

DOCTORS

Volume 29, No. 1

Spring/Summer 2021



BUSINESS CONTINUITY WHAT'S YOUR PLAN?

find out...

- The proper steps to take when planning for a disaster
- How designating personnel for specific roles plays an integral part in business continuity planning
- The importance of business network security and its effect on proper business continuity

A LETTER FROM THE CHAIR OF THE BOARD

Dear Colleague:

What's in a plan? Since the pandemic, business continuity planning has become a vitally important part of safeguarding your practice. This first newsletter of 2021 will take you through what you need to put a plan in place and the importance of preparation to safeguard your operations for the future.



George S. Malouf, Jr., M.D., FACS
Chair of the Board
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate Insurance Company



ISSUE HIGHLIGHTS



PHYSICAL AND OPERATIONS PLANNING	1	COMMUNICATIONS AND OPERATIONS MANAGEMENT	3	KEY TAKEAWAYS AND ACTION REVIEW	6
----------------------------------	---	--	---	---------------------------------	---

DOCTORS RX

Elizabeth A. Svoisky, J.D., Editor
Vice President - Risk Management

Dr. George S. Malouf, Jr., M.D., Chair of the Board
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

Copyright © 2021. All rights reserved.
MEDICAL MUTUAL Liability Insurance Society of Maryland

Articles reprinted in this newsletter are used with permission. The information contained in this newsletter is obtained from sources generally considered to be reliable, however, accuracy and completeness are not guaranteed. The information is intended as risk management advice. It does not constitute a legal opinion, nor is it a substitute for legal advice. Legal inquiries about topics covered in this newsletter should be directed to your attorney.

All individuals involved in the creation and planning of continuing medical education activities sponsored by MEDICAL MUTUAL are expected to disclose to program participants any real or apparent conflict(s) of interest related to the content of their presentation. All individuals in control of content for this education activity have indicated that they have no relevant financial relationships to disclose.

CONTACT

Home Office Switchboard	410-785-0050
Toll Free	800-492-0193
Incident/Claim/ Lawsuit Reporting	800-492-0193
Risk Management Program Info	ext. 215 or 204
Risk Management Questions	ext. 224 or 169
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	mmlis.com proad.com



BUSINESS CONTINUITY WHAT'S YOUR PLAN?

Physicians and business owners were never more in need of comprehensive business continuity planning than in 2020. We made it through, and we learned a great deal about business adaptation and practical change. The questions facing us now are: "Where do we go from here as we slowly resurface from a global pandemic?" and "What changes do we still need to make?"

Many of us were forced to make significant and prompt modifications to our professional and personal lives with the onset of the COVID-19 pandemic. The more each of us had prepared for such an interruption, the better we fared. Doctors, specifically, were separated from their patients, their offices, and their peers. Often, the only solution was to render care remotely utilizing some version of telemedicine. Those with no prior experience with telemedicine found it slow and expensive to initiate such a program after the disruptive event occurred. This also was a problem with all other business aspects of running a practice. Our goal is to put you in a better place when the next disruptive event occurs.

In this article, we provide two real-life examples of substantial hurdles Maryland Doctors faced in 2020. These examples give further guidance for revisiting business continuity in 2021 and beyond. Whether your office must be temporarily closed due to a viral outbreak, shuttered for months and relocated, or digitally rebuilt from a network security breach, you can

mitigate the damage with appropriate planning and preparation.

PHYSICAL AND OPERATIONAL PLANNING

Consider the following example:

On Monday morning, your employee arrives to find the fire alarm activated and water running everywhere. A small fire started in the ceiling from a malfunctioning bathroom fan. The fire spread, causing smoke damage throughout much of the office. The fire then caused water pipes to burst, flooding the office (but, miraculously, put out the fire!). The network and phones are down. The business should be opening in minutes, but much of the staff now work remotely due to COVID-19, leaving few people to figure out what steps to take. Your office must be shut down.

The first steps to responding to this disaster hopefully took place long before the disaster itself. With foresight, you already had a written **business continuity plan** (maintained separately from your network servers) complete with a list of key individuals to notify, including a telephone communication tree to immediately contact employees and staff, an IT response plan for internet and remote accessibility, copies of insurance contacts and coverages, and contact information for all third-party vendors. You also may have identified an alternative work site plan to temporarily



**Jeremy R. Krum &
Ken Armstrong**
*Trial Attorneys
and Partners
at Armstrong,
Donohue, Ceppos,
Vaughan & Rhoades*



Is your practice prepared for an emergency?



Remember...

The best planning necessarily includes active involvement of your support staff. Having designated personnel appointed for specific roles and responsibilities can be a business-saving endeavor.

relocate your practice, depending on the type and length of the emergency event.

The best planning necessarily includes active involvement of your support staff. Having designated personnel appointed for specific roles and responsibilities (selected and appointed in the planning stage) can be a business-saving endeavor. You will need help not only for the immediate response and emergency incident but also for ongoing day-to-day business operations. Someone to handle both incoming and outgoing mail. Someone to handle checks. Someone to communicate with the landlord. Someone to communicate with contractors.

In our own legal practice, we have two sets of a comprehensive **incident response binder** (kept off-site with management personnel) containing all pertinent business information to restore and recover critical business functions, including an **emergency preparedness plan**. An emergency preparedness plan, stated simply, outlines procedures for responding to a workplace emergency, including any unforeseen situation that threatens the safety and welfare of employees and/or the public. This can include natural disasters such as fire, weather-related events, loss of power and/or utilities, as well as security threats and emergencies. An emergency preparedness plan should overlap with a **business continuity plan**, which includes risk assessment, maintenance of essential operations, restoration, and recovery. While planning and preparing can

be time-consuming, the work performed will pay dividends in reducing potential business interruptions following a disaster.

Written planning is essential for any business continuity event, but you also must have the physical and operational capability to implement the plan. For example, do your administrative staff and employees (who may be able to work remotely) have the resources they need? Are you prepared in the event that you have to rely on telemedicine if you do not have access to your practice? How would you transition to telemedicine if need be? Who will need a company laptop, complete with appropriate encryption and security protocols? Who will need a business issued cell phone, complete with remote wiping software? Who will handle vendor accounts, along with accounts receivable and accounts payable? Who will handle patient calls, patient questions, and patient appointments? Can you quickly transition from electronic medical record keeping to handwritten charting and vice versa?





One of the most significant consequences of a business interruption event is the actual length of time it takes to return to your operational baseline. Even a simple broken water pipe can result in several months of restoration efforts. While proper planning will not prevent the incident, well-thought-out preparation can help restore your practice's operations more quickly.

At its most basic level, a business continuity plan should include the following items and should be accessible off-site in both paper and electronic formats:

COMMUNICATIONS AND OPERATIONS MANAGEMENT

Notification Plan/Protocols: Who will be responsible for managing your business continuity plan?

Employee Emergency Contacts: Full name, cell phone numbers, and email addresses for all employees

Telephone Communications Tree: Each person on the call tree contacts the next person on the list and so on, until everyone has been contacted.

Contacts for Third Party Vendors: A list of all companies that the practice does business with, including phone numbers and email addresses

Insurance Policies: Copies of complete policies with producers' phone numbers and email addresses

Lease Agreements: A copy of the lease or ownership documents for the business(es)

location(s) with contact names, phone numbers and email addresses

Company Licenses/Registrations: A copy of all software and hardware license agreements or registrations along with contact information for the individuals who maintain your computer systems

Provider Licenses/Registrations: Copies of all state licenses and credentialing information, with usernames and passwords, so that renewals can be accomplished to maintain licenses for medical staff and third-party payor status

INFORMATION TECHNOLOGY (IT)

Emergency Contacts: First priority – get your computer systems back up and running. Know who to call immediately to get your computers working.

Network Diagram: Have a basic diagram and system review so that your IT provider will be able to rebuild and operate your system remotely for maintenance and repair.

Passwords and Access Controls: Make sure your Manager/Primary Responder has the usernames and passwords for all hardware and software system accounts stored in a secure physical location or an electronic password locker.

Bank Accounts/Credit Cards/

Payroll/401K: Obtain secure remote access to your bank accounts/payroll accounts/funding accounts so that all banking operations can be completed remotely if physical access to the office is restricted or impossible.



Did you know?

One of the most significant consequences of a business interruption is the actual length of time it takes to return to your operational baseline.



Don't forget training!

All staff and employees should not only be aware of business continuity planning and management but also should be actively involved in helping the practice execute and implement the plan when needed.

Secure Patient Lists/Contacts (Encrypted): Maintain a secure patient list with last known contact information on a regular basis (monthly/quarterly/annually).

EMERGENCY PREPAREDNESS

Emergency Call Centers/Locations: If a physical location is necessary or required, have alternate locations planned.

Workplace Emergency Plan/Training: Consider a training session to test your business continuity plan.

Evacuation Plan/Lockdown Protocols: Have an emergency evacuation plan and lockdown procedure in place for the safety of employees and, in the era of COVID-19, preplanned protocols for cleaning and preparing the physical premises for reoccupation.

PHYSICAL AND ENVIRONMENTAL SECURITY

Assets List and Property Photos: Annually, take photos of each office to document equipment present for insurance purposes.

Floor Layout: Update a copy of your floor plan annually.

Alternate Work Site Plan (If possible): Select a suitable location or temporary office site for 30-day use in an emergency and select who and what will be placed there to transition the office to more permanent reconstruction.

Don't forget training! All staff and employees should not only be aware of business continuity

planning and management but also should be actively involved in helping the practice execute and implement the plan when needed. Your practice might even consider getting staff and employees involved in reviewing and updating the business continuity plan each year. Knowing that the practice is prepared and ready for a disaster and knowing that the practice can adapt and accommodate staff in any situation will provide employees with reassurance, comfort, and job satisfaction.

BUSINESS NETWORK SECURITY

To no one's surprise, we saw a tremendous upswing in cybersecurity threats and ransomware attacks in 2020. With the ongoing transition to remote operations and telehealth, threat actors have targeted medical offices, clinics, and both small and large business owners. This trend is expected to continue.

In 2020, the following incident took place:

A Physician opens the front office preparing for the day's patient appointments. Times have been difficult, as several months of patient care have been lost due to COVID-19. Patients remain reluctant to return. However, appointments are finally starting to fill up again. The computers are turned on for the morning. The Physician sees no screen prompt. No Windows operating system. The Physician sees only a demand for \$10,000 in bitcoin.



All files have been encrypted. No patient schedules are available. No patient records are accessible. No radiographs are obtainable to view. The Physician learns that a remote desktop (provided for billing staff, working remotely) was not secure. Patient records have likely been accessed and taken. In addition to restoring computer operations, all patients for the practice must now be notified and informed of the security breach.

When it comes to network security, prevention is key. While most providers think, "It will never happen to me," threat actors have become savvier and more sophisticated. New methods are employed regularly, and bad actors are now finding ways to encrypt both servers and external backup tapes. We strongly recommend that providers retain and rely upon competent IT vendors. More importantly, we recommend that providers obtain vulnerability assessments of their computer systems and networks. Vulnerability assessments are generally affordable and cause little inconvenience. A forensic vulnerability review can identify significant weaknesses that your IT team may have overlooked.

If your network and electronic health records were disabled, could you notify your patients? Do you have a secure and encrypted list of all patient names and addresses, separate from your server, such that you could inform patients of a data breach? If a true data breach occurs, you must have a feasible strategy to rebuild

your network systems quickly, and you must have the ability to access and utilize patient data, including protected health information. We recommend having several redundancies in secured patient data, most importantly an off-site external copy of data that is not connected to any internal network device. The copy should be encrypted and kept physically secure.



Beyond business continuity and operations, you must respond to potential unauthorized access and/or exfiltration of patient data in compliance with the detailed reporting obligations of the Health Information Portability and Accountability Act (HIPAA) and applicable state laws. In the event of an incident like that described above, patients may become upset, frustrated, and may no longer have trust in your practice's security and privacy responsibilities. The business impact of such an event can be substantial. Thus, ensuring that your practice's network and data are secure is essential. Protecting your patients' data is vital to a



Business Network Security:

Beyond business continuity and operations, you must respond to potential unauthorized access and/or exfiltration of patient data in compliance with the detailed reporting obligations of HIPAA.

FOR MORE
INFORMATION, VISIT

MMLIS.COM/
BUSINESSCONTINUITY
OR
PROAD.COM/
BUSINESSCONTINUITY

successful practice, and network protections should be reviewed and reevaluated at least every two years, if not more frequently.

For more information on the cyber security resources offered by MEDICAL MUTUAL/ Professionals Advocate Insurance Company, please see page 9 of this newsletter.

A WORD ON VACCINES IN THE CONTEXT OF BUSINESS CONTINUITY

Finally, an additional concern for business continuity in 2021: vaccinations. While health care providers and employers may certainly desire that all employees and staff obtain vaccinations for COVID-19, employers also need to comply with federal and state employment laws and regulations, including providing reasonable accommodations for employees with disabilities and providing equal employment opportunities. Maintaining separate office pods, ensuring disinfection protocols continue and providing remote capabilities will likely remain for the foreseeable future. This landscape will likely continue to evolve and develop in the months and years to come.

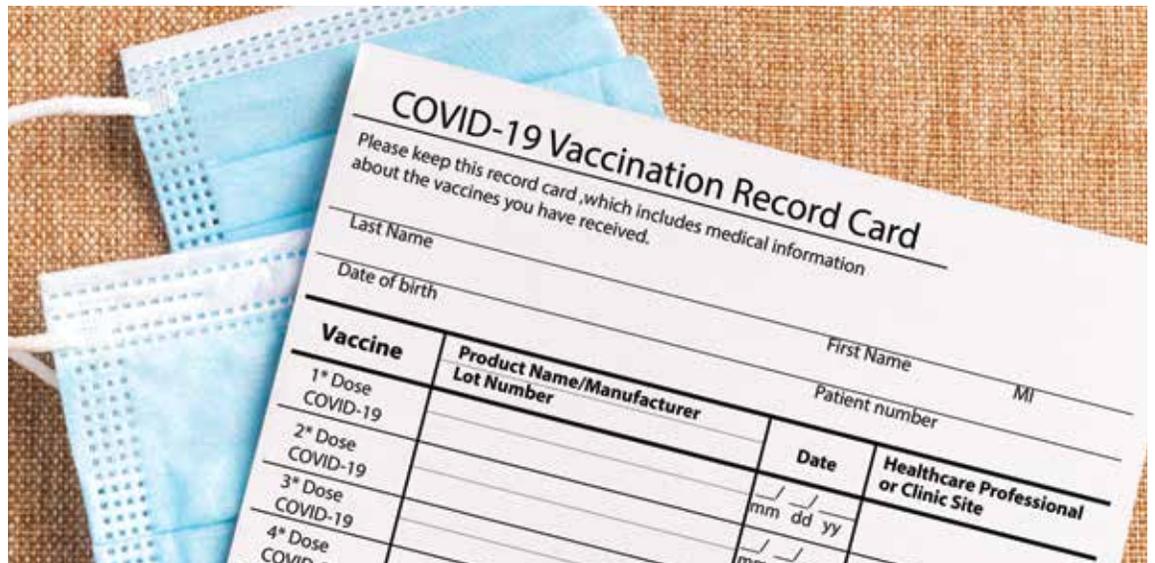
KEY "TAKEAWAY" POINTS – ANNUAL ACTION/REVIEW

- Review your business continuity plan and emergency preparedness plan every year.
- Update your telecommunications tree for all employees and staff.

- Update your vendors list and contact information.
- Update your assets list and property photos.
- Review your floor plan, evacuation plan, and network diagram.
- Assign roles and responsibilities to employees and staff for responding to an emergency or business interruption.
- Train your employees and staff on your business continuity plan and emergency preparedness plan.
- Review your business continuity plan and emergency preparedness plan with your IT team and consider obtaining a network vulnerability assessment.
- Maintain secure off-site copies of your business continuity plan and emergency preparedness plan.
- Maintain a secure and encrypted list of patient contact information separate from your network server. Consider using an encrypted external hard drive or an encrypted flash drive.

CONCLUSION

In summary, there is no question that the best approach for maintaining business continuity and responding to a business disaster is preparation, preparation, and more preparation. Every provider and business owner should revisit their plans for 2021 and review them with their organization and staff.



CME TEST QUESTIONS

1. Business continuity plans should be reviewed and updated every five years.
A. True B. False
2. Network vulnerability assessments can identify weaknesses overlooked by your IT team.
A. True B. False
3. Staff and employees should not be included in business continuity planning.
A. True B. False
4. A business continuity plan is the same as an emergency preparedness plan.
A. True B. False
5. Staff and employees may have remote access to your network server if proper security and encryption protocols are utilized.
A. True B. False
6. Most business interruptions are minimal, and you do not need to plan for them.
A. True B. False
7. Ongoing efforts to combat cybercrime have resulted in reduced network security threats.
A. True B. False
8. All pertinent business continuity data should be maintained on your secure network server.
A. True B. False
9. Remote access or mobile banking should be avoided.
A. True B. False
10. The best approach for maintaining business continuity is preparation.
A. True B. False

Instructions – to receive credit, please follow these steps:

Read the articles contained in the newsletter and then answer the test questions.

Mail or fax your completed answers for grading:

Med•Lantic Management Services, Inc. | Fax: 410-785-2631
P.O. Box 8016 | 225 International Circle | Hunt Valley, Maryland 21030
Attention: Risk Management Services Dept.

1. One of our goals is to assess the continuing educational needs of our readers so we may enhance the educational effectiveness of the *Doctors RX*. To achieve this goal, we need your help. You must complete the CME evaluation form to receive credit.
2. Completion Deadline: August 31, 2021
3. Upon completion of the test and evaluation form, a certificate of credit will be mailed to you.

CME Accreditation Statement

MEDICAL MUTUAL Liability Insurance Society of Maryland is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for Physicians.

CME Designation Statement

MEDICAL MUTUAL Liability Insurance Society of Maryland designates this enduring material for a maximum of one (1) *AMA PRA Category 1 Credit*.[™] Physicians should claim only the credit commensurate with the extent of their participation in the activity.

CME EVALUATION FORM

Statement of Educational Purpose

Doctors RX is a newsletter sent twice each year to the insured Physicians of MEDICAL MUTUAL/Professionals Advocate.[®] Its mission and educational purpose is to identify current health care-related risk management issues and provide Physicians with educational information that will enable them to reduce their malpractice liability risk.

Readers of the newsletter should be able to obtain the following educational objectives:

- 1) Gain information on topics of particular importance to them as Physicians
- 2) Assess the newsletter's value to them as practicing Physicians
- 3) Assess how this information may influence their own practices

CME Objectives for "Business Continuity, What's Your Plan?"

Educational Objectives: Upon completion of this enduring material, participants will be better able to:

- 1) Have a better understanding of physical and operational planning associated with business continuity
- 2) Learn a basic understanding of the elements of a business continuity plan
- 3) Address the complexities surrounding vaccines in the context of business continuity

	Strongly Agree				Strongly Disagree
Part 1. Educational Value:	5	4	3	2	1
I learned something new that was important.	<input type="checkbox"/>				
I verified some important information.	<input type="checkbox"/>				
I plan to seek more information on this topic.	<input type="checkbox"/>				
This information is likely to have an impact on my practice.	<input type="checkbox"/>				

Part 2. Commitment to Change: What change(s) (if any) do you plan to make in your practice as a result of reading this newsletter?

Part 3. Statement of Completion: I attest to having completed the CME activity.

Signature: _____ Date: _____

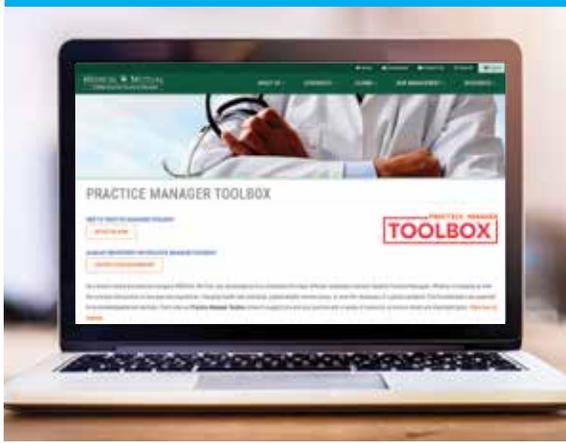
Part 4. Identifying Information: Please PRINT legibly or type the following:

Name: _____ Telephone Number: _____

Address: _____



RISK MANAGEMENT NEWS CENTER



EQUIP YOUR PRACTICE MANAGER FOR SUCCESS

Your Practice Manager is on the front lines of the business side of medicine. Provide the tools needed by encouraging them to register for our *Practice Manager Toolbox* (PMT). The online PMT offers guidance on a variety of topics, such as practice operations and EHR optimization. Sample resources include an employee handbook, hiring forms, and a confidentiality agreement. Finally, when Practice Managers register, they can select a free gift. For more details and to register, visit mmlis.com/practice-manager-toolbox-faq or professionalsadvocate.com/practice-manager-toolbox-faq



EVALUATE YOUR CYBER SECURITY WITH OUR ONLINE TOOL

As health care cyber breaches have risen in the past year, it is more important than ever to make sure you and your practice are protected. MEDICAL MUTUAL and Professionals Advocate offer a free online tool to help evaluate your practice's cyber security. The survey focuses on topics such as electronic security and PHI protection planning. After each question, you will receive practical feedback to help strengthen your I.T. system. For more information and to complete the survey, visit mmlis.com/security-survey or professionalsadvocate.com/security-survey



RESOURCES FOR BUSINESS CONTINUITY PLANNING

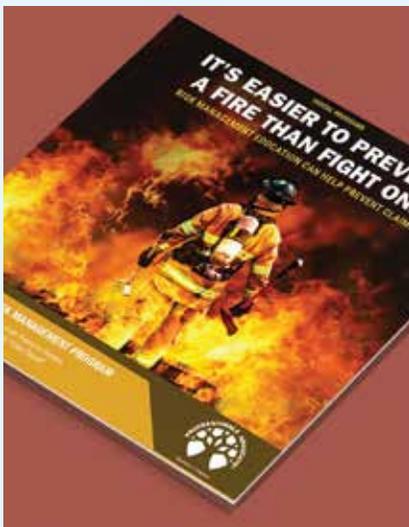
COVID-19 has shown that it's prudent to take the time to develop a robust business continuity plan. To assist you, we have compiled additional resources on how to prepare for an unexpected event in the future. At mmlis.com or proad.com, we offer guidelines about telehealth, office reopening procedures, Physician and staff wellness, and more. Much of this information comes from authoritative sources such as the CDC, the U.S. Dept. of Labor, the American Medical Association, and others.



To stay in the know about the latest risk management news and alerts issued by medical organizations, visit our web site at mmlis.com/rm-alerts and proad.com/rm-alerts

DOCTORS

Publication of MEDICAL MUTUAL/Professionals Advocate®



REGISTER NOW FOR A 2021 RISK MANAGEMENT EDUCATION PROGRAM

Our 2021 Physician risk management education programs run the gamut of topics, from opioid prescribing to HIPAA compliance. You can peruse and register for programs at mmlis.com/content/rm-education-programs or professionalsadvocate.com/content/rm-education-programs-pap

As you review the program descriptions, you will notice that, as in 2020, no in-person programs are currently scheduled this year. To ensure we continue to meet your risk management education needs while following guidelines for social distancing, we continue to host our program virtually via live webinars, home study and online courses. Eligible insured participants who complete a Physician risk management program will receive a 5% premium discount on their next professional liability insurance renewal policy. CME credits also are earned for completing a risk management education program.