of power or heat in the auditoriums.

Establishment of an incident command structure and procedures for activating the plan—An institution should determine under what conditions and by whom the disaster plan may be activated. Most emergencies do not require activation of the full disaster plan, but it is important to identify who has authority to activate the plan so that response time is not wasted on consensus

building. The incident command structure, a formal management hierarchy, clarifies how information and directions will flow both within the institution and between the institution and outside agencies and organizations while the institution is operating in disaster mode. In general, the incident command structure varies from the normal organization structure, in that the incident commander, who is quite often the head of security/public safety, is at the top of the chart. The rest of the departments that have defined roles under the institutional disaster plan are typically divided into

functional areas of operations, planning, logistics, and finance/administration.

Establishment and operation of a command center—To facilitate both internal and external disaster response communication, it is prudent to establish a command center where key response personnel can convene. Ideally, the command center is equipped with access to the Internet, television and radio broadcasts, and landline and cellular phone service and is backed up with emergency power. The institution should identify alternate locations for a command center in case the primary command center is compromised.

Guidance for decision makers—Although we recommend an all-hazards plan, it is helpful to provide brief, general guidance for responding to the most common or most likely events to assist the institutional leadership. Elements addressed in this section typically are identified through the hazard vulnerability analysis. This guidance section should not be considered all-inclusive. The specific response actions should be determined by an on-scene situational evaluation with input from key emergency responders. Examples that may be included in this section are the first actions to take in response to a utility failure, active shooter, bomb threat, missing person, high winds, information security breach, and environmental release.

Roles and responsibilities for first responders and decision makers—This section should list the specific disaster-related roles and responsibilities developed for each job title and should clearly identify who does what during an emergency/disaster situation. This should help maximize effectiveness and minimize anxiety/chaos during an actual event.

Identification of essential personnel and alternates—Essential personnel are those that fill roles required to keep critical research, facility, and residential functions operational. It is important to communicate to those in essential roles what the responsibilities will be during a disaster situation well in advance of any emergency, especially given that these employees are likely to be expected to remain on duty and on-site while other employees are released or directed to leave. The institution needs to determine if and how those fulfilling essential roles will be compensated for actions taken during disaster response (e.g., overtime pay, compensatory time off).

Security and traffic control—The plan should describe how the institution will secure its facilities, control pedestrian and vehicular traffic, and shelter or mobilize the community as needed.

Coordination of procedures for obtaining medical care—In an emergency situation, the institution may need to address medical needs on-site, regardless of whether the

institution has on-site medical or occupational health facilities. The plan should address both how the institution will summon medical assistance and facilitate transport of personnel to off-site medical facilities and how injured or ill personnel will be addressed on-site. This section of the plan may also refer to provision of trauma and psychological counseling for affected personnel.

Internal communications and relief information center—Disaster response activities and communication about those activities are controlled by and distributed by the incident response team. The institutional community will also need access to information that is not disaster response related but is still event related and critical. For this reason, the institution should be prepared to set up a relief information center. The relief information center should be designed and equipped to provide employees with assistance for addressing stress and housing and transportation needs.

Public relations and media—The institution should decide in advance who has responsibility and authority for communicating with the press and the public and logistics for handling questions from the public and press (i.e., designated phone lines, designated press areas). The institution should consider crisis communication training for the incident command team and should set a policy that all personnel will direct media inquiries to the department/person assigned responsibility for speaking with the press. This cannot be emphasized too strongly because the media are persistent and will seek information from any and all who will speak with them. During a disaster response, your resources need to focus on response and recovery, not damage control for inaccurate press.

Evacuation procedures—Procedures for evacuating a building in a fire/smoke condition are generally well known and understood. However, under an all-hazards plan, a building-wide evacuation is only one contemplated scenario. This section of the disaster plan should address shelter-in-place, floor-by-floor, multiple building, and even entire campus evacuation scenarios. These should be defined and drilled on a recurring basis.

Return to normal operations—Before employees and students are told to return to their workplaces, the institution has an obligation to ensure that it is safe to return. The institution has a vested interest in ensuring that damages and losses are verified and documented. The return to normal operations should provide procedures for meeting both of these goals.

External disasters, impacts, and role of the institution—Most colleges and universities play important roles in their communities and have been assigned or volunteered

to take responsibility for emergency and disaster response and management for people and facilities beyond their campus. This section should address those responsibilities.

Review, evaluation, and training—This section should describe the methods by which the plan will be reviewed and evaluated and by whom, as well as the training requirements for all members of the institution.

CORE DISASTER PLAN

In a disaster situation, the principle responsibilities for cores, regardless of the services and support provided by the core, are similar [In this article, we exclude specific reference to and recommendations for disaster and business continuity planning for laboratory animal facilities because there are long standing, well-recognized requirements for institutions that conduct laboratory animal research to develop plans to protect animal welfare and preserve animal life when possible during emergencies or other conditions that compromise animal care.]^{13–17}

The key elements for a core disaster plan are indicated as follows.

Notification and communication—Having the ability to contact and communicate with key personnel is essential, and taking steps to ensure that you can is a high, if not the highest, priority.

Audience

Staff: primary, secondary, and alternate/back-up contact information (mobile and land numbers); institutional and personal e-mails; spouse, parent, and significant other contact information

Critical vendor and support service contact information.

Customers: ensure timely information regarding the status of your operations and what services/products they can and cannot obtain. For this purpose, it is helpful to create and maintain email lists.

Medium: often dictated by availability, so have several options!

Content: KISS (keep it short and simple).

Frequency: more often in the beginning until a routine is established or changes.

Self-rescue by staff—Core staff may not typically be involved in first response activities and will best support the first responders by getting themselves out of harms' way. The core disaster plan should include procedures for evacuating and accounting for staff. [Remember that evacuation is recommended in many but not all situations (*i.e.*, in the event of a tornado or earthquake, sheltering in place is recommended).] If an area of refuge is not assigned by the institution, the core director and staff should agree on an area that they will

convene in the event they must evacuate the building. Ideally, an area of refuge is located inside (to provide shelter from weather and assist with traffic control) a building remote from the incident affecting the evacuated building. Once at the area of refuge, the core staff should conduct a "head count." The core director or designee should alert security whether all core staff is accounted for or not. This will assist the responders who need to know whether people may still be in the affected building.

The core disaster plan should also consider the possibility that a staff member may have a vision, hearing, or mobility disability that hinders the ability to self-rescue and may therefore need assistance to evacuate the building or may need to be sheltered in place until responders can arrive to assist. Remember that not all disabilities are obvious or permanent (*e.g.*, someone may have short-term ambulatory restrictions because of an injury or surgery).

Roles and responsibilities for first responders and decision makers—For each core, specific disaster-related roles and responsibilities should be developed for each job title, clearly delineating expectations during an emergency/disaster situation. This will help maximize effectiveness and minimize anxiety/chaos during an actual event.

Identification of essential personnel and alternates—Every role should have a named alternate in the event of staff absence (vacation, sick leave). As most cores are run in a lean model, assigned essential duties may overlap, which is better than gaps in coverage.

Securing facilities prior to evacuation—If the condition calling for evacuation does not present immediate threat to life or health, the core staff should implement procedures for shutdown and securing of instrumentation, equipment, hazardous operations, and critical document/data backup. Every core should have these procedures at the ready for a shutdown. The institutional incident command team will have provided information on expected length of interruption to business. Therefore, it is best to have a staged plan for securing costly instrumentation and equipment for both extended and short-term interruptions, including critical document/data backup and/or retrieval.

Following directions of the incident commander and institutional leadership—In disaster situations, those responsible for the overall institutional response will set the priorities for how and when employees may return to the workplace. As frustrating as it may be to be told to remain off site, that is exactly what you need to do if so directed. The first priority of essential personnel will likely be reestablishment of infrastructure and safe work conditions. In such a situation, any concerns, questions,

or requests regarding the condition of or accessing the core should be presented to the incident commander using the procedures established under the institutional disaster plan for internal communications.

Return to the workplace—Upon return to workplace (post “all clear” that it has been deemed safe to return), the core staff should evaluate and document any damage and losses and provide reports about these to leadership (*e.g.*, research administration, finance, risk management). This documentation must include assessment of the dollar value of the damage or losses for insurance purposes.

Reestablishing operations—In the best case scenario, reestablishing operations will be as simple as turning on lights and repowering instrumentation; however, based on the extent of damage and how long the core was shut down, you will likely need to implement a business continuity plan to address the loss of staff, utilities, instrumentation, equipment, and/or supplies.

BUSINESS CONTINUITY

Planning for business continuity, defined as the institution’s ability to maintain or restore its business and academic services when some circumstance threatens or disrupts normal operations, requires a collaborative and integrated campus approach in which each institute, department, or institutional organization understands the role it will play in restoring services, managing the crisis, and returning to normal operations.

In many ways, cores are small businesses that commonly are operated under the umbrella of a centralized core administration. To be successful, core directors and managers must keep their business running on a daily basis despite all the various exigencies and impediments that arise even in the absence of a disaster. Although this may not be formally acknowledged as business continuity planning, it is business continuity. What seems new is the recognition that academic institutions and research centers are also businesses that need to engage broadly and seriously in business continuity planning. Good planning requires that key stakeholders work together to assess risk, prioritize work, and engage other campus units. When done well, planning also develops understanding across campus units, builds relationships, and fosters confidence.

The good news is that most of the elements needed for a strong business continuity plan flow out of good work practices that strengthen overall operations. The bad news is that it does not take a full-blown disaster to create a need to implement a continuity plan. Staff shortages can arise at any time (*e.g.*, staff quit, retire, are terminated, get sick, or take extended medical leave or vacations). Instruments may fail,

computers may crash, reagent shortages may arise, or funding may run out at any time.

BUSINESS CONTINUITY PLAN PRIMER

Business continuity plans are playbooks for how to operate if key staff, infrastructure, utilities, and/or materials are interrupted and remain unavailable for an extended period of time. Developing a good business continuity plan requires a close look at what is needed to deliver at least the minimum level of service and functionality required to support the research enterprise. It should be specific to the cores, support and also be supported by the institutional plan, and define the roles and responsibilities of the core and core staff.

As with the section on disaster planning above, abundant literature and advice on development of business continuity plans, as well as multiple companies willing to consult, provide, and run plans, are available (see Table 1). Here we present an overview of major elements and considerations for business continuity plans and advice on specific elements and considerations for core business continuity plans. Key elements of business continuity plans include the following:

Identification and prioritization of essential functions and critical processes and services—Essential functions are those that must be conducted even in an emergency to meet the institution’s mission. Critical processes and services are those that support essential functions, and without which the essential function, cannot be maintained. For longer duration events, it is prudent also to identify functions that are of lower priority but still necessary or desirable. Doing so will assist you and leadership to determine the overall priorities for response and recovery efforts. Advance thinking on how to mitigate the effects of staffing shortage, equipment, or infrastructure failure can help not only following a disruption to operations but also in the process of business continuity planning (Fig. 3A and B).

Identification of critical infrastructure support—Determining in advance what operations will be affected by infrastructure failures or loss will help you set priorities and respond more quickly to the failure or loss. This assessment is basically asking which operations can continue to run with limited or no staff, electricity, natural gas, vacuum, reverse osmosis water (RO), cooling, heating, internet, computers, procurement, or other financial systems, etc. (Fig. 3C).

Notification and communication—Procedures for effective communication are just as essential for business continuity as for disaster planning. Systems for getting appropriate information to others within your institution and to your essential suppliers should be developed. During a period when it is not “business as usual,” ensure

A IDENTIFYING MITIGATION STEPS TO ADDRESS STAFFING SHORTAGE

Critical Function/Service	Effect of Staffing Shortage/Staff Expertise Absence	Mitigation Actions
		A)
		B)
		C)
		A)
		B)
		C)

B IDENTIFYING MITIGATION STEPS TO ADDRESS EQUIPMENT FAILURE

Critical Equipment	Effect of Failure	Mitigation Actions
		A)
		B)
		C)
		A)
		B)
		C)

C IDENTIFYING IMPACTS OF INFRASTRUCTURE FAILURE/LOSS

Service/Process	Service/Process Requires the Identified Utility/System:								
	Electricity	HVAC	Natural Gas	Refrigeration	Compressed Air	Vacuum	Water	Intra-/Internet	Others (e.g., RO Water, Telephone)

D EVALUATING REMOTE OPERATIONS CAPABILITIES

Staff Position/Name	Appropriate Computing Hardware/Software?	Broadband Internet Capability?	Can Access VPN? Can Access Business Files through VPN?	Can Access CFS Remotely?	Cell Phone?	Smartphone with E-mail Capability?	Private E-mail Account Address?	Comments

FIGURE 3

Checklist of steps to take when faced with staffing shortage (A), equipment failure (B), and infrastructure failure and loss (C), and evaluation of remote operations capabilities (D).

that the key stakeholders get information about the status of your operations and what services/products they can and cannot obtain. For this purpose, it is helpful to create e-mail lists for your key stakeholders and for your full set of users.

Staff responsibilities—Identifying which personnel will take on which responsibilities in advance should help you highlight where additional training and/or cross-training will be beneficial. This section should also identify which responsibilities can be delegated and to whom.

Cross-training of staff—Ensure that all staff members are familiar with critical steps for essential operations and with locations of critical equipment, files, and information. This will help immensely in dealing with unexpected events and staff shortages in general. The logical starting position is to have staff members within a core cross train each other. For greater resiliency, consider cross-training staff between cores.

Inventory of instrumentation/equipment—In many cases, cores house the majority of instrumentation for the institution. An accurate inventory is essential, particularly if there is a disaster and this information is needed for FEMA, U.S. National Institutes of Health (NIH), and insurance documentation. Although many institutions

now maintain a centralized inventory of all instruments and equipment, it is the responsibility and to the advantage of the core administration to ensure that this information is current. Document each instrument, piece of equipment, including computers and accessories, and catalog:

Vendor name

Description

Make/model number

Asset tag number

Photograph (helps to establish proof of ownership)

Other supporting documentation to prove ownership (e.g., invoices, purchase orders, maintenance logs, service contracts, warranties)

This inventory should be considered a living document, with regular review and revision to include new and retired instrumentation and equipment. At the minimum, this document should be reviewed for accuracy annually.

Inventory of all valuable consumables/supplies—Similar to an instrument/equipment inventory, an accurate inventory of valuable consumables/supplies is essential for insurance reasons and for determining which services can be supplied and for how long. The inventory of supplies should include the following:

Vendor name

Description, including quantity of reagents in containers

Lot number

Expiration date (shelf life)

Photograph (should illustrate quantities clearly as listed within the inventory; this is important for establishing reagents/supplies on hand)

Documented standard operating procedures (SOPs)—

Detailed written instructions describing the steps, required materials, potential hazards, and appropriate work practices, including those that minimize risk of exposure or injury to personnel are highly desired for a number of reasons, including training, safety compliance, quality control/assurance and are essential for effective business continuity. Advice and guidance on developing SOPs, as well as template samples and examples are available from a number of sources (see Table 1). If your institution has adopted a standard format, you should use that format for the SOPs you develop. The SOPs should be available in electronic and hard copy format, and all staff members should be familiar with the contents of the SOPs and where they are located.

Remote operations capabilities—With appropriate hardware, software, and internet connections, a surprisingly significant number of tasks can be accomplished by staff working remotely. Core laboratory information management system (LIMS) and instrumentation manufacturers increasingly are providing software that supports remote monitoring and use of core instruments. As part of the business continuity planning, you should identify not only which operations can be conducted via remote operations but also your staff's capabilities in conducting remote operations (*e.g.*, what hardware, software, Internet carrier, phone access they have at home) (Fig. 3D) and the institution's capabilities for supporting remote connections (*e.g.*, number of VPN connections). Furthermore, the institution should establish priorities for whom will be granted access during times when there is a broad need for remote operations.

Alternative sources for the core's services—Identify location and contacts for similar instrumentation and services on your own campus, from cores at other institutions, and from commercial sources. If you are unable to resume operations, this will assist you in advising your leadership and users on where they can obtain similar services.

Mutual aid agreements—A mutual aid agreement is a prearranged understanding between entities to provide help to each other if their business operations are disrupted. The fact that NYULMC cores were providing services to investigators within 2 weeks of Superstorm Sandy decimating NYULMC and the buildings that the

cores occupied was attributed to the welcoming partnership extended by The Rockefeller University, Memorial Sloan Kettering, Mount Sinai School of Medicine, Weill Cornell Medical Center, Rutgers University, and the New York Genome Center. With regard to colleges, universities, and research institutions, mutual aid agreements are predicated on the acknowledgment that one institution may not have all the resources needed to respond to an incident and may include provisions for requesting or providing use/loan of facilities, equipment, or personnel in a variety of disciplines, including police, human resources, and crisis communications as well as direct access to resources at the other institution and/or from government agencies. It is common, and in some cases required, for colleges and universities to have established mutual aid agreements for police, fire, and medical emergency support. Less commonly, they may have established mutual aid agreements for teaching, student services, and research operations.

Alternate sources for supplies—In today's global economy, crises and events far remote from your institution can still have significant impacts on your operations. For example, the impending (but now delayed) close of the National Helium Reserve in 2013 raised concerns around the ability to operate magnetic resonance imaging, NMRs, and many other instruments (and obtain party balloons) throughout the United States.¹⁸ In the research world, sole source options are common, and the desire to minimize research variables means, in many cases, relying upon a single vendor. However, whenever possible, you should identify alternate sources for services and supplies. An added benefit from this process may be finding or negotiating a better price for these services and supplies.

Critical vendor and support service contact information—Find and document the names, addresses, phone numbers, e-mail, and web addresses for the vendors and service companies that provide supplies or service for your critical operations. Keep this list in a hard copy and electronic format. If known, include the names of the personnel that provide on-site service and any direct contact information for them.

Data storage and backup—Document where data are stored, the method, and frequency with which backups of data are conducted, and instructions for retrieving data from backups.

Status review and reporting—For internal departmental purposes, daily status review and reports to the core administrator should be conducted. This will help assess the effectiveness of the business continuity plan, identify new issues, and help determine whether priorities need to be adjusted or assistance is needed. If the event affected

the larger institution or area, it is likely that departments will be asked to provide status reports on a frequent basis to the leadership. These may include data on usage and billing that the institution will need to meet obligations to its funding agencies.¹⁹

If the need to implement the core business continuity plan arose in the context of a larger scale challenge facing the institution, it will be important to follow the direction of the institutional leadership, even if you are directed to remain off-site. It will be likely (and frustrating to you as you sit at home worrying about samples thawing or instrumentation failing) that resumption of operation of the cores is not one of the early top priorities, but that does not negate the need to develop plans for implementation at the time that leadership does call for the start-up of operations. In most instances, the need for contingency operations will be for reasons that affect a narrower range of institutional operations and facilities, and most likely, it will be for those that affect only your core.

PLAN TEMPLATES

The core facility disaster plan template provided in Appendix 1 is based on departmental plans developed and used at The Rockefeller University over the last 12 yr.

The format of the core facility business continuity plan template provided in Appendix 2 is based on plans under development at The Rockefeller University and lessons learned at NYULMC.

CONCLUSION

In recent years, research institutions and biomedical centers have suffered significant losses to research because of severe weather and other disasters. Unfortunately, severe weather events are becoming more commonplace, and Superstorm Sandy brought climate impacts and risk into the conversation in ways not even contemplated before this October 2012 event. Today, NYULMC has implemented a robust disaster response plan, an efficient incident command office, and has gratitude for our colleagues and friends who supported us in our time of need.

From a biomedical research enterprise perspective, the business of research increasingly relies on centralized resource centers/cores, making them a critical and highly vulnerable component because of the concentration of instrumentation and resources. By the time Sandy hit Manhattan, the NYULMC cores had implemented their disaster response shutdown, and all cores were secured for an anticipated 1-d interruption to business operations. However, no one anticipated the extent of damage that Sandy caused to the buildings and services, the essential infrastructure for medical and research operations. As such, research recovery was a lengthy and staged process. The first

response focused on immediate needs—most urgent was preservation of the research and clinical samples at risk in rapidly thawing freezers, followed by relocation of researchers from damaged laboratories to short-term locations. In all, the contents of 1100 freezers, 800 scientists, and staff from 90 research laboratories and 12 cores had to be physically relocated into significantly less space and then relocated again as infrastructure repairs were completed. The second phase was documenting losses, followed by a final phase of systematically replacing losses. Three years later, we are close to completing the final phase. However, the lessons learned can be distilled to the following:

1. Communication is the most frequent point of failure—Having primary and secondary contact information for staff, vendors, and suppliers is essential, and the information should be updated frequently. After Superstorm Sandy, NYULMC telecommunication systems were disrupted for an extended period of time. Having the cell number of every core staff member allowed communication across all cores via text messaging. On the institutional level, texting and cell phones were indispensable for establishing communications, as was the twice daily meetings convened by the incident commander. Keep your customers informed and updated during all phases of recovery via text, e-mail, Twitter, and website.

2. Know your inventory—Annual review of the following enables quick decisions (see **Fig. 4** as an example): list of instrumentation/equipment; identification of critical infrastructure; data storage locations/backup; list of essential responsibilities and/or services; alternate sources of your services (internal, external); alternate sources for your supplies; and off-site copies of critical contact information.

3. Know your MINIMUM location requirements—Faced with significant infrastructure damage, the majority of the NYULMC cores had to be relocated. This meant that we needed to know our minimum space, HVAC (heating, ventilating, and air conditioning), and power requirements to continue operations. Having a complete and detailed inventory facilitated rapid relocation and a return to business operations.

4. Plan for the unexpected (have a plan B)—Eighty percent of NYULMC cores was shut down because of infrastructure loss, and yet 50% was providing services 2 wk after Sandy and 86% was operational 1 mo after Sandy. This was only possible through our network of colleagues at The Rockefeller University, Memorial Sloan Kettering, Mt. Sinai School of Medicine, Rutgers University, Weill Cornell Medical College, and the New York Genome Center. Have SOPs for core service operations, and cross-train staff to facilitate flexibility; and network and collaborate across cores, inter- and intrainstitutionally, and establish contacts with commercial options; establish mutual aid agreements

Instrument/equipment inventory and infrastructure requirements.

7. Implement an institutional cold storage policy—Although 100% of biospecimens in the NYULMC BioRepository was stored securely off-site, the majority of NYULMC investigators had on-site research collections. These collections were the biobanks of their careers and the basis for new research and grants. Biostorage & Cryostar facilitated emergency retrieval and relocation of more than 1 million biospecimens held in 1100 freezers from both clinical and research operations. Off-site storage of all precious biomaterials is now a priority, ensuring research continuity for resources and protecting samples for future awards and collaborations.

The authors thank Judy C. Stribling for her assistance and support on literature and reference searches, and manuscript preparation, and the RU and NYULMC core directors and staff for their contributions and commitment. The authors declare no conflicts of interest.

1. Eisenhower DD. Remarks at the National Defense Executive Reserve Conference. 1957.
2. Fishell G. Hurricane Sandy: After the deluge. *Nature* 2013;496:421–422.
3. Pulliam JK, Roble GS, Raymond MA. Emergency planning: Be prepared. *Nature* 2014;514:430.
4. Disaster Mitigation Act. 2000. 42 USC 5121. *Public Law* 2010;106–390.
5. U.S. Government Publishing Office. Electronic Code of Regulations. Title 44: Emergency management and assistance. Available at <http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=44:1.0.1.4.53>; Accessed October 13, 2015.
6. U.S. Government Publishing Office. Code of Federal Regulations (Annual Edition). 29 CFR 1910.38—Emergency Action Plans. Available at <http://www.gpo.gov/fdsys/granule/CFR-2013-title29-vol5/CFR-2013-title29-vol5-sec1910-38>; Accessed October 13, 2015.
7. U.S. Government Publishing Office. Code of Federal Regulations (Annual Edition). 40 CFR 262.34—Accumulation time. Available at <http://www.gpo.gov/fdsys/granule/CFR-2011-title40-vol26/CFR-2011-title40-vol26-sec262-34>; Accessed October 13, 2015.
8. Bush GW. Management of Domestic Incidents. Homeland Security Presidential Directive-5. Washington, DC. 2003. <http://www.dhs.gov/publication/homeland-security-presidential-directive-5>
9. National Incident Management System (NIMS). <http://www.fema.gov/national-incident-management-system>. Accessed September 28, 2015.
10. California Hospital Association. Hazard Vulnerability Analysis: Kaiser Permanente HVA Tool. <http://www.calhospitalprepare.org/hazard-vulnerability-analysis>. Accessed September 28, 2015.
11. U.S. Government Publishing Office. Code of Federal Regulations. 34 CFR 668.46—Institutional security policies and crime statistics. Available at http://www.ecfr.gov/cgi-bin/text-idx?SID=0da211174b824fb7eb135d45a588e05b&mc=true&node=se34.3.668_1468&rgn=div8. Accessed January 24, 2016.

12. Ebersold P. Amassing mass notification know-how. *Campus Safety Mag.* June 2011. <http://www.campusmagazine.com/article/Amassing-Mass-Notification-Know-How>. Accessed September 28, 2015.
13. Vogelweid CM. Developing emergency management plans for university laboratory animal programs and facilities. *Contemp Top Lab Anim Sci* 1998;37:52–56.
14. National Institutes of Health Office of Laboratory Animal Welfare. 2002. *Institutional Animal Care and Use Committee Guidebook*, 2nd Ed. p. 71–81. National Institutes of Health, Bethesda, MD.
15. Roble GS, Lingenhol NM, Baker B, Wilkerson A, Tolwani RJ. A comprehensive laboratory animal facility pandemic response plan. *J Am Assoc Lab Anim Sci* 2010;49:623–632.
16. Swearingen JR, Vargas KJ, Tate MK, Linde NS. Disaster preparedness in biocontainment animal research facilities: developing and implementing an incident response plan (IRP). *ILAR J* 2010;51:120–126.
17. National Research Council. 2011. *Guide for the Care and Use of Laboratory Animals*, 8th Ed., p. 35. National Academy of Sciences, Washington, DC.
18. Reisch MS. Coping with the helium shortage. *Chem Eng News* 2013;91:18–19.
19. NIH Extramural Response to Natural Disasters and Other Emergencies. http://grants.nih.gov/grants/natural_disasters.htm. Accessed September 24, 2015.

Appendix 1

Institution Name

Core Facility Name Disaster Plan [year]

INTRODUCTION

The purpose of this plan is to outline the duties of the [CORE FACILITY NAME] in the event of a disaster. It is imperative that throughout an emergency situation, routine activities be maintained to the greatest extent possible, in order to ensure that the needs and safety of faculty, students, staff and visitors are maintained.

[CORE FACILITY NAME] staff is not responsible for emergency first response actions. These actions will be undertaken by institutional emergency response departments as outlined in the institution's Disaster Plan and in those individual emergency response departments' plans.

The primary responsibilities of the [CORE FACILITY NAME] during a disaster are:

A. Appropriate evacuation and accounting of staff members.

B. Notification of staff, including those who are off-site at the time of the disaster.

C. Shut down of critical instrumentation, equipment and operations (e.g., equipment that could potentially become unsafe if left running unmanned or could potentially be damaged if left on).

NOTIFICATIONS

Once an on-scene decision has been made to activate the Disaster Plan, written instructions will be developed and the information communicated via telephone or fax to each area. If the telephone system has been compromised, the information will be distributed by hand. Notifications to the

[CORE FACILITY NAME] will be made by the [ROLE OR DEPARTMENT ASSIGNED TO NOTIFY THE CF UNDER THE INSTITUTIONAL PLAN] according to the institution's Disaster Plan. Notification to the [CORE FACILITY NAME] staff will be made by the Director or designee as follows:

[Once your department has been notified that a disaster situation has been declared, how and by whom will members of your department be notified?]

A. During regular working hours (8 AM to 5 PM, Monday–Friday), the employee of the [CORE FACILITY NAME] who receives notification will relay communication to all employees who are present in the CF.

B. During Off hours (second and third shifts, weekends, holidays), employees of the [CORE FACILITY NAME] will be contacted by telephone/email. (See Appendix A)

Shared Resource Core FUNCTIONS

In a disaster situation, it is the responsibility of the [CORE FACILITY NAME] to fulfill the following functions:

[This section should describe in detail, the functions of your core facility during a disaster situation. Your text should address how normal activities will be provided (or modified), as well as your core facility's role/response during a disaster situation.]

A. **Laboratory Activities**—Identify critical processes in each area and establish emergency shutdown procedures (including scheduling, modification, control of information and transportation).

B. **Staff Activities**—notification, housing, transportation.

C. **Staff Family-Support Activities**—assisting staff with child, elder and/or pet care emergency arrangements; e.g., providing phone access, privacy and time allowance away from designated responsibilities to make personal arrangements.

D. **Logistics of critical supplies**—Identify critical supplies needs, (pharmaceuticals, medical, food, water supplies, laboratory supplies) and communicate those needs to the command center.

E. **Core Chain-of-Command**—Identify a chain of command and avenues of communication. [This section typically uses an organization chart, populated with titles, not names, to illustrate the chain-of-command.]

F. **Evacuation Procedure**—Follow the institution's evacuation plan. Once you have evacuated the building, proceed to the designated Area of Refuge for your building, which is [insert location of the assigned Area of Refuge]. Special attention should be given to individuals with disabilities.

G. **Removal/Relocation of Materials**— [This section will address the order and methods of removing materials/equipment and will note that: At all times priority should be given to the safety of human life. In the event of a disaster where the threat is immediate, consideration of

safety and evacuation should be given to human life first, and only after the area of disaster/emergency has been deemed safe by the Incident Commander or the outside agency Incident Commander, may the removal of lab animals and then the removal of materials/equipment be carried out. If the disaster does not pose immediate threat to life or safety, arrangements can be made for the removal of animals and critical materials/equipment in coordination with the Incident Command team].

H. **Personnel Tracking**—One or two individuals should be identified as coordinators and monitors of persons moving to and from the area of refuge.

I. **Management of Personnel Necessities**—Establish the order and methods of moving medications, records, etc., to and from the area of refuge.

J. **Interdepartmental Communication**—Develop avenues of communications between the organization and the area of refuge.

K. **Special Requirements for Animals**— [This section will include guidelines for the safe removal of animals and address their special needs and will include predetermined safe areas established for the keeping of animals during an emergency/disaster situation, procedures for the care of such animals during the emergency and methods of transportation, *e.g.*, location of transportation cages, water, and food and other items needed for the animals' care].

L. **Process to Return to Normal Operation**—Following the "all-clear" signal, notification that it is safe to return to the building will be made to each department according to the same outline in the institution's Disaster Plan document.

PERSONNEL ROLES

[This section addresses "who does what" during a disaster response, for each job title within your department. You must also address (a) assignment of available personnel during emergencies to cover all necessary staff functions; and (b) alternate roles and responsibilities of personnel during emergencies]

REPORTS AND RECORDKEEPING

The [DESIGNEE] will be responsible for maintaining records during a disaster situation.

EVALUATION

As soon as is feasible after the resolution of a disaster situation and return to normal operation, all staff who were involved in disaster operations will report to their department offices for a debriefing session with their department manager. Department managers will provide a written evaluation of the disaster response (from their department's perspective) to the Disaster Coordinator, for review, discussion and follow-up.

TRAINING

The [CORE FACILITY NAME] will provide an orientation and education program for personnel who participate in the disaster response, addressing:

- A. Specific roles and responsibilities during emergencies;
- B. The information and skills required to perform duties during emergencies;
- C. The backup communication system used during emergencies; and
- D. How supplies and equipment are obtained during disasters or emergencies.

APPENDIX A

[CORE FACILITY NAME]

Emergency Contact Information

NAME	TITLE	PHONE(S)	EMAIL1	EMAIL2
------	-------	----------	--------	--------

Appendix 2

Institution Name

Core Facility Name Business Continuity Plan [year]

INTRODUCTION

The purpose of this plan is to outline the process and procedures to minimize disruption and allow maximum provision of the Core Facility's services and support following an incident that renders normal operations not possible. As with the disaster plan, it is imperative to ensure that the needs and safety of faculty, students, staff and visitors are maintained.

In order of priority, the [CORE FACILITY NAME] will provide the following services and support as soon as possible following a disrupting incident. Status of required infrastructure may require reordering the order of priority. As recovery proceeds, the [CORE FACILITY NAME] will resume other activities as possible:

Critical services and support (*list as many as you identify*):

- 1.
- 2.
- 3.
- 4.

NOTIFICATIONS

Once an on-scene decision has been made to activate the Business Continuity Plan, follow the Disaster Plan procedures for notification of staff.

ASSESSMENT OF CORE FACILITY STATUS

Once your emergency coordinator has determined that it is safe to enter the Core Facility, the Director will tour the facility to determine extent of and document damage and

losses. Following review of utility and infrastructure status, staff availability, and available supplies, the Director will determine which functions can be undertaken, with priority given to establishing the critical services and support identified above when possible. For those functions that cannot yet be reestablished, the Director will determine if the institution should seek alternative sources, such as from other internal core facilities or departments, other institutional core facilities, or commercial sources.

INITIATING AND SUSTAINING WORK ACTIVITIES

Critical Service/Support 1

Staffing: List the principal staff and their roles. Identify alternate staff, if available, that are trained to perform the role. If the task can be performed remotely, describe whether and which staff has the appropriate hardware, software and internet connections to work remotely.

Instruments: Describe which instruments are involved, whether they are under service contract, warranty, and whether there is redundancy for the instruments.

Utilities: List which utilities (*i.e.*, electricity, gas, vacuum, house air, HVAC, water, RO water, Internet, etc.) are required for the service.

Supplies: Identify the needed supplies and estimates of amounts/volumes needed (*e.g.*, amount/volume per run, day, week). Include the amount/volume generally ordered and maintained in inventory in order to evaluate the minimum and maximum time the service can be provided should the vendor be able to deliver additional supplies.

SOPs: Maintain both electronic and hardcopies and make sure that staff know where both are located.

Backup: If available, describe when backups are conducted and how to retrieve files, if needed.

Internal alternative resources: List other occurrences of needed staff expertise, instrumentation, and supplies that are present at your institution and contact information for the person(s) with whom you will need to coordinate if any of these are to be used (Appendix C).

External alternative resources: List other core facilities at other institutions that could provide the same service/product. Provide contact information of that core facility. If commercial alternative exist, provide contact information for them (Appendix C).

Repeat for additional Critical Service/Support

APPENDIX A

[CORE FACILITY NAME] Staff

Emergency Contact Information

NAME	TITLE	PHONE(S)	E-MAIL1	E-MAIL2
------	-------	----------	---------	---------

APPENDIX B

Vendor information for critical supplies/service

Vendor	Contact Information	Critical Supplies/Service	Contract Terms for Response	
			Time or Mutual Aid	Alternative Source

APPENDIX C

Alternative sources for services/support

Service/Support/Instrument	Department/Company	Contact Information	Access Information	Mutual Aid Agreement?
----------------------------	--------------------	---------------------	--------------------	-----------------------