SEPTEMBER 2023 EST 1998 MONTHLY EDITION

Domestic Preparedness Journal

REAL-WORLD INSIGHTS FOR SAFER COMMUNITIES

VOLUME 19 ISSUE 9

Business Office: 313 E Anderson Lane, Suite 300 Austin, Texas 78752

Staff that makes this publication possible:

Jasper Cooke - Publisher

Catherine “Cathy” Feinman - Editor

Bonnie Weidler - Publications Liasion

Madison Leeves - Marketing Coordinator

About the Staff

About the Advisors

Cover Design Credit: Madison Leeves.

For more information about the cover please contact us at journal@tdem.texas.gov

Table of Contents


Unsplash/ Lerone Pieters

Michael Breslin

Director, Strategic Client Relations, Federal Law Enforcement, LexisNexis Special Services Inc.

Michael Breslin is a retired federal law enforcement senior executive with 24 years of law enforcement and homeland security experience. He served as the deputy assistant director in the Office of Investigations focusing on the integrated mission of investigations and protection with oversight of 162 domestic and foreign field offices. He served as the event coordinator for the National Special Security Event Papal visit to Philadelphia in September 2015 and was appointed by the Secretary of Homeland Security to serve as the federal coordinator for the Papal Visit to the Mexico-U.S. Border in 2016. He is a member of the Senior Executive Service and is a published author of numerous articles on homeland security, defense, and threat mitigation methods. He serves on the Cyber Investigations Advisory Board of the U.S. Secret Service and is a Board Member for the National Center for Missing and Exploited Children. He also serves on the Preparedness Leadership Council. He has a B.A. from Saint John's University, Queens, NY, an M.S. in National Security Strategy and a Graduate Certificate in Business Transformation and Decision Making from The Industrial College of the Armed Forces; and an MPA from John Jay College of Criminal Justice.

Kay C. Goss

President, World Disaster Management

Kay Goss has been the president of World Disaster Management since 2012. She is the former senior assistant to two state governor coordinating fire service, emergency management, emergency medical services, public safety, and law enforcement for 12 years. She then served as the Associate Federal Emergency Management Agency (FEMA) Director for National Preparedness, Training, Higher Education, Exercises, and International Partnerships (presidential appointee, U.S. Senate confirmed unanimously). She was a private sector government contractor for 12 years, at the Texas firm, Electronic Data Systems (EDS) as senior emergency manager and homeland security advisor and SRA International's director of emergency management services. She serves as a nonprofit leader on the Board of Advisors for DRONERESPONDERS International and for the Institute for Diversity and Inclusion in Emergency Management, and as graduate professor of Emergency Management at University of Nevada at Las Vegas for 16 years, İstanbul Technical University for 12 years, the MPA Programs Metropolitan College of New York for five years, and George Mason University. She has been a Certified Emergency Manager (CEM) for 25 years and a Featured IAEM CEM Mentor for five years, and Chair of the Training and Education Committee for six years, 2004-2010.

Sadie Martinez

Access and Functional Needs Coordinator, Colorado Division of Homeland Security and Emergency Management

Sadie Martinez is the access and functional needs coordinator for the Colorado Division of Homeland Security and Emergency Management. She also serves as the Access and Whole Community Inclusion Caucus chair for the International Association of Emergency Managers (IAEM). Previously, she was the emergency program coordinator and independent living program manager for The Independence Center in Colorado Springs, Colorado, where she trained and advocated for people with disabilities by helping to build personal preparedness for disasters and emergencies, acting as a liaison with local governments, and creating a statewide group of disability-competent emergency coordinators with the governor, members of the legislature, and other public policy makers.

Click here to meet the rest of the advisors

Unsplash/ Anthony Fomin

Always Prepare for the Future, But Never Forget the Past

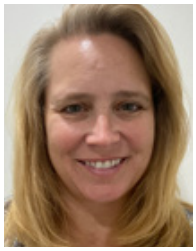
By Catherine L. Feinman

September is a month to remember lives that were lost in the line of duty and prepare for future emergencies and disasters to minimize the consequences and reduce the number of lives and properties that could be lost. Three notable lessons emerged when terrorists attacked the United States on September 11, 2001 (9/11). First, the United States is not immune to terrorist threats on its own soil. Second, interoperability gaps between agencies and organizations must be closed to ensure the safety and security of communities, states, and the nation from domestic and foreign threats – whether they originate from nature, humans, or technology. Third, the physical and psychological effects of a major disaster can have significant lasting effects on those who respond to help.

This September edition of the *Domestic Preparedness Journal* addresses these and other key preparedness efforts that should be considered when planning for future incidents. Reflecting on the events of 9/11, consider the personal costs that emergency responders pay for serving their communities and develop mitigation strategies to reduce those costs. Also, evaluate the organizational changes that have occurred since 9/11 and the gaps that still need to be addressed.

For potential future incidents, consider public-private and interagency collaboration to plan for events that span jurisdictions and ensure that all community members, including vulnerable populations and people with disabilities, are included in those plans. Discover new ways to incorporate existing underutilized resources, such as state defense forces and volunteer groups, as force multipliers.

Anyone with a role in emergency preparedness, response, and recovery has a lot to consider to best protect the communities they serve. Whether preparing for an act of Mother Nature, a public health threat, a violent attack, a cybersecurity threat, or something else, collaboration and coordination across and between communities builds resources and capabilities, supports communities in crisis and those who respond to help, and speeds recovery efforts. During National Preparedness Month and the rest of the year, remember the events of the past and prepare for the future.



Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as Editor of the *Domestic Preparedness Journal*, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and recovery communities. She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Source: U.S. Air Force photo by Staff Sgt. Alexandra M. Longfellow

Responding to the Call - The Cost of Caring for Others

By Mary Schoenfeldt

There is a cost to caring for others, but it does not need to be a lifelong debt that continues to overwhelm not only the people who stepped up but those around them. With the right plan of support and the willingness to explore coping options, that cost is manageable. It becomes an investment with a very positive return rather than a crippling debt that seems never to be satisfied.

Responders of all types bring a level of caring to work with them each day. Most days are typical – the days they trained for, the daily routines they expected when they got dressed to go to work, and their return home as usual at the end of the shift. However, sometimes, it is not a typical day – when a police officer, firefighter, hospital worker, or emergency medical technician (EMT) has the privilege (and the responsibility) of being part of someone else's worst day of their lives. Furthermore, it may be one of those days no one wants to happen, but when it does, these responders step up and step in to give it all they have.

On typical days, professional responders – those giving care (the caregivers) – go to the next call, the next assignment, and the next patient while reflecting on another experience. Again, they leave each call with new thoughts, memories, and maybe mental pictures that seem stuck in their heads and are not easily washed or wished away. They continue their day feeling satisfied that they have done their jobs to the best of their abilities, training, and experience. In other words, they put this call on the shelf with the others they have responded to in the past, with the hope that it gets filed away as just part of the job.

For some reason, responders have the desire and the aptitude to go to these calls for other people. It is what they do and who they are, and the world is thankful for them. Many people understand that this is a job they cannot do. Whether a typical day or an unimaginable one, consider what happens to those experiences, thoughts, memories, sights, and sounds that are a part of the job. The brain is an amazing organ that collects experiences and stores them in "files." Sometimes, the memories and experiences of those they have treated mix with their own lives – their children, parents, neighbors, or friends. That is not to say they always overlap, but they can and often do.

Managing Emotions

At times when leaving a scene, responders think about not only the people they served but also their own families, their own lives, and their communities. For example, a personal family member who is a law enforcement officer responded to a fatal auto accident that involved teenagers. When he left the scene, he called his just-turned-13 teenage daughter to tell her he loved her. She answered the phone in a typical teenage fashion with a brisk "What do you want, Dad? I'm busy!" That was what he needed to hear at that moment, to know that his sassy, charming, sweet, sarcastic daughter was just fine. She was still there and would be there when he got home. That short interaction between dad and daughter helped to put his experience of managing a scene with the bodies of young people into perspective. He had great empathy and compassion for the parents who had lost children, but he also knew it was not his loss. He knew he had done his best that day, but the memory would stay with him forever. Being able to find perspective and balance in professional and personal life is an important factor in managing the emotions that come with any experience, whether acknowledged or not.

Some people run toward danger while others run away. However, disaster responders can bring home more than dust from the rubble.

Some experiences have more impact than others, such as "critical incidents." The World Health Organization (WHO) describes a critical incident as:

> [A]*n event out of the range of normal experience – one which is sudden and unexpected, involves the perception of a threat to life and can include elements of physical and emotional loss. Often such events are sufficiently disturbing to overwhelm, or threaten to overwhelm, a person's coping capacity. Most people would be severely shaken by a critical incident but are likely to recover from its impact with appropriate support.*

A definition used in International Critical Incident Stress Foundation training presentations adds the elements of "sudden, out of the ordinary, perceived as life-threatening to someone you know or involves children." Others would add events that include having to witness or experience tragedy, death, serious injuries, and other threatening situations. The definitions can vary, but all include witnessing or being a part of an emotionally overwhelming event, even if the emotional reaction does not come until later.

Most people who experience a critical event will have some type of reaction within 30 days. Some resources say that can be as high as 85%. Nevertheless, long-term impacts can be mitigated with support and understanding from others and themselves. Some responders tend to second-guess themselves later about what they did or could have done differently. They can blame themselves with thoughts of "I coulda, or I shoulda, or If I woulda done [fill in the blank], things would be different." The reality is that, despite the differences, there are no guarantees that the outcome would not have been the same. Many programs and services are available to help manage these reactions, and the simple acknowledgment in the workplace that the job can be emotionally difficult is helpful.

Responding to Mass Casualty Events

Those who respond to catastrophic events such as 9/11, the Boston Marathon bombing, school shootings, or COVID-19 – especially in the early days when there was so much loss of life – face additional challenges. The impacts of these types of events are complicated by not only the horrific experience itself but also the media attention, political climate, and human response to blame someone (and sometimes, it involves the responders or their agencies who stepped in as everyone else was running away).

When COVID-19 emerged, it was not a single local event. It was a global event, and the magnitude was such that anyone in any country could be at risk of dying and causing the death of others, including loved ones. For those who responded directly to the sick and dying people – doctors, nurses, other medical staff, EMTs, and funeral home workers – it was a frightening,

new experience. For the first time in their careers, those front-line personnel – despite years of training and experience – may not have been able to change the outcomes for those infected. However, in the process of caring for them, they may have been putting their own lives and families at risk of illness or death. Helplessness, exhaustion, and emotionally intense situations magnified what would have been called a critical incident under the best of circumstances.

Targeted violence incidents like school shootings and the Boston Marathon bombing are naturally extreme events that leave carnage in their wake. Carnage to not only the victims and families but also the responders, who often are overwhelmed by the sheer magnitude of the event, the number of people involved, and the sights and sounds of the scene. Neuroscience researchers talk about survival chemicals that protect workers as needed to do the job. These chemicals can help responders tune out the larger scene, concentrate on what is in front of them, and perform their jobs based on training and experience, which may seem like superhuman strength and competence. However, survival chemicals that help bodies and brains confront the unimaginable go away, leaving questions about what to do next.

Much has been written about 9/11 responders and others whose lives changed forever after going to the scene of targeted violence, an active assailant, a catastrophic accident, or a destructive natural disaster response. No one is entirely immune to lingering thoughts, memories, or reactions that overwhelm the emotional and mental health systems of the individuals who respond to others' pain and suffering. These may include an occasional memory, a flashback, or a triggered emotional reaction to a sight, sound, or smell. Fortunately, society, in general, is talking more publicly about post-traumatic stress disorder (PTSD) in responders and others exposed to sights, sounds, and experiences they run toward as others run the other way. PTSD, in its simplest form, includes intrusive thoughts or reactions that last more than 30 days. Those intrusive thoughts or reactions can last a lifetime, and a long-term plan of support to deal with them is essential.

Getting Help for Responders and Caregivers

If you or someone you know is one who steps up in roles as responders or caregivers, expect that the experience has changed who you were and made you who you are now. Make a difference to yourself and others by getting the help and support needed to manage the outcome of these experiences.

Remember that caring for others may come with a cost that can be overwhelming to both the responders and those who care about them. However, coping options and support plans can make this cost more manageable. Resources that can help educate and provide support and guidance are plentiful. The task is to find one that fits your needs and feels right. Not all are right for everyone, but here are a few to consider:

- Disaster Distress Hotline 1-800-985-5990,
- The International Critical Incident Stress Foundation,
- Substance Abuse and Mental Health Administration, and
- Make The Connection – a resource for veterans (many responders are also veterans).

Mary Schoenfeldt, Ph.D., is the board president of Green Cross Academy of Traumatology and has responded to countless disasters. She is an emergency management professional specializing in community and school crises and has a passion for disaster psychology. She is a faculty member of FEMA Emergency Management Institute, an adjunct faculty at Pierce College, and a subject matter expert for the U.S. Department of Education. She also serves clients through her consulting business. She can be reached at yoursafeplace@msn.com

EOD / IED & COUNTERMINE SYMPOSIUM

CONFIRMED SPEAKERS

COL SHAWN L. KADLEC, USA
EOD COMMANDANT,
US ARMY ORDNANCE SCHOOL

COL RUSSELL HOFF, USA
PM CCS PROJECT MANAGER,
JPEOAA

COL BRENNAN C. FITZGERALD, USA
71ST ORDNANCE GROUP

LTC CORBIN E. COPELAND, USA
INCOMING DEPUTY COMMANDER,
52ND ORDNANCE GROUP

OCTOBER 25-26, 2023 | NATIONAL HARBOR, MD

(Source: Paul Gunnels, 2001).

Three Puzzle Pieces That Increase Community Preparedness

By Paul Gunnels

When wondering if the nation is better prepared today than it was 22 years ago on September 11, 2001, first responders would like to say it is. The following details are a personal account of actions in response to the 9/11 terrorist attacks and key takeaways for increasing community preparedness.

For anyone who watched the 9/11 incident unfold on live television, it initially seemed unreal and unbelievable. With my eyes glued to the screen watching the news that morning, I received a notification to deploy. I had been a Texas A&M Task Force 1 member for over a year at that point as a rescue specialist, attending many structural collapse training courses and exercises at Disaster City, preparing for such an event.

Six years earlier, after the April 19, 1995, Alfred P. Murrah Federal Building bombing, Dr. G. Kemble Bennett (then-director of the Texas A&M Engineering Extension Service, TEEX) made it his mission to help Texas prepare for such an event. He worked toward establishing Texas A&M Task Force 1 in 1997 and the premier 52-acre urban search and rescue (US&R) training center, Disaster City, located at Brayton Fire Field as part of TEEX, in 1998.

By 2001, the Texas A&M Task Force 1 US&R team was fully equipped and trained to respond to the terrorist attacks because, first, the National US&R program had provided the team's training. Secondly, the National US&R type 1 cache included ample equipment and supplies to support a response to a structural collapse. Thirdly, the type 1 US&R team was prepared to be self-sufficient for 72 hours. At the time of deployment, the team members were ready to fulfill their role as a small piece of the puzzle within the large-scale mission.

While local leaders plan, prepare, organize, and continually evaluate their programs to be prepared for the many risks within their communities, they struggle to maintain proficiency in all areas. It is unrealistic to believe that all preparedness plans will cover every possible scenario. The 9/11 incident introduced many new challenges. The lessons learned helped the response community identify many areas that needed to be addressed. Some of the puzzle's critical components included communications interoperability, multiagency coordination, and specialized teams.

Communications Interoperability

Having interoperable communications is essential for any organization to communicate with other

agencies and jurisdictions during emergencies. Over the past 22 years, interoperability in communications has improved among multi-jurisdictional and multi-disciplinary response agencies. The 9/11 Commission Recommendations started that initiative.

The 9/11 report revealed the inability of first responders to communicate effectively with each other during the response. The Tenth Anniversary Report Card (in 2011) and 20 Years After 9/11: Examining Emergency Communications (in 2021) published their findings stating that New York still has limited success in communications interoperability. Although these reports focus on New York post-9/11, the fact is that similar issues exist at different levels and still challenge some jurisdictions across the nation. Some significant challenges include internal politics, financial costs, limited multiagency coordination, jurisdictional priorities, and a list of many other factors too long to list. There is no cookie-cutter solution across the board to solve these issues. Every jurisdiction should develop an interoperability plan. For the plan to be successful, it must include coordination between agencies and jurisdictions within their communities.

Large-scale disasters present unique challenges. The 9/11 terrorist attacks provided lessons learned to better handle adverse situations and challenges.

Improved interoperability developments and coordination have occurred at several high-profile national events such as the Political Conventions, World Series, and Super Bowl Games. Public safety national broadband networks such as FirstNet continue to expand and are used at large sporting events, disasters, and other emergencies to improve communications. These and many other technological advancements have been supported by funding that became available after 9/11. Funding and technological advancements are not the only things that will improve communications among different agencies and jurisdictions. Success relies on agencies and jurisdictions having a strong operational plan for communicating and confirming that information sharing is prompt and effective. Best practices include regularly training and exercising the plan, system, and processes while identifying improvement areas, according to the Department of Homeland Security (DHS) National Emergency Communications Plan.

Multiagency Coordination

While some agencies and jurisdictions may be working closer together since 9/11, the planning, preparedness, response, and recovery to incidents require strong coordination. The prevention or response to incidents requires increased coordination between agencies. The National Response Framework states multiagency coordination can be in emergency operation centers (EOCs), fusion centers, joint operation centers, and other coordination centers. These coordination centers usually have workstations, communication equipment, meeting rooms, and other specialized equipment that provide an environment for multiagency coordination. Another way to improve multi-jurisdictional and multiagency communications is by establishing a unified command, typically at the incident's command post.

Some jurisdictions have improved communication in the past two decades by establishing permanent local, state, and federal coordination centers. Intelligence agencies use coordination centers to strengthen communication to prevent future terrorist attacks. EOC activations are no longer just for emergencies but also for planned events such as large venues like concerts, trade days, college football games, and other significant events.

To be more effective during real-time disasters and emergencies, personnel must be trained in their specific roles by utilizing a variety of emergency exercises to evaluate their operational effectiveness. When deficiencies are identified during trainings and exercises, the organization is ultimately responsible for closing the gaps by improving the process.

Specialized Teams

Each large-scale emergency or disaster presents unique challenges. The 9/11 terrorist attacks had

many unique challenges requiring assistance from specialized teams. These teams can help with rescue, medical services, mass care, debris removal, legal services, and other supporting areas. By comparison, New York City has many internal resources, but no community has unlimited resources. When developing planning and preparedness plans, communities should identify resources needed to address the risks within their jurisdictions. Many resources may need to come from other jurisdictions to support an incident. These resources could be more specialized, such as US&R teams, or more generalized teams like Voluntary Organizations Active in Disaster (VOAD):

- A US&R team consists of diverse skill sets working together to accomplish challenging goals. The US&R team comprises command, medical, rescue, search, planning, technical, logistical, hazardous materials, and communication specialists. Each position's role now receives the specialized training and equipment that was lacking in New York in 2001.
- Since 9/11, the development of specialized teams for structural collapse, wide-area search, and swift water rescues has been added. While the National US&R system has maintained the same number of teams since 9/11, the State Urban Search and Rescue (SUSAR) Alliance has grown significantly.
- VOAD consists of non-government teams that deploy to assist a community in managing its immediate needs during a disaster. Responding to countless disasters and helping to serve some of the impacted areas, National VOAD has seen significant growth (158%) in its membership between 2000 and 2021.

Increasing Community Preparedness

Despite having complete confidence that Texas A&M Task Force 1 was fully prepared to respond to 9/11, the team had to overcome unforeseen challenges once on the scene to keep the rescue mission moving forward. For example, the team had not been trained on hanging from rescue ropes while cutting metal. A critical lesson learned from 9/11: no matter how well responders prepare, unforeseen challenges will arise that must be resolved on the fly.

Dwight D. Eisenhower's words, "Plans are useless, but planning is indispensable," should resonate with those in planning and preparedness. Developing a plan facilitates the organization of thoughts and the development of processes to achieve strategic goals while preparing for a future disaster. Catastrophic events bring unique challenges that responders must overcome. There is no way to be 100% ready for every challenge. However, planning and preparedness efforts before an incident allow responders to have more knowledge to make better decisions during it.

The 9/11 reports point out that teamwork, collaboration, and cooperation are equally essential for success. Effective planning and preparedness programs involve communications interoperability, multiagency coordination, and specialized team utilization. Realizing that they must work together to be efficient and successful, each community should aim to be as prepared as possible for a large-scale emergency or disaster. Every community may not be entirely ready for any possible incident, but most, if not all, are much more prepared to handle adverse situations and challenges based on lessons learned from 9/11.

Paul Gunnels has 37 years of experience in emergency services and is currently a regional section chief for the Texas Division of Emergency Management (TDEM). He retired from the College Station Fire Department as an assistant chief, former rescue program director for Texas A&M Extension Service, and a member of Texas A&M Task Force 1. He holds a bachelor's degree in Emergency Management from West Texas A&M University and a Master of Public Administration and Policy degree from Grand Canyon University. He also is a graduate of the Executive Fire Officer Program at the National Fire Academy

Texas A&M Engineering
TEEX
EXTENSION SERVICE

Fire & Emergency Services Career Day

THURSDAY, OCTOBER 19, 2023

TEEX Brayton Fire Training Field® - Bunte Complex

9 - 11:30 AM

Job Search/Career Advice Panel Discussion with Q&A
Listen and engage with a panel of experienced professionals who share insightful job search, hiring and career advancement advice.

1 - 4 PM

Hiring Resource Tables
Visit with Fire and EMS departments from around Texas looking to hire firefighters and EMT/Paramedics.

For information on reserving a Hiring Resource Table please email careerservices@teex.tamu.edu.

Register to Attend
tx.ag/TEEXCareerDay

©Mark Margolis/Rainbow Symphony via the American Astronomical Society.

Planning for a Cross-County Special Event

By Mark Howell and Laurel Radow

In the United States, some localities from Oregon to Texas will witness only the totality of the October 14, 2023, annular eclipse (also known as a "ring of fire"), which will result in a partial eclipse for much of the country. During a subsequent event, a far more populated portion of the country will experience the April 8, 2024, total solar eclipse. However, where these two paths cross, some in Texas will view both the 2023 annular eclipse and the 2024 total solar eclipse.

These events provide opportunities for the preparedness community to collaborate and serve as members of eclipse planning committees for their respective localities or states. The 2023 annular eclipse would be a good day to test systems and implementation plans for the more significant 2024 event. Emergency managers and public safety officers could offer their expertise in community preparedness, hazard assessments, risk mitigation, contingency planning, and other special-event best practices.

Some jurisdictions have already completed their viewing event plans, and their sites' implementation efforts are ready to get underway. Others have yet to begin. Regardless of which event a locality will witness, the preparedness community brings vast strengths to eclipse planning efforts. Since planning for gatherings and events related to an eclipse is often conducted by "professional and amateur astronomers, formal and informal educators, eclipse chasers, science writers, and outreach specialists," many members of the local or state eclipse planning effort may not have considered including the community's emergency preparedness and response capabilities or their operational knowledge during planning discussions.

Emergency Preparedness and Response Planning

Special event planning without emergency contingency planning negatively impacts event staff and emergency responders' ability to adapt and respond to adverse or changing conditions. As such, collaborative efforts between eclipse planning committees and local emergency preparedness and response agencies could guide the testing of local contingency plans and capabilities before the event. From tabletops to full-scale exercises and training can help plan for adverse weather conditions or emergencies on the day of one or both eclipses.

When an emergency arises (e.g., severe weather events, significant traffic congestion or collisions, technological failures, violence) during a large-scale event or gathering, it may require rapid deployment of the Incident Command System (ICS) to manage the incident and any cascading effects. Despite abundant skills and abilities in managing and responding to large-scale events, emergency preparedness and response professionals do not always participate in the planning and logistics of eclipse events. Special event planning uses the same process as planning for emergencies – organizing people, equipment, and supplies so that everything is in the right place at the right time to accomplish a mission and protect lives and property.

A solar eclipse is a unique form of special event that does not always fall under emergency planning protocols, but it should.

In some cases, planners for solar eclipse events are able to formulate ideas and basic plans but then fall short of implementing the strategies and tactics on the ground in the days leading up to and during the event. For example, the American Astronomical Society (AAS) Solar Eclipse Task Force described in a plenary session in June 2023 the traffic congestion, crowd control, first responder access, and other public safety and emergency management concerns related to the 2017 eclipse, along with "lessons learned" from that event.

To ensure that public safety issues are addressed in future eclipse planning, emergency managers and public safety professionals can help explain how to transition from planning to operations and promote an understanding of what operational plans and procedures would be beneficial to incorporate before the event. Since preparedness and response professionals regularly build critical skills in putting plans into action on the ground – in exercises or actual events – it makes sense for these professionals to provide guidance and assistance for eclipse events, which may not already be on their planning schedules.

For localities that will benefit from both events' rare and delightful experiences, collaborative efforts between the eclipse planning committees and emergency planning professionals in the final weeks before the annular eclipse could offer valuable insights. Lessons learned and best practices that emergency planners currently have for planned special events within their jurisdictions could apply to the planning efforts for these anticipated special events, which will span cities and states. Building these relationships will also facilitate the process if an incident occurs during the event and response units need to mobilize.

Pre-Event Action Items

Since planning committee members may be unfamiliar with pre-event exercises and planning checklists, below are some suggestions to help when shifting from planning to preparedness. In the weeks before October 14 or sometime before the end of 2023 for the Total Eclipse of April 8, 2024, the preparedness community should reach out to the eclipse planning committee to assist in leading and designing exercises. They also should work with committee members to develop tabletop exercises with believable scenarios requiring all to participate in decision-making. Examples of field exercises to build awareness and confidence could include mass-casualty drills and readiness for emergency operations centers and dispatch. In rural areas, consider search and rescue exercises.

Even without all the volunteers being available to test the plans, the leaders facilitating any activities related to these eclipse events should test the capabilities to find gaps and address any potential concerns. Following are some, but not all, of the operational matters to consider:

Eye/Viewing Safety

- What are the availability and locations of glasses?
- How will information be conveyed regarding the availability of glasses?
- Will glasses be available before the event or on the day of the event?
- If glasses are available before the day of the event, how will they be distributed?

Medical/Public Health

- Where will first aid personnel and ambulances stage?

- What is the mass-casualty incident capability of the local emergency medical services (EMS) system and emergency room(s) capacity?
- What communications issues and diversion stress-testing should the EMS central receiving facility plan and test for?
- How will COVID and other public health concerns be addressed?

Transportation

- Will roads be closed on the day of the event? If so, how will that information be provided before and on the day of the event?
- Where will traffic incident management vehicles be staged (locate these vehicles on a map)?
- Are volunteers (e.g., Community Emergency Response Teams [CERT] or Citizens on Patrol) available to assist in traffic control?
- Where will readerboards and portable signage be placed to inform travelers of important information?

Parking

- Are the parking lots marked on a map?
- Has the information been shared with all involved in the field test?
- Is the event planner (museum, city, etc.) responsible for parking? If yes, how will that information be conveyed?
- If private organizations will manage parking, how will that information be conveyed?
- Are access and egress ensured for emergency responders?
- Are evacuation routes easily accessible?

Aid and Information Stations

- Will there be aid and information stations?
- What are their locations?
- Do they have or need the property owners' permission?
- What services will these stations offer?
- Where are they located on a map?

Multi-Disciplinary Collaboration Before and During the Event

The sheer number of visitors could be unprecedented for some communities hosting events for or simply in the path of the April 8, 2024, eclipse. As such, public and private sector agencies, nonprofit organizations, public safety officers, emergency managers, and eclipse planning committees must work together to ensure the safety and security of those participating in eclipse activities and anyone else in the vicinity. Because the success or failure of an event relies on how much attention is paid to plan details, the more time spent on the operational components, the more likely visitors will be to arrive early, stay safe, and leave late, pleased that they were part of an exciting act of Mother Nature.

Mark Howell is Grounded Truths LLC's director and emergency and fire management specialist. He has 25+ years of public safety experience, including fire, law enforcement, emergency medical services, and emergency management at the local, state, and federal levels, including 14 years with the U.S. Forest Service (USFS) full-time in progressive fire and emergency management positions. He is a graduate of the Wildland Fire Apprenticeship Program and the first cohort of the USFS's Field Command School, an Incident Management Team Academy program designed and taught by the National Incident Management Organization. During the 2017 Great American Eclipse, while a supervisory fire prevention officer on the Malheur National Forest, he served as the federal interagency liaison between the Northeast Oregon National Forests and their federal, state, and local government cooperators and provided substantial planning and operational support to affected communities and jurisdictions within totality in Northeast Oregon.

Laurel J. Radow, AAS SETF member and Co-chair, AAS Local Planning Working Group. She joined the Federal Highway Administration (FHWA), U.S. Department of Transportation in 1996. From 2004 until her retirement at the end of 2016, she served as a member of the FHWA Office of Operation's Traffic Incident and Events Management Team. In that capacity, she served as program manager for the agency's Evacuations/Emergencies and Planned Special Events programs and managed a range of Traffic Incident Management tasks. From 2014-2016, she served as vice chair of the National Academy of Sciences Transportation Research Board's (TRB) Standing Committee on Critical Transportation Infrastructure Protection (AMR10). She recently completed her second and final term as chair of the same committee. In addition to co-chairing the TRB at the October 2018 Resiliency Conference (T-RISE), she also served as guest managing editor for the TR News September/October 2021 Issue no. 335,"State of Emergency: What Transportation Learned from 9/11."

THE MAGICAL SCOOP UP COMMAN CENTER! No worries! No matter where you are, the chip inserted under your skin allows the highly trained Evacore despatchers to mobilize teams of pilots to instantly find you

Beyond Registries: Better Solutions for People With Disabilities

By June Isaacson Kailes

Emergency planners often identify volunteer disaster registries as a solution for assisting people with disabilities before, during, and after a disaster despite serious flaws with this approach. Perhaps this is because jurisdictions do not understand that there are better options and how to implement them. The National Council on Disability (NCD) asserted in a May 24, 2019, report that it.

> *[C]annot overstate how detrimental registries for people with disabilities are in disasters. Stakeholders across the spectrum of disability advocates and emergency managers still struggle to find ways to make registries a viable solution to identify, rescue and evacuate people with disabilities affected by disasters despite repeated failures of registries. Registries isolate and marginalize people with disabilities and create a false sense of expectation among people with disabilities and their family members. Like institutions, registries have been proven to be an ineffective method to ensure proper evacuation and sheltering of people with disabilities during emergencies.*
>
> *People with disabilities have a right to equal access to emergency services. Registries have both impeded equal access solutions and established inadequate alternatives for using federal funds. NCD recommends that no federal funds, including but not limited to federal funds from the U.S. Department of Homeland Security and the U.S. Department of Health and Human Services, be used in development, deployment, and maintenance of emergency "special needs" registries intended to include people with disabilities.*

Registries, as used here – sometimes referred to as "special needs" registries – are sponsored primarily by a government as a disaster response and planning tool. The information typically collected includes at a minimum the individual's name, location, contact information, and other details of people who voluntarily register and may need disaster help.

Registry Problems & Better Solutions

This article describes eight common problems with developing and using a volunteer disaster registry and suggests better solutions for each. The focus here is on disasters versus emergencies because local emergencies (e.g., house fires, downed power lines, and vehicle collisions) are generally dealt with using available response resources (see California Disaster Coalition Meeting, 2022; Kailes, 2023). Disasters cause severe disruptions to a community's functioning that exceed

its capacity to cope using available resources. These widespread, large-scale events may cross geographic and political boundaries and require coordinated action across multiple entities and levels of government. Disasters can include natural, technological, or human-caused events, such as earthquakes, extreme weather, hurricanes, tornadoes, heat waves, tsunamis, wildfires, mudslides, floods, droughts, pandemics, power outages, chemical spills, terrorism, and cyberattacks.

While registries may work in small local emergencies, they fail during large-scale events primarily because of the mismatch between the magnitude of the needs and the availability of resources to address disaster-related needs. Voluntary disaster registries are based on seriously flawed assumptions by planners and potential registrants that involve planning (assumptions, evidence, response capacity, and data and planning tools) and modernizing communication. Sometimes, these assumptions can lead to fatal consequences.

Planning – Assumptions

Registry Problem 1 – A registry is assumed to be a straightforward, simple, and compelling approach to including and assisting people with disabilities and others with access and functional needs before, during, and after disasters. However, this commonly held belief has not been systematically tested and usually represents dis-, mis-, and flawed information (see also California Disaster Coalition Meeting, 2022). Instead, registries are based on guestimates that lack capacity specifics, including the who, what, where, when, and how. These guesses can lead to symbolic, unproven plans and overpromises. Thus, the registry model is a flawed approach to taking care of the "disability problem" and may be an attempt to appease the community and meet the superficial requirements of a planning checklist. Although a registry may have a specifically stated purpose, such as evacuation transportation or life-safety checks after a disaster, registrants typically assume implied rescue.

Better Solution 1 – Engage the disability community in the development of plans that are tested, exercised, revised, and sustained with a commitment to a continual improvement process. Involving these disability partners helps to address implicit disability biases, discrimination, lack of access, and accommodation. The support helps prevent civil rights violations by delivering assistance that allows individuals with disabilities to participate equally in and benefit from emergency services. Contracts, agreements, and memoranda of understanding (MOUs) with these partners can help provide needed resources such as accessible transportation, Communication Access Real-Time Translation (CART), accessible transportation, sign language interpreters, and life-safety checks.

An effective partnership tool employed for the first time during the 2007 California wildfires and subsequently during disaster responses is disability emergency briefing team calls. The group consisted of staff from disability organizations, state and county governments, and the Federal Emergency Management Agency (FEMA). The calls' focus is problem-solving regarding meeting essential unmet needs – for example, replacing left-behind, lost, or damaged consumable medical supplies and equipment such as wheelchairs, canes, walkers, shower chairs, hearing aids, etc. A similar practice started in 2018 in North Carolina during Hurricane Florence.

Registry Problem 2 – A registry is often based on the inaccurate idea that people with disabilities are sick, homebound, and in need of disaster assistance.

Better Solution 2 – Recognize that rarely is anyone homebound. The Bureau of Transportation Statistics estimated that approximately 3.6 million people with disabilities in the U.S. do not leave their homes. The U.S. Census estimated that, as of July 1, 2022, the country's population aged 18 and over is 260.8 million, of which the Centers for Disease Control and Prevention (CDC) estimate that about 27% (70.4 million) are people with disabilities. This means that only about 5% of those with disabilities are homebound. Understand that most disabled people are not sick, nor do they live in institutions. Some people will need immediate help, and some will not. Some may even be disaster responders. (*Note*: These statistics are provided for reference based on available data. Due to different definitions, different timeframes, etc., the exact number of people in the U.S. with a disability varies between resources.)

Base plans on realistic projections that include people with disabilities and others with access and functional needs. People with disabilities are a "protected class." This means protected from discrimination as defined by federal civil rights laws such as the Americans with

Disabilities Act (ADA) of 1990 and other federal and state civil rights protections. Beyond the CDC's estimated 27% of adults having some disability, others with access and functional needs may not meet the protected class definition but still benefit from these protections. These individuals can include people with the limited ability to walk, run, see, drive, read, hear, speak, remember, or understand. When planning integrates the known needs of people with disabilities, including physical, equipment, programmatic, and communication access, a larger segment of the population (others with access and functional needs) benefits. These two groups can represent 50% of the population.

Planning – Evidence

Registry Problem 3 – Evidence has not proven that registries work. Registry failures have been repeatedly exposed in multiple reports during disasters in three states. In Texas during Winter Storm Uri in 2021, some registrants reported that the paperwork was "cumbersome," making it difficult to register. Then, after registering, those who needed help did not receive support they expected. In California, issues included keeping registries current, retrieving the data, and responding when needed. In 2004, In 2004, the Los Angeles County Office of Emergency Management conducted research that concluded that the costs of developing and implementing a voluntary registry would cost nearly $1.4 million per year for the first three years. In Florida, Hurricane Irma in 2017 highlighted issues with registrants being confused about what they were supposed to do with "special needs" registries. As a result, some were denied services because they self-evacuated or no longer met the registry's requirements for aid. As these examples demonstrate, registry failures lower public confidence and trust.

Better Solution 3 – More research is needed that analyzes the effectiveness of existing registries' outcomes, impacts, and results (see California Disaster Coalition Meeting, 2022). This research should consider the following factors:

- Community partnerships (see Planning – Response Capacity, Better Solution 5) response models;
- Tools individuals can use to signal for and get help (use of existing and emerging technology: apps, global positioning systems, satellite, etc.; see Modernizing Communication, Better Solution 8); and
- Community education and training that counteracts beliefs that help will come immediately (see Response Capacity, Better Solution 4).

Integrating genuine and accountable stakeholder involvement helps prevent research drifts, shifts, and sometimes a total change in the intended focus. Stakeholder involvement is "a must do, not a nice to do!"

Planning – Response Capacity

Registry Problem 4 – Emergency personnel may believe that registry disclaimers are sufficient. However, disclaimers do not mean that responders will act on or know what to do with the information, leaving registrants with a false sense of security. Despite disclaimers, registrants persistently think that, "If I register, they know where I am, and they will come to help me." However, this belief decreases and diverts attention from developing, reviewing, and strengthening personal preparedness plans (see California Disaster Coalition Meeting, 2022; Kailes, 2023).

Better Solution 4 – Help people with disabilities and others with access and functional needs to engage in specific preparation planning. This process requires ensuring a careful thought process, taking steps toward establishing preparations, and maintaining current personal support systems, helpers, and evacuation plans. Contracts with disability-led organizations that have staff with lived experience can be effective with these tasks. For example, California's Disability Disaster Access & Resources program, through contracts with investor-owned utilities, provides resources to people with disabilities affected by power outages common to many disasters.

Registry Problem 5 – For planners, registries may divert energy from developing specific procedures, assets, and response capacity needed for response and recovery.

Better Solution 5 – Use broad community partnerships and connections to build response capacity with government, businesses, community-based organizations, self-organizing groups, and Voluntary Organizations Active in Disasters (VOAD). It takes teamwork and hard work to build assets and resource capacity to operationalize, embed, and sustain viable and specific help. Partnering with community groups is more likely to result in better solutions and outcomes for disaster-impacted communities. For example, in Puerto Rico, the Mayor's Office for People with

Disabilities coordinated a shipment of supplies and durable medical equipment in October 2017. However, after months of delays, the release of the shipment was still denied. It took "a strong advocacy effort led by local disability advocates and supported by Portlight and the Partnership finally succeeded in the release of these critically needed goods." These partnerships include completing and sustaining contracts and agreements for:

- Helping people with disabilities with specific, not vague, personal emergency plans;
- Conducting life-safety checks; and, when needed,
- Providing:
    - Food, medications, supplies, backup power,
    - Evacuation assistance from structures,
    - Transportation out of and back into affected areas,
    - Personal assistant services to help an individual with bathing, dressing, eating, grooming, toileting, transferring, shopping, or communicating (personal assistants can be a family member or friend, paid or volunteer, and are sometimes called attendants or caregivers),
    - Telehealth and telemedicine services, and
    - Sheltering, temporary, and permanent housing.

By planning with and not for people, planners can integrate diverse perspectives. However, it will take more than one meeting. Developing, refining, and sustaining specific solutions may take months or years. Planning partners must include and represent diversity in perspectives to create equitable policies and conduct planning, programs, and response capacity that include and benefit all rather than harm the most disproportionately impacted groups and communities. Planning also must not use the lens of middle-class privilege, ageism, and ableism, which includes not assuming everyone has a stable internet connection, has money to buy emergency supplies, owns a working vehicle, and can walk, run, see, hear, speak, remember, and understand.

Planning – Data and Planning Tools

Registry Problem 6 – A voluntary list is perishable and can quickly become outdated because registries may be difficult to keep current.

Better Solution 6 – Partner with disability community organizations and vendors (independent living centers, durable medical equipment, and consumable medical supply providers, etc.) that actively support people, customers, clients, consumers, and members, because their contact information is more frequently updated (see California Disaster Coalition Meeting, 2022; Kailes, 2023).

Registry Problem 7 – Planners may assume that registries are good planning tools because of the expectation that "when you register, responders will know how many will need help, and they can plan accordingly." This assumption is false because registries are always incomplete, as they include only a small percentage of people who may need assistance. People with disabilities may not register because they do not believe registries work, have privacy reasons, are fearful of being tagged as vulnerable, have concerns regarding legal status for themselves or their family members, or are afraid of losing their independence. Using a registry to define the size of the population that will need disaster assistance is a convenience sample that results in inadequate baseline numbers. This approach is dangerous and violates civil rights protections of people with disabilities who are not in the registry.

Better Solution 7 – Utilize more accurate planning data tools and ways to define needs (see California Disaster Coalition Meeting, 2022). Data sources for these tools could include:

- Program administrative data from sources such as human service agencies, social security, Veterans' Administration, etc. (e.g., Florida's County Profiles for Access and Functional Needs provides examples of both survey data sources and administrative data sources. A link at the bottom of the county profiles shows the data sources used) show locally relevant data for people with disabilities and other access and functional needs within jurisdictions;
- Census Data;
- Social Vulnerability Index; and
- FEMA's Resilience Analysis and Planning Tool.

A close-up of a helicopter deploying its super-scooper s to grab & hoist a dangling terrified, shaking and teeth-chattering wheelchair user. Amused flying geese approach. Who could ask for better **evidence** of the great effective pluck-up!

Modernizing Communication

Registry Problem 8 – Because most people with disabilities are not homebound, knowing where people live does not tell where people are before, during, and after a disaster.

Better Solution 8 – The focus must be on modernizing how people communicate when they need help and what they need versus assuming all people with disabilities need the same support and are in fixed locations (see California Disaster Coalition Meeting, 2022). When people can signal their need for help or the status of their safety, it eliminates the need for non-inclusive registries that use out-of-date lists and lead to unnecessary calls, wasted trips, and lost time for overstretched, scarce first responders and volunteers. Diverse applications and options for smartphones and wearables (like smartwatches) have applications and integrated sensors with prompts for users, such as "It looks like you have had a hard fall. Press emergency, SOS, or press I'm OK." Use and improve the technology which:

- Allows signaling for help by a call, text, email, or button press;
- Uses precise location services and sensor technologies; and
- Uses global positioning system-enabled applications that allow users to choose contacts who can track their locations in real-time, and contacts receive an "I'm Safe" or "Need Help" message to their selected lists.

Implementing Better Solutions

The eight registry problems outlined above highlight some of the problems with using disaster registries for people with disabilities. As American journalist and scholar H.L. Mencken said, "For every complex problem, there is an answer that is clear, simple, and wrong." Understanding the flaws in these assumptions and possibilities for better solutions and outcomes is the first step toward providing more effective support and safety for the diverse communities of people with disabilities and others with access and functional needs. Hold each other accountable for the partnerships, hard work, and problem-solving needed to create, embed, deliver, and sustain real impacts and outcomes. The time is now to make changes to help people protect their health, safety, and independence and successfully cope with and live through the increasing and inevitable disasters.

Additional Resources

California Disaster Coalition Meeting: Emergency Registries: A Misleading, Harmful & Non-Inclusive Fix.

- Part 1 (2022, September 8) https://www.youtube.com/watch?v=mexNCwt1lw8and, Slides: http://www.jik.com/2022%2009-08RegistriesSlides.pdf.
- Part 2 (2022 October 13) https://www.youtube.com/watch?v=0RyvS9TG1QQ, Slides: https://mcusercontent.com/ee4ede4e4b843b579fff1fd86/files/6b7b1548-e1bd-a95b-c7ca-949ae83cc6c5/2022_10_13_registriesslides.pdf

J. I. Kailes (April 10,12, 2023) Disaster Registries for People With Access & Functional Needs: Pivoting the Model to Address Real Solutions, Colorado's 3rd Annual Access and Functional Needs Conference – Getting it Right: A "Plan With" Approach.

- Pre-Conference 1 (at 17.55-minute mark), https://www.youtube.com/watch?v=b412qBC3zaI&list=PLQDCae5hPt4aKzkVv1KRaQIygq0-YQRDK&index=2.
- Day 2 (at 17.05-minute mark), https://www.youtube.com/watch?v=OIEaGWeKtGY&list=PLQDCae5hPt4aKzkVv1KRaQIygq0-YQRDK&index=8

June Kailes, a disability policy consultant (jik.com), has over four decades of experience as a writer, trainer, researcher, policy analyst, subject matter expert, mentor, and advocate. June focuses on building disability practice competencies and health care and emergency management capabilities. She uses actionable details, the "how, who, what, where, when, and why," to operationalize the specificity needed to include people with disabilities and others with access and functional needs. June's work converts laws, regulations, and guidance into tangible building blocks, tools, and procedures that close service gaps, prevent civil rights violations, and deliver inclusive, equally effective services.

Source: Georgia National Guard photo by Capt. William Carraway/released

Citizen Soldiers and American State Defense Forces

By James P. Howard

State defense forces (SDFs) are state-level military organizations authorized by state law and operate under the authority of the state governor. These forces are tasked with providing support to the state National Guard and can be activated in times of emergency to assist with disaster response, homeland security, and other missions.

Although the size and structure of SDFs can vary by state, they generally consist of a mix of retired military personnel, civilians with prior military experience, and other volunteers committed to serving their communities. Despite their volunteer status, SDFs are highly trained and well-equipped to carry out their missions, and they play an important role in supplementing the efforts of the National Guard and other state and federal agencies.

A Historical Look at SDFs

SDFs have a rich and varied history in America, dating back to the colonial era when militias were used for defense. During the Revolutionary War, militias played a crucial role in the war effort. After the war, state militias continued to be the primary means of defense for many states. These militias were often composed of citizen soldiers who volunteered to defend their communities when needed.

In the early 20th century, the role of state militias began to evolve as the United States became increasingly involved in global conflicts. Each state militia was separated into two components under federal law. One was a contribution to the newly named National Guard, while the second was a reserve force for the state. During World War I, many states created dedicated SDFs, then known as state guards, to provide security within their borders while the National Guard was deployed overseas. These state guards were composed of volunteers who underwent military training and were subject to the same regulations and standards as the National Guard. Following the end of World War I, the role of state guards began to shift as the country focused on preparing for the possibility of future wars.

During World War II, SDFs played a critical role in the war effort, augmenting the National Guard and other military units in their homeland defense missions. These SDFs were often called upon to provide local security and assist with logistics and transportation.

In the post-World War II era, the role of SDFs continued to evolve as the country faced new challenges, such as natural disasters, civil unrest, and terrorism. Today, many states maintain SDFs alongside their National Guard units. Although the role and structure of SDFs may vary by state, they are generally composed of volunteer personnel who undergo military training and are subject to the same regulations and standards as the National Guard.

Modern Disaster Response Efforts

SDFs play an important role in disaster response efforts, as National Guard units are often stretched thin during emergencies due to overseas missions and long deployments. In times of natural disasters, such as hurricanes, floods, or wildfires, SDFs can be activated

to provide aid and assistance to local communities. These forces have proven to be critical assets in disaster response efforts, as they are able to quickly mobilize. Despite limited funding and training challenges, SDFs have demonstrated their ability to effectively respond to emergencies in their communities.

In recent years, SDFs have been increasingly utilized in disaster response efforts, providing valuable assistance to the National Guard and other emergency responders. During natural disasters such as hurricanes, floods, and wildfires, SDFs can be activated to provide additional resources and staffing to local authorities. For instance, in 2017, the Texas State Guard (TXSG) activated hundreds of personnel in the aftermath of Hurricane Harvey, which caused widespread flooding and destruction in the Houston area. The TXSG provided a range of services, including search and rescue operations, logistics, and distribution of supplies to affected communities.

During the 2018 Camp Fire, the California State Military Reserve (CSMR) played a vital role in responding to the deadliest wildfire in California's history. The CSMR provided a range of services, including logistics, evacuation of residents, and coordination with local authorities. In the months following the fire, the CSMR was also involved in recovery efforts and helping to rebuild communities. The CSMR has also been an active response component in other California wildfires, providing timely and effective support to help protect communities and mitigate the impact of these devastating natural disasters. The CSMR's contributions demonstrate the importance of SDFs in disaster response efforts and their ability to work closely with other agencies.

In 2019, the Ohio Military Reserve (OHMR) was activated to assist with disaster response efforts following severe storms and tornadoes that swept through the Dayton area. The OHMR worked with local authorities in a variety of ways, including recovery operations and logistics. The OHMR played a critical role in responding to the disaster, which caused widespread damage and destruction in Ohio. By working closely with local authorities and other emergency responders, the OHMR was able to provide timely and effective aid to those in need.

Actions Needed to Strengthen State Disaster Response Efforts

Currently, SDFs are a crucial component of disaster response efforts in the United States. They provide critical resources to state and local authorities in times of crisis, leveraging their local knowledge and flexibility to quickly mobilize and respond to emergencies. SDFs can also provide important specialized skills and resources that free up National Guard personnel to focus on other critical tasks outside of emergencies. For instance, some states have dedicated teams of attorneys to work with National Guard soldiers on legal matters, like wills. Teams of medical personnel from multiple SDFs distributed and administered vaccines during the COVID-19 pandemic. Several SDFs have band units that play at funerals and other ceremonial occasions.

Despite their effectiveness, SDFs face significant challenges in disaster response efforts, including limited funding, equipment, and training. Some states provide no funding to their SDFs and may provide no other resources. This limits their ability to provide new training and modern equipment to work with. These challenges can impede their ability to work with affected communities and impact their ability to coordinate with other state and federal agencies involved in the response effort. As such, it is essential to recognize and address these challenges to ensure that SDFs are better equipped to fulfill their mission.

To support the vital work of SDFs, state agencies and the federal government need to provide them with the necessary resources and training to help them effectively respond to emergencies, including increasing funding, improving equipment and resources, and enhancing coordination and communication between state and federal agencies. This can be done without impacting their state-specific role and mission, like how the federal government provides homeland security grants to local agencies. Governments also need to raise public awareness about the role and capabilities of SDFs, to help build trust and understanding with local communities.

Overall, SDFs are critical in protecting the country and serving local communities. By providing a safety net of capable and well-trained personnel to state and local authorities during times of crisis, they help ensure the safety and well-being of communities nationwide. With the right funding and resources, SDFs can continue to play a critical role in disaster response efforts and help build stronger and more resilient communities.

As an accomplished data scientist with over two decades of experience, Dr. James P. Howard II has made significant contributions to the field of data analytics and machine learning, with a strong background in public policy and a Ph.D. from the University of Maryland Baltimore County. His expertise extends to various domains, including health-related research and computational methods. Notably, Howard is a Maryland Defense Force captain, contributing his skills and knowledge to his community's defense and security efforts.

©iStock/artisteer

Bioterrorism – Could Smallpox Return?

By Robert C. Hutchinson

The variola major virus, which causes smallpox, had a long and terrifying pathogenic history in the human population – the only natural host. Examinations of 3,000-year-old Egyptian mummies identified markings similar to smallpox scars. The smallpox-like disease has been documented worldwide in writings for over 1,000 years. With a mortality rate of approximately 30%, along with possible blindness and severe scaring experienced by the survivors, it was a greatly feared pathogen over recorded human time.

The last natural smallpox outbreak in the United States was in 1949. The last documented naturally occurring case was in 1977 due to an aggressive and successful worldwide vaccination campaign. Due to a very effective global vaccination program, the World Health Assembly declared smallpox eradicated in 1980.

Although smallpox was eradicated from its human population and reservoir, it is still in designated stockpiles controlled by two nations. With the negative lessons learned and not learned from SARS-CoV-2 and possible laboratory leaks, suppose smallpox or a close variant returned to the human population. Immunity to the virus has faded with the end of the routine vaccination process and time, raising concern about how prepared the nation and world would be if smallpox re-emerged accidentally through a laboratory leak or intentionally through an act of bioterror or biowarfare.

Biowarfare or a Naïve Population

It allegedly happened before. Reports state that, in 1763, British officers traded two smallpox-infected blankets to Native Americans during the French and Indian War. They were reportedly from the smallpox hospital inside Fort Pitt. There was a siege by Native Americans at the fort with over 500 settlers gathered inside. The plan was reportedly to reduce the number of Native Americans outside the walls by disease before the dreadful disease spread further within the fort.

The three items were reportedly from the smallpox hospital inside Fort Pitt – the British fort built on the confluence of the three rivers in current-day Pittsburgh, Pennsylvania. There was a siege by Native Americans at the fort with over 500 settlers gathered inside, some ill with smallpox. The plan was reportedly to reduce the number of Native Americans outside the walls

by disease before the dreadful disease spread further within the fort. The siege broke when the Indians moved their resources from the fort to intercept 500 British troops responding to rescue Fort Pitt.

According to historical research, it was unknown if the exposed blankets could have transmitted the disease due to the age of the blankets. The very contagious disease was reportedly already circulating in the Indian population since 1759 before the transfer of the blankets at the fort. There were additional allegations that smallpox was present in other items traded by early settlers. Either from intentional infection or interactions with infected settlers, smallpox most definitely entered the naïve population with horrifying consequences. It was estimated that between 500,000 and 1.5 million Native Americans died from smallpox. It was yet another example of how smallpox could ravage a population anywhere in the world.

The CDC is working with vaccine manufacturers to develop new smallpox vaccines and therapeutics. However, they may not prevent a return of the eradicated virus.

Eradication and Stockpiles

The Thirty-Third World Health Assembly formally declared the global eradication of smallpox. The resolution declared smallpox as a devastating disease sweeping in epidemic form through many countries since the earliest times causing disfigurement, blindness, and death. The World Health Organization (WHO) initiated the global program to eradicate smallpox in 1959 and intensified it in 1967. Success was achieved in just a couple of decades.

Four countries – South Africa, England, the United States, and Russia (Soviet Union) – retained the variola virus after its eradication for research purposes. By 1984, South Africa and England either transferred or destroyed their viral stocks. Currently, the variola virus is reportedly only stored at the State Research Center of Virology and Biotechnology in Russia and the Centers for Disease Control and Prevention (CDC) in the United States (Atlanta, Georgia). According to the CDC:

- The goal of smallpox research is to address three areas that are essential for public health:
  - Finding better antiviral drugs to treat smallpox disease.
  - Making safer vaccines.
  - Improving tests to detect variola virus.

In 1996, the Forty-Ninth World Health Assembly recommended destroying the remaining stockpiles of variola virus in 1999. The declaration recognized that the genome sequence information for the variola virus strains allowed scientific questions to be solved and permitted the diagnosis of suspected smallpox. The variola virus escaping laboratories would be a serious risk as an increasing proportion of the population lacks immunity. The World Health Assembly would again discuss or recommend destroying the variola virus stocks in 1999, 2007, 2011, 2016, and 2019.

A 2007 World Health Assembly resolution mandated WHO to inspect the variola virus storage locations every two years to ensure the highest biosafety and biosecurity requirements. In accordance, WHO biosafety inspection teams visit the repositories and inspect the Russian and American containment facilities. The same team reportedly conducts both inspections and provides reports made available on the WHO website. No significant findings were observed in either nation's 2019 inspections, but there were recommendations for improvements in both countries.

Vaccines and Antivirals

Immunity to the variola virus is likely very low. Routine smallpox vaccinations ended in 1972 after the disease was eradicated in the United States. The antibody levels were estimated to decline five to 10 years after vaccination. Before eradication, WHO recommended revaccination every five to 10 years for international travelers and three years if traveling to endemic areas. Research indicated that decades-old vaccinations would not protect from the disease but could prevent a fatal outcome.

The United States reportedly possesses sufficient smallpox vaccine in its Strategic National Stockpile

(SNS) to vaccinate everyone who would need it for an outbreak if utilized as an agent of bioterrorism. Approximately three-quarters of the federal funds obligated for SNS medical countermeasures (MCM) between 2015 and 2021 were to purchase smallpox and anthrax MCM. The current smallpox vaccine does not contain the variola virus but a similar poxvirus. According to the CDC, the current smallpox vaccination protects for approximately three to five years.

CDC reportedly works with federal, state, and local officials to prepare for a smallpox outbreak. These public health officials would decide who would receive the vaccine, focusing on those directly exposed to the virus with prolonged face-to-face contact. After the challenges of the recent response to SARS-CoV-2, a smallpox outbreak response may not be as easy to execute as described by the CDC. There would likely be trust and confidence issues in the process, affecting outcomes.

The CDC is working with vaccine manufacturers to develop new smallpox vaccines. However, since the virus has been eradicated in humans, the ability to prevent the virus is not directly studied. The researchers use indirect methods by using vaccinated subjects' blood samples and testing the serum against the virus in a laboratory setting.

The Food and Drug Administration (FDA) has approved two antiviral drugs to treat smallpox – teccovirimat and brincidofovir. However, the drugs have not been tested on humans with smallpox disease, so the actual benefit is unconfirmed.

Retention Failure

The smallpox storage and tracking process may not always meet expectations and requirements. The United States experienced the improper storage and handling of smallpox on at least one occasion. During the clean-up of FDA laboratories in 2014 to prepare for a move from the National Institutes of Health (NIH) campus, six vials of variola virus were discovered in a cold storage room. The vials were found among 327 unclaimed vials in the back of the storage area. The variola virus vials, along with a vial of Russian spring-summer encephalitis and nine unidentified vials, were turned over to the CDC. The 16 vials were destroyed in 2015. The remaining 311 vials were either destroyed or retained for research.

According to the FDA, the 327 vials were reportedly made between 1946 and 1964. It was unknown what entity created the vials and how they came to be placed in the storage room. The FDA laboratory shared the cold storage room from 1992 to 2014. An FDA researcher reported that the room was not empty when they started using the space in 1992. The CDC and the Federal Bureau of Investigation investigated the incident. The FDA conducted a review. The FDA identified six findings with corrective actions in 2016 to prevent a similar occurrence with hazardous biological agents and toxins (HBAT) in the future. Below are the FDA review's corrective measures:

- Enact policies and procedures to ensure that biological material is not orphaned when its owner departs the laboratory;
- Enact policies and procedures to ensure that a single individual is responsible for all contents, including HBATs, in shared storage areas;
- Conduct a full inventory of all units that store HBATs, and require periodic updates to ensure the inventory list remains current at all times;
- Enact appropriate policies and procedures to ensure that individuals are aware of the proper actions to take when they encounter a select agent or toxin in an unregistered facility or laboratory for which they are not trained to handle;
- Enact procedures to ensure that individuals are aware of the proper officials to contact immediately when there is a safety or security incident; and
- Communicate the best practices to ensure that individuals are aware of the proper way to store materials in a cold room.

These corrective actions should have already been in place for the sensitive FDA laboratories on NIH property. From the report, it was unclear how the variola virus was outside the designated CDC storage

location – especially after its eradication in 1977 and declaration in 1980. The concerns remain that another vial could be sitting in an unauthorized area anywhere in the world pending accidental exposure.

The Threat

The variola virus can be hardy if protected from heat and ultraviolet light but is relatively easy to kill with strong disinfectants. However, it can be a serious bioweapon since it is easy to grow and aerosolize for delivery. The Soviets reportedly produced massive bioweapon quantities for research and offensive biological warfare decades ago.

According to the CDC website, there is no immediate, direct threat of bioterrorist attack utilizing smallpox. However, even though it has not been used in modern times, the CDC identified that:

> *There is credible concern that in the past some countries made the virus into weapons, which may have fallen into the hands of terrorists or other people with criminal intentions.*

There have been concerns that quantities of variola virus may have been taken or transferred from the Russian stockpile at the end of the Soviet Union. Some fear that then-unemployed scientists or former Soviet bloc nations may have retained, received, or transferred quantities of the pathogen. Also, Russia could possess uninspected covert stocks due to their enormous previous production. There also were allegations in 2002 that France, North Korea, Iraq, and Iran may have had undeclared stockpiles. The offshoring of sensitive or restricted biological research to other countries could be another danger. The actual amount of existing smallpox virus is quite likely unknown.

With the previous smallpox handling and storage violation and the possibility of human error in biosafety laboratories, the smallpox threat could be a public health concern for the United States. The concern could be more significant from unauthorized and undeclared virus possession and research. The possible access by unfriendly actors and gain-of-function or directed evolution research and technology would support current and enhanced planning and considerations. The recent identification of a suspicious biological research site in California with at least 20 potentially infectious agents only highlights these concerns.

Although naturally occurring smallpox was eradicated from the human population, that does not mean it can never return from a bio-leak or bioweapon. The efficacy of current vaccines and MCM may not be sufficient for smallpox or a newly enhanced variation. SARS-CoV-2, with a mortality rate of approximately one percent, would appear quite manageable compared to a virus with a 30 percent death rate – 30 times greater. Although there are numerous other significant biological concerns to consider and plan for, smallpox should continue to be high on that list.

U.S. pandemic preparedness strategies and plans appeared sufficient until SARS-CoV-2 emerged in early 2020. Existing smallpox planning and preparedness levels could be in the same position with much more serious consequences. The strategy looks good on paper, but the vaccines and MCM may not be readily available and sufficiently effective for an entire nation. Smallpox could return.

Robert C. Hutchinson was a former police chief and deputy special agent in charge with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations in Miami, Florida. He retired in 2016 after more than 28 years as a special agent with DHS and the legacy U.S. Customs Service. He was previously the deputy director of the agency's national emergency preparedness division and assistant director for its national firearms and tactical training division. His numerous writings and presentations often address the critical need for cooperation, coordination, and collaboration between public health, emergency management, and law enforcement, especially in the area of pandemic preparedness. He received his graduate degrees at the University of Delaware in public administration and Naval Postgraduate School in homeland security studies. He is a long-time contributor to Domestic Preparedness and serves on the Advisory Board.


©iStock/Caiaimage/Robert Daly

Reducing Workplace Violence in Healthcare Facilities

By Corina Solé Brito

Violence in healthcare facilities significantly challenges patients, providers, support staff, visitors, and first responders. The most recent data in 2016 from the Occupational Safety and Health Administration (OSHA) estimates that nearly 75% of about 25,000 workplace assaults reported annually happen in healthcare settings. More recent survey data published in 2022 by the International Association for Healthcare Security & Safety (IAHSS) found increased violent crime in healthcare facilities from 1.4 per 100 beds in 2019 to 2.5 incidents in 2021. Simple assaults rose from 10.9 incidents per 100 beds in 2019 to 17.7 in 2022. Violence directed at staff by non-employees accounted for 73% of aggravated assaults and 86% of simple assaults. Anecdotal evidence suggests that the problem only increased during the COVID-19 pandemic and extended off campus, as community members verbally and physically attacked healthcare providers because they were angry about social distancing, vaccination mandates, restricted visitation policies, and other disease prevention protocols and strategies.

Responding to healthcare workplace violence can be particularly challenging for local law enforcement, who may not be familiar with the facility layout, staff, or established procedures. This unfamiliarity can potentially lead to a delay in response or worse. Once the incident is over, the crime scene must be secured and thoroughly investigated, temporarily removing a significant amount of workspace and requiring staff to suspend or relocate critical medical services. Many healthcare facilities have solid relationships with local law enforcement, but this still seems to be the exception, not the rule.

There is some "good" news. While violent incidents are increasing, victimized healthcare workers are likelier to report them than dismiss maltreatment as "part of the job." In the May 2023 issue of the Domestic Preparedness Journal, certified protection professional Kevin Jones provided a comprehensive overview of workplace violence and listed robust prevention and preparedness suggestions. Recent incidents have demonstrated the need for improved collaboration and joint exercises between healthcare facility emergency management and security and local law enforcement to solidify relationships and guarantee the best response possible. This article provides a snapshot of healthcare-specific information and tools designed to protect staff, patients, and others in what was traditionally one of the safest locations in a community.

Workplace Violence in Healthcare Facilities: A Snapshot of the Problem

Patients and visitors bringing weapons to healthcare facilities is a challenge, particularly for emergency department (ED) staff, where time is of the essence, and interpersonal conflict (e.g., domestic disputes, gang activity) may carry over into the facility. Staff at the Cleveland Clinic (which has been using metal

detectors since 2016) confiscated 30,000 weapons (e.g., knives, box cutters, and guns) from patients and visitors in 2018 alone in its Northeast Ohio region. In a 2018 study by Omar et al. from Oakland University's William Beaumont School of Medicine, more than 70% of respondents reported experiencing any form of violence, nearly three-quarters had personally witnessed assaults during their shifts, and close to 22% frequently felt afraid of becoming a victim of violence. In addition, a 2022 report by the IAHSS Foundation found that EDs are among the highest-risk areas for workplace violence, with most ED nurses stating they have been hit or kicked while on duty.

Between 2010 and 2020, Joint Commission-accredited organizations reported 39 shootings in healthcare facilities that resulted in 39 deaths:

- 21 were staff members (10 were shot by a patient, five by a visitor, four by a family member, and two by a current or former staff member); and
- 18 were patients (15 were shot by a family member, two by a visitor, and one by another patient).

Nearly 30% of the shootings were murder/suicides (the report notes these were primarily mercy killings that resulted in the deaths of the patient and the shooter, typically a significant other). Another 2012 study published in the Annals of Emergency Medicine noted reasons for hospital-related shootings, including settling a "grudge," attempting suicide, "euthanizing an ill relative," and prisoner escape (11%). The same study found that nearly one-third of these shootings occurred in the ED area, followed by the parking lot and patient rooms.

However, these statistics only represent reported incidents. The bulk of workplace violence incidents occur in the emergency department and inpatient psychiatric settings (The Joint Commission, 2021). However, violence committed against healthcare workers is not limited to hospitals. It can happen in outpatient clinics, patient transport, in-home health settings, and pharmacies (one international literature review found that 65% of pharmacists included in these studies had experienced some form of workplace violence).

Security in healthcare facilities varies widely. Larger systems may have their own security forces. Others may employ local law enforcement officers (some working overtime). Not all healthcare facility officers carry guns, but they may carry handcuffs, batons, pepper spray, or conducted electrical weapons (e.g., tasers). Levels and the nature of training vary, too, as does the amount of formal collaboration between hospital security, emergency management, and local law enforcement.

Finally, workplace violence is expensive – in addition to treating physical injuries (e.g., concussions and lacerations), there are costs associated with the negative mental health effects survivors may experience (e.g., missing work or taking time off to seek behavioral healthcare). The healthcare field also just witnessed "The Great Resignation" (due, in part, to workplace violence and burnout) and must now invest heavily in recruitment and retention strategies, including workplace safety programs.

Risk Factors

As Jones noted in his May 2023 article, there are "warning signs and pre-incident indicators" of violent incidents that trained staff are more likely to notice and report. In the healthcare workplace, The Joint Commission notes that risk factors can include:

- Patients with various forms of mental illness;
- Patients in police custody;
- Stressful conditions (e.g., long wait times, crowding, being given bad health-related news);
- Lack of policies and training related to de-escalation;
- Gang activity;
- Domestic disputes among patients or visitors;
- The presence of weapons;
- Understaffing (including on-site security or mental health personnel and providers);
- Poor environmental design (e.g., lighting and factors that affect visibility in hallways, rooms, parking lots, and other areas);
- No access to emergency communication; and
- Unrestricted public access to healthcare facilities.

Risk factors can vary by location, too. Working in homes with limited space and skilled nursing facilities can present unique challenges to healthcare providers.

Legislative and Standards Changes

Updates to Federal Legislation

In 2023, OSHA convened a Small Business Advisory Review Panel to begin work on developing a new Prevention of Workplace Violence in Healthcare and Social Assistance standard. According to the press release and related fact sheet, topics OSHA is considering include:

- A programmatic approach to workplace violence prevention,
- Workplace violence hazard assessments,
- Workplace violence control measures,

- Preventive training,
- Violent incident investigations and recordkeeping,
- Anti-retaliatory provisions, and
- Approaches that avoid stigmatization of healthcare patients and social assistance clients.

Updates to State Legislation

Many states have recently passed new laws or established or increased penalties for assaulting healthcare workers. The American Nurses Association notes there is variation in these laws. In some states, the penalties only apply in specific settings (e.g., ED personnel, mental health personnel, and public health personnel). Laws protecting staff vary, too. Maryland, for example, is the only state not to require healthcare staff to put their full names on their name badges (thus making it harder for patients to target staff via social media or in person at their home addresses).

Updates in Standards

Due to a "high incidence of workplace violence," The Joint Commission released in January 2022 new workplace violence requirements for accredited facilities. These requirements focus on managing safety and security risks, collecting information to monitor environmental conditions, participating in ongoing education and training, and creating a culture of safety and quality. Before the update, The Joint Commission released a Compendium of Resources that includes information and links to resources hospital staff can incorporate when implementing these standards.

Steps Healthcare Facilities Can Take to Prevent Workplace Violence

As changes continue from a federal and state perspective, it is essential to note that there are several steps healthcare emergency managers can take to prevent, respond to, and recover from workplace violence incidents. First, healthcare facilities and systems must have a workplace safety and violence prevention and reporting program. Staff should be familiar with and comfortable knowing the definition of an incident and how to report it. Data collection could enable more tailored programs and policies.

Jones mentioned the importance of having threat assessment teams and protocols. In healthcare, security, social work, risk management, and nursing administration staff could collaborate on creating threat protocols:

- Forms like the Violence Reduction Protocol Treatment Plan and the Brøset Violence Checklist can be a good starting point.
- Providing staff with panic buttons and mobile applications can help monitor situations and notify security if, for example, an employee does not confirm receipt of a message.
- De-escalation training (for all facility employees) can teach staff how to interact with agitated patients, coworkers, and visitors.
- Making adjustments to the physical layout of facility areas (e.g., improving lighting and sight lines, using metal detectors or signage that implies they are in use, using sloped desks that are more difficult to jump over, providing additional egress points for staff) can create a more resilient workspace.

And finally, working with facility security and local law enforcement is crucial to building relationships when things are calm and ensuring the safest, best response possible. Routine visits and regular exercises can help first responders learn the layout of a facility and adjust healthcare staff expectations of the role of law enforcement during and after an incident (e.g., temporarily closing parts of the facility for evidence collection). Giving officers access to live camera footage can help them rapidly locate threats and victims. Stashing go-kits for law enforcement near the ED entrance can improve overall response time and help protect patients and staff while ensuring operations quickly return to normal.

To help healthcare planners prepare their facilities to mitigate, respond to, and recover from an armed assailant situation, the U.S. Department of Health and Human Services' Administration for Strategic Preparedness and Response's Technical Resources, Assistance Center, and Information Exchange (ASPR TRACIE) released a comprehensive On-Campus Healthcare Facility Armed Assailant Planning Considerations document (with assistance from IAHSS, The Joint Commission, and other subject matter experts). This document can be used as a checklist and includes links to free resources to help with workplace safety planning efforts. In conjunction with a top-down approach to workplace safety, tools like this help ensure healthcare facilities remain as safe and resilient as possible.

Corina Solé Brito, MA, has had the honor of working with first responders for nearly three decades. As a senior manager with the Police Executive Research Forum, she co-authored guides on preparing the law enforcement system for a public health emergency. She helped conduct case studies on four departments at various stages of pandemic planning. She served as the communications manager for the Substance Abuse and Mental Health Services Administration Disaster Technical Assistance Center, where she developed materials for disaster responders and survivors. Since its inception, she has managed communications for the U.S. Department of Health and Human Services' Administration for Strategic Preparedness and Response's Technical Resources, Assistance Center, and Information Exchange (ASPR TRACIE) project. Currently, she serves as the ICF International's deputy program manager.

Peachaya Tanomsup/Free Stock photos by Vecteezy.

Cybersecurity in Hospitals and the Public Health Sector

By Dan Scherr & Tanya Scherr

Healthcare cyberattacks continue to increase in frequency. The primary methods used in these attacks include phishing and email compromise (e.g., ransomware and other malware), fraud scams, network server breaches, inappropriate access to medical records, insider threats, and standard theft. In 2022, HHS published *The Impact of Social Engineering on Healthcare*, which found that phishing attacks were the top threat, representing 45% of all attacks. Ransomware (most commonly delivered through phishing emails, malicious links, or malicious advertising) accounted for another 17%, leaving almost two-thirds of all attacks deriving from these two vectors. Reporting on attacks against healthcare organizations outlines some malware and techniques used in recent years. The main takeaway for most practitioners is understanding every employee has a part to play in keeping organizations safe. The most robust and impactful defenses can be ineffective if employees fall victim to phishing attacks or fail to follow established protocols.

Hospital Corporation of America (HCA) Healthcare, one of the nation's leading providers of healthcare services, was recently targeted. Their data breach was one of the largest healthcare breaches in history, involving at least 11 million patients residing in 20 U.S. states. Additional notable cyberattacks on healthcare organizations in 2023 include:

- 8.9 million patients in May at Managed Care of North America (Georgia)
- 5.9 million patients in May at PharMerica (Kentucky)
- 3.4 million patients in February at RMG, LMO, ADOC & GCMG (California)
- 3.2 million patients in March at Cerebral, Inc. (Delaware)
- 2.5 million patients in June at Enzo Clinical Labs (New York)
- 2.5 million patients in April at Harvard Pilgrim, Point 32 Health (New Hampshire)
- 997K patients in March at Zoll (Massachusetts)
- 618K patients in February at CentraState Healthcare System (New Jersey)
- 559K patients in April at Murfreesboro Medical Clinic (Tennessee)

The recent HCA data breach is the 4th largest cyberattack on a healthcare organization in the U.S. The top 3 healthcare cyberattacks involved:

- 79 million patients in 2015 at Anthem (Indiana)
- 21 million patients in 2018 at American Medical Collection Agency (New York)
- 11 million patients in 2014 at American Medical Collection Agency (Washington)

Healthcare Cyberattacks Reported – The Numbers

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Breach Portal tracks breaches of unsecured protected health information when the event affects more than 500 patients, a reporting requirement under the HITECH Act. As of August 15, 2023, there were 901 breaches reported within the last 24 months (with the Breach Portal using a rolling report where older reports drop off and new ones are added as the calendar moves), including 355 from January to July 2023 (compared to 224 over the same period in 2022).

The healthcare industry is targeted based on the lucrative nature of its records, its vulnerability, and its visibility as this industry is considered one of the country's 16 Critical Infrastructure Sectors. According to the Cybersecurity & Infrastructure Security Agency (CISA):

> *There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.*

Healthcare is vulnerable and targeted, in part, due to the rapid adoption and deployment of technology driven by the COVID-19 pandemic and a lack of available cybersecurity talent to harden networks and strengthen defenses. The rapid scaling and implementation of technology to meet needs and demand during the pandemic produced a larger "attack surface that was less well defended." As hospitals focused on patient care, the attacks increased, stretching already thin resources to the limit, further constraining the ability to invest in additional security. As the industry works to close the gaps, recruitment and retention of cybersecurity professionals is a challenge, as lack of talent creates intense competition for services across industries.

It is critical for agencies and organizations to build a culture of compliance and awareness to protect the healthcare system and its patients.

The Healthcare and Public Health sector is the hub that protects all the other sectors against natural disasters, infectious diseases, outbreaks, and even terrorism.

Additionally, the compromised patient information (including credit card information, health insurance information, clinical detail) is worth a lot of money. The healthcare industry has increased its use of remote data, leaving each organization to address new vulnerabilities. Clinical workers need to have easy, streamlined processes to ensure timely care to patients. With the myriad of devices used in patient care, clinical workers are not always trained on cybersecurity measures, even though workers share data for patient care. Lack of training and outdated technology makes healthcare a desirable target and increases the healthcare industry's challenges. An increase in remote, off-site work creates new challenges for non-clinical workers. Studies show workers have become more comfortable using company computers for non-related work items, such as checking personal emails, social media, shopping, etc.

Not only is the information available in the healthcare setting valuable (with each healthcare record worth up to 10 times that of credit card numbers), but the attack surface is vast. According to the Healthcare Information and Management Systems Society (HIMSS) (a nonprofit organization focused on improving healthcare worldwide through information and technology), in addition to standard attack vectors, the attack surface includes:

> *[V]arious types of specialized hospital information systems such as EHR systems, e-prescribing systems, practice management support systems, clinical decision support systems, radiology information systems and computerized physician order entry systems. Additionally, thousands of devices that comprise the Internet of Things must be protected as well. These include smart elevators, smart heating, ventilation and air conditioning (HVAC) systems, infusion pumps, remote patient monitoring devices and others.*

Implications of the Attacks

The financial impacts of cyberattacks on healthcare organizations can be significant. Beyond the obvious implications if the hospital chooses to pay the ransom, there are other factors, such as HIPAA fines, cost to contact impacted patients, re-educate staff, and regain trust in the communities they serve. The financial impact often costs healthcare organizations millions of dollars for one attack. It is estimated that cyberattacks' economic impacts on healthcare organizations are three times higher than on other industries. IBM Security's Cost of a Data Breach Report 2023 states healthcare data breach costs increased 53.3% from 2020 to 2023 and marked the 13th year in a row as the sector with the most expensive breaches, averaging almost $11 million

per breach. The recovery cost for a cyberattack can be significant enough to shutter smaller hospitals, which may face additional barriers in adequately training security staff or affording cybersecurity insurance. The impact of a lost hospital is substantial in any location, but the loss of hospitals in rural areas can be devastating as the loss of a local facility may add significant commute and response times for medical care. There may also be an increased demand for service at remaining facilities, or patients may forego care entirely.

Attacks on healthcare are not just financial attacks – they are attacks on human life. These attacks put patients at risk, such as disrupting patient monitoring during electronic system downtime. The inability to see records, test results, appointments, scans and images, and real-time monitors can delay or prevent appropriate patient care. Additionally, manual updates to patient records can lead to a lack of communication, delay in care, or increased errors in patient care. System downtime can also lead to the cancellation of scheduled and elective care, ambulance diversion, and loss of communication with other hospitals and healthcare entities. Cyberattacks during periods of increased vulnerability – such as COVID-19 when the healthcare industry was already under significant strain – can lead to increased risk and impact on patients.

In the wake of the cyberattack on Scripps Health (San Diego, CA) in 2021, the University of California San Diego Health Center (UCSDHC) published a report tracking impacts on their hospital from the attack on the neighboring facility. The report noted increases in:

> [P]*atient census, ambulance arrivals, waiting room times, patients left without being seen, total patient length of stay, county-wide emergency medical services diversion, and acute stroke care metrics.*

These findings demonstrate the increased strain on functional hospitals in the wake of cyberattacks and follow the CISA reporting on the impacts of COVID-19 on the healthcare infrastructure. The CISA report noted the larger the strain, the larger the degradation in patient care and the cascading effects on infrastructure overall. The results of a cyberattack hitting a hospital or other healthcare facility ripple throughout the community as a wide-scale assault, not a pinpoint strike.

There have been growing concerns in recent years about the impact on patients in the event of cyberattacks, for example:

- A 2019 attack at Springhill Medical Center, Alabama, resulted in a lawsuit alleging responsibility for the death of a newborn. The lawsuit states that the medical center did not properly notify the patient of the cyberattack and led the patient to believe that operations were normal when monitoring was not up to par. Lack of fetal monitoring resulted in staff not realizing that the umbilical cord was wrapped around the baby's neck, resulting in brain damage and ultimate death.
- In 2020, a patient traveling via ambulance in Germany was diverted to another hospital due to an attack, delaying care for an hour – the patient died shortly after.
- A 2022 claim at a hospital in Des Moines, Iowa, stated that a child received five times the normal dose of a medicine due to system downtime due to an attack.
- In 2022, a patient's cancer treatment was delayed for a week due to an attack that prevented clinical staff from accessing the patient's treatment plan.

A 2021 Ponemon Institute study, Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care, surveyed more than 600 practitioners in healthcare organizations regarding cyberattacks and outcomes. Approximately one-quarter of respondents reported increased mortality rates after attacks, and over two-thirds noted disruption of care.

Path Forward – What Is Needed?

The need for additional support and training for healthcare has been discussed well beyond the sector, with two pieces of legislation introduced at the federal level. In 2022, the Healthcare Cybersecurity Act of 2022 was introduced in the Senate and House and would require HHS "to undertake activities to improve the cybersecurity of the healthcare and public health sector." Under this legislation, HHS would coordinate with CISA, which would provide threat indicators and defense measures available to all entities receiving information through HHS programs. Further, HHS would be required to provide training on risks and mitigation strategies to those across the sector and identify risks in rural, small, and medium-sized entities, workforce shortages, and other challenges. In 2023, senators also introduced S.1560, the Rural Hospital Cybersecurity Enhancement Act, which would require CISA:

> [T]*o develop and annually report to Congress about a workforce development strategy to address the unmet need for cybersecurity professionals in rural hospitals…*[*and*] *disseminate materials that rural hospitals may use to train staff about cybersecurity.*

Both pieces of legislation remain in the introductory stages with respective committees.

While Congress works to provide additional resources at that level, federal agencies and public-private

partners continue to provide resources and training for the Healthcare and Public Health sector. CISA offers a variety of resources across critical infrastructure sectors, from news and updates on threats to training, resources, and services. These resources range from how to set up an anti-phishing program for an organization to cyber-incident response and are identified by the topic and level (foundational to advanced). Training opportunities include cyber range events, exercises, incident response, insider threats, and more. CISA also offers several programs, including the Cybersecurity Awareness Program, which can provide individual users with additional information, resources, and tools to stay safe online. Resources specific to the Healthcare and Public Health sector include ransomware awareness and updates, information on malware and threat actors targeting healthcare, and explanations of Domain-Based Message Authentication, Reporting, and Conformance (DMARC) and Multi-Factor Authentication (MFA).

The U.S. Department of Health and Human Services also provides resources and training to the Health and Public Health Sectors. Many of these offerings are hosted and managed by the HHS' 405(d) Program, which is a collaboration between HHS and industry:

> *[T]o align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats.*

The initiative offers publications, education, news, and a resources library free of charge, including best practices, infographics, analyses, and more. In April 2023, the HHS 405(d) Program released three additional resources: *Knowledge on Demand, Health Industry Cybersecurity Practices (HICP) 2023 Edition, and Hospital Cyber Resiliency Initiative Landscape Analysis.*

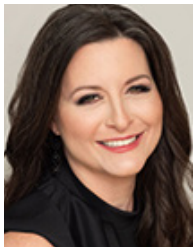
The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a federally funded organization that provides incident response support and information sharing to state, local, tribal, and territorial (SLTT) organizations at no cost, including free access to the Malicious Domain Blocking and Reporting (MDBR) tool. This tool prevents users' systems from connecting to harmful websites and mitigates malware, ransomware, phishing, and other threats.

HIMSS offers training and collaboration on safety and security matters and seeks to enhance systems' interoperability across healthcare. Organizations with local chapters can provide additional training, like the Cloud Security Alliance, ISACA, the International Information System Security Certification Consortium (ISC2), Information Systems Security Association (ISSA), and many others, depending on the budget and scope desired.

Conclusion

Ransomware and data breaches will likely continue to increase before effective controls can be found and implemented. Engaging with law enforcement partners before and immediately following a breach are opportunities to improve security and minimize impacts for organizations. As noted previously, the value of healthcare records and large attack surfaces make healthcare an attractive target, and one where cybersecurity often is seen as secondary as organizations focus on patient outcomes and scarce resources. A renewed focus on training and keeping up with changes in attack vectors and technical details of attacks will be crucial in the months and years ahead. With phishing the leading attack vector, concentrating on awareness and training in that area can provide the most significant return on investment. Engaging with users and building a culture of compliance and awareness, not for the program's sake but for the system's security and the safety of the patients, should be a focal point for investment and development.

Dan Scherr holds a Ph.D. in Public Policy Administration with a terrorism, mediation, and peace focus. He is an assistant professor in Criminal Justice and Homeland Security at the University of Tennessee Southern and program coordinator for the Cybersecurity Program. He is also a co-director of the Honors College. He is a Certified Fraud Examiner and Army veteran that served stateside during the September 11th attacks and has over two decades of experience in homeland security and operations.



Tanya Scherr holds a Ph.D. in Public Policy and Administration with a healthcare and emergency preparedness focus. She is an associate professor in Healthcare Administration for the University of Arizona and has over 28 years of healthcare experience. Along with being a Certified Fraud Examiner since 2011, she is also a former firefighter-emergency medical technician (EMT), previously licensed in several states, and holds national certification. She has held several executive and board of director positions for community nonprofits that focus on women's equality, domestic violence, and sexual assault.


EST 1998
Domestic Preparedness
Real-World Insights for Safer Communities
We Cover It All
Subscribe Today!