

# Pandemic Preparedness

*Joint Written Project – SANS Technology Institute*

Authors: Jim Beechey, [beechey@northwood.edu](mailto:beechey@northwood.edu)  
Rob VandenBrink, [rvandenbrink@metafore.ca](mailto:rvandenbrink@metafore.ca)



# 1. Table of Contents

- 1. Table of Contents.....2
- 2. Introduction .....3
- 3. Technical Considerations.....3
  - 3.1. Virtual Private Network.....3
  - 3.2. Traditional VPN Alternatives.....6
  - 3.3. Business Communications.....7
  - 3.4. Work at Home Training .....8
  - 3.5. Data Center Management.....8
  - 3.6. Security Posture During a Pandemic .....9
- 4. Non Technical Considerations..... 11
  - 4.1. Business Unit Input ..... 11
    - 4.1.1. What data is critical? What servers? (Data classification) ..... 11
    - 4.1.2. Classification of Job Roles..... 11
    - 4.1.3. Business processes that require physical presence..... 12
  - 4.2. Corporate Process Issues ..... 12
    - 4.2.1. Electronic Methods ..... 12
    - 4.2.2. Physical Methods ..... 13
    - 4.2.3. Shipping and Receiving jobs..... 13
    - 4.2.4. Alternate Delivery Methods..... 14
- 5. Making things Mandatory ..... 17
  - 5.1.1. Vaccinations and Antiviral Drugs ..... 17
  - 5.1.2. Curtailing travel ..... 18
  - 5.2. Declaring your emergency..... 18
    - 5.2.1. Notifying Employees ..... 18
    - 5.2.2. Notifying Business Partners and Customers..... 19
  - 5.3. Pandemic Exercises ..... 20
- 6. Pandemic Specific Issues ..... 20
  - 6.1. Calendar considerations ..... 20
  - 6.2. Incubation Periods..... 21
  - 6.3. Infectious Period..... 21
  - 6.4. Symptoms..... 21
  - 6.5. Mortality Rates ..... 21
  - 6.6. “The Kid Factor” ..... 23
  - 6.7. Refusal to Participate..... 24
- 7. Conclusion..... 25
- 8. References..... 26
- 9. Appendix A - Pandemic Plan Checklist.....27
- 10. Appendix B - Sample Pandemic Plans.....29

## 2. Introduction

Worldwide concern over pandemics has increased greatly over the past few years due to high profile events such as the SARS outbreaks in 2003, Avian Flu (H5N1) concerns from 2003 - 2007, and, most recently H1N1 or swine flu. Predicting the severity of H1N1 is very difficult, however many health organizations such as the Center for Disease Control are warning businesses of the need to prepare for what could be a rough flu season. While organizations have spent significant time and money formulating their business continuity and disaster recovery plans, many of these plans do not account for the issues a pandemic can bring. Traditional DR (Disaster Recovery) plans focus on catastrophic events where business assets are damaged or destroyed. Pandemics hit hardest at an organizations most important asset, its people. Therefore, traditional DR plans are not adequate when planning for a pandemic. This paper details some specific technical and non-technical steps that organizations should take in considering a pandemic and its impact on their business.

## 3. Technical Considerations

### 3.1. Virtual Private Network

Virtual Private Networking is one of the staples of any pandemic preparedness plan. A VPN allows workers to connect, via the Internet, to the corporate network. The ability for work to continue while employees are at home is critical to continuity of operations. Most organizations already have VPN access for employees as part of their normal business operations; however simply having a VPN is not adequate. Companies need to plan for the challenges a pandemic can bring. “You need to be realistic and ask whether your existing IT infrastructure can support your entire workforce working from home at once. Business plans need to take into account how the IT systems work.”<sup>1</sup> Preparing an organization’s VPN for a pandemic requires a focus on six distinct areas.

First, when considering any VPN solution, the product decision often starts with a discussion about IPSEC client based VPNs and SSL based VPNs. IPSEC VPNs have been around longer and have a larger market penetration. They require client software to

be installed on any machine accessing the VPN. Typically, this requires pre-planning in terms of a pandemic situation. Users of SSL VPNs authenticate over secure web sessions. Applications are then provided via proxy or client software is pushed down for more fully featured network access. There are various pros and cons to either architecture, but either can be effective for pandemic situations. The key is to understand the technology you have, and any technical limitations that may affect your plan.

Second, a pandemic ready VPN must have adequate bandwidth as usage will likely skyrocket. When planning for a pandemic, take a look at what bandwidth levels are required for normal usage and estimate pandemic usage requirements based upon high absentee rates. Gartner estimates “a minimum of 40% absenteeism for as long as eight weeks during peak outbreaks” and “the possibility of absentee rates close to 100% in some organizations”.<sup>2</sup>

Third, VPN availability is critical during a pandemic. Redundancy in both the VPN solution itself and also the enterprise Internet connection is extremely important. Enterprise level VPN solutions should be deployed in a high availability configuration. Internet redundancy can be accomplished many ways, but is equally important. Larger organizations may choose the traditional route of deploying BGP (Border Gateway Protocol) across multiple providers. Smaller organizations might consider options built into already deployed firewalls and third party appliances. Products such as Barracuda Networks Link Balancer ([www.barracudanetworks.com](http://www.barracudanetworks.com)), ECESSA Power Link ([www.eccessa.com](http://www.eccessa.com)) and Radware LinkProof ([www.radware.com](http://www.radware.com)) are appliances capable of load balancing two or more Internet connections for redundancy and increased bandwidth. Many VPN clients have a “backup gateway” or similar option, which can provide effective redundancy without advanced load balancers or routing solutions.

Choosing Internet providers is also very important. Make sure that your providers are not limited to a single upstream provider. For instance, if two local companies both use AT&T for their backhaul to the Internet, your organization may still have a single point of failure. Organizations should also ask about provider fiber paths and ensure that different providers do not use the same path. Pandemic preparation is also a good argument for using a business class Internet provider. Small organizations may be

tempted to consider lower cost solutions from local cable or DSL providers. Consider what would happen if most of the local community was asked to stay in their homes due to a pandemic. Local ISPs bandwidth would likely be overrun depending upon the level of over-subscription and could cause performance issues for your organization while trying to compete for available bandwidth.

Fourth, many VPN products are licensed based upon user counts. Check to see how your VPN solution is licensed and make sure there is adequate licensing to cover 90% of the organization. This can be costly for solutions with licensing based upon concurrent user models. However, certain vendors provide special considerations for this type of scenario. Juniper, for instance, offers an ICE (In Case of Emergency) License to address this specific need. During emergency situations, the ICE license can be deployed for a limited timeframe to accommodate the increased demand for the VPN.<sup>3</sup> Even companies who do not offer such a service to all customers may be inclined to do so as part of the initial purchase negotiation. Consider the entire process though when evaluating these emergency licensing options. If contact with the vendor is required in order to implement increased licensing, how can your organization be sure the vendor will be operating if a pandemic is ongoing?

Fifth, during a pandemic event, VPN traffic will likely become a large portion of any organization's Internet traffic. For some organizations this is not a problem, but for others this could cause undesirable results for existing publicly available web infrastructure. Having the capability to prioritize incoming and outgoing Internet traffic is important during emergency situations. Some companies may want to give VPN traffic higher priority during an event while others may be more concerned with ensuring the availability of their public web sites. Most enterprise firewalls offer some rudimentary traffic shaping options. Enterprise customers concerned with prioritization should consider more dedicated solutions from vendors such as Allot, Cisco, NetEqualizer and Procera.<sup>4</sup> Note however that prioritizing internet traffic generally only applies to traffic as it exits the network; Internet Service Providers do not honor TOS or DSCP methods for end-to-end QOS.

Finally, it is important that your user community tests their VPN solution regularly, both to ensure that their solution works and to verify performance. In these days of “net neutrality” debates, it is not unheard of for an ISP to artificially degrade the performance of encrypted traffic. The rationale behind this is that encrypted traffic should be classified as “enterprise”, and a premium should be charged on home users generating enterprise traffic. The frustrating thing about these artificial throttles is that the ISP almost never notifies their clients when these limits are implemented, so it’s important that affected users test regularly for adequate performance.

### **3.2. Traditional VPN Alternatives**

Traditional VPN architectures certainly apply when thinking about pandemic planning. A traditional VPN is generally focused on simply getting the client computer connected to the corporate network in a secure manner. However, there are alternatives which should be considered for any deployment, but especially when thinking about a pandemic. The advent of SSL VPNs and virtualization has brought several new options for remote connectivity.

Citrix has a SSL based VPN solution called Client Access Gateway which can be used to provide virtual desktops and applications. “VMware offers an end-to-end solution called VMware View (formerly VMware Virtual Desktop Infrastructure (VDI)) that organizations use to provide remote users with access to virtual desktop machines that are hosted in a central data center.”<sup>5</sup> Combining these options can also provide solutions for organizations with several requirements. For instance, some organizations deploy SSL VPNs and provide full network access for company owned computers. However, computers not company owned are only provided RDP (Microsoft remote desktop) access to the users office workstation. This allows users to use the VPN without having to fully expose the corporate network up to home PCs.

Another solution is low-end virtualization products such as VMware ACE. This allows deployment of an “enterprise owned” computer, complete with VPN solution and business applications installed, often on a USB disk or memory stick. ACE images are generally considered isolated enough that they can be easily deployed on home

computers, without worrying about any malware that may be on those computers. Products of this type generally have additional features such as policy control over USB ports, expiry features and image encryption that make them attractive in enterprise deploys.

These alternative solutions have several advantages. First, they are easy for both end users and IT staff as they do not require software installations on home computers. Second, the user experience is very consistent with their normal day to day activities. The biggest negative these solutions can bring is that they often do not necessarily integrate well with corporate voice or video communications tools.

### **3.3. Business Communications**

Business communications during a pandemic are key to the success of an organization's plan. How do your employees communicate with customers, co-workers, suppliers and vendors? Technologies, such as VOIP and unified communications, have brought many new options to the table, however an organization's communications need to be re-evaluated based upon pandemic requirements.

Regardless of the telephony technology available in an organization, at a minimum employees need to be able to forward their office phone to home or mobile phones. This must be able to be accomplished remotely, without intervention from IT staff.

Beyond this basic need, VOIP technologies and unified communications solutions can dramatically help while staff are working from home. Organizations with these technologies should have a distinct advantage when dealing with a pandemic, assuming appropriate connectivity is available both at the corporate headquarters and the homes of its employees. Being able to continue to use the corporate phone system via soft phone, collaborate with co-workers, meet via video conference, chat using instant messenger and login to a call center remotely provide the tools necessary to keep business communications flowing while employees are unable to be in the office. Licensing is again another key caveat to consider during a pandemic. Many solutions license soft phone capability separate from traditional phone handsets. Organizations need to determine if licensing could become a concern as large percentages of employees may be working from home and attempting to use soft phone capabilities.

### 3.4. Work at Home Training

Enterprise users who work from home regularly are best prepared for the technical changes a pandemic can bring, but how prepared is your general user population? Is VPN access and any required client software standard for all users? Is there easily accessible instructions and training available in case large numbers of employees are required to telecommute? Many organizations use two-factor tokens for authenticating remote access users. If this technology is not used for other systems this may be a barrier to access for those not accustomed to using token technology.

One suggestion for preparation is to require all employees to telecommute at least once a quarter. This will help address any technical issues and give all employees a basic comfort level with telecommuting. This can also bring to light any unforeseen issues such as applications which do not work well over the VPN or processes which must still be performed in the office.

### 3.5. Data Center Management

The core of any organization's IT infrastructure is the data center. While the organization may be able to live without pockets of its IT resources, losing data center operations for any length of time could be catastrophic. The key question when it comes to data center management during a pandemic is: How does an organization manage its key resources without staff onsite?

Large data centers with 24/7 staffing can fall into a false sense of security as staff are always onsite. During a pandemic that may not necessarily be the case.

Organizations need to ensure that datacenter staff have both the same remote access as other departments, as well as additional access required specifically for datacenter tasks.

VPN access will be the most predominant method for data center management; however what happens if the network or Internet connection goes down? Off-network remote management tools are a critical piece to an organization's plan. For example, organizations need to have the capability to dial-in using standard phone lines and gain console access to network equipment. Systems Administrators need KVM (keyboard, video, mouse) solutions to access various servers in the data center either through direct attachment or IP. Organizations should ensure that these solutions include "out of band management" via dialup in case the network is unavailable. Also, sometimes nothing

Jim Beechey, [beechey@northwood.edu](mailto:beechey@northwood.edu)  
 Rob VandenBrink, [rvandenbrink@metafore.ca](mailto:rvandenbrink@metafore.ca)

works better than a good power cycle. Can your organization cycle the power on all critical pieces of equipment remotely? Solutions that can accomplish this are embedded in many modern server platforms, but many organizations are now using intelligent PDU's in their UPS infrastructure for this purpose.

Backups can pose an interesting problem for data center staff. Organizations can likely get away without staff entering the data center to change backup tapes for several days depending upon their library capability and capacity. However, at some point physical access is likely required in order to change tapes and rotate media to the appropriate off site location. The people responsible for this task should be identified in advance and have adequately trained backups.

Once the data center is properly equipped there are several considerations outside the data center itself. One of the more difficult issues is dial in access. Many people are moving to VOIP at home or simply using their cell phones. Organizations cannot assume that key staff members have standard dialup capability from home anymore. Should the company provide phone lines for key data center staff? Even laptops are coming with modems less frequently. In many cases, 3G access via dedicated cards or tethered cell phones are considered adequate alternatives to traditional dialup access. In many cases using a tethered cell phone for internet access in this way means that the voice functions of the phone are not usable at the same time. While these measures are not required for most employees, data center staff still may need them for redundancy purposes. Identifying and addressing these issues prior to a pandemic is critical. Organizations should consider drills placing their data center management group in various situations to see what capabilities would be lost if forced to work from home or if the network was unavailable.

### **3.6. Security Posture During a Pandemic**

During times of emergency, keeping the corporate security posture intact can be very challenging. Security policies and procedures may have to be more flexible during a pandemic; however this doesn't mean all the rules go out the window. Having previously agreed upon standards during emergency situations or specifically a pandemic can be extremely helpful. As with technical issues, preparation is the key to success. There are several security posture issues to consider and evaluate prior to a pandemic; however, in

Jim Beechey, [beechey@northwood.edu](mailto:beechey@northwood.edu)  
Rob VandenBrink, [rvandenbrink@metafore.ca](mailto:rvandenbrink@metafore.ca)

the end, each organization must evaluate these issues for themselves based upon their security requirements.

Data security can be very challenging during a pandemic. A pandemic situation is likely not going to strike an organization out of the blue. Consider the buildup as an organization gets closer and closer to having employees stay home. Also, remember that a pandemic is not a one or two day event, but rather could last weeks or months. Employees are likely to want to be prepared and that means taking data home both electronically and hard copy. From a technical perspective, encryption of laptops, removable media and mobile devices is the best option for protecting company data regardless of whether a pandemic is ongoing or not. Paper copies are a much different story. Organizations likely have existing policies regarding data classification and what can and cannot be taken outside the office. The question organizations should ask prior to a pandemic is whether or not these policies should change in times of emergency.

Workstation security can also be cause for concern during a pandemic. Consider operational type issues such as antivirus definition updates and security patches. Given the amount of time a pandemic could last, it is very likely that an organization may need to deploy workstation updates while employees are away from the office. Several questions need to be addressed:

- Should antivirus software be configured to download updates directly from the vendor as well as the corporate update server? This will ensure that machines that do not connect regularly to the VPN will still continue to receive updated virus definitions
- Do patch deployments typically run for VPN users? Can the VPN handle your regularly scheduled patch maintenance? Do patch deployments need to be broken up into separate pieces or staggered? Should clients be configured to automatically update applications and operating system files?

These questions often are contradictory with current organizational policies regarding control of the desktop environment. Organizations need to re-evaluate the risks/reward of such policies during a pandemic.

## 4. Non Technical Considerations

Of course building a pandemic plan requires a focus on much more than technology alone. Continuity of business operations is critical during a pandemic and as such, a pandemic plan will require many of the same components as any disaster plan.

### 4.1. Business Unit Input

#### 4.1.1. What data is critical? What servers? (Data classification)

Data classification is an important component in compliance discussions. The rationale behind this is that once data is classified, then you know what data and which servers fall under compliance regulations. However, server and especially process classification are both important when discussing Business Continuity Plans. Once business processes are classified, it becomes much easier to make intelligent decisions about which processes are important in running the business, which processes have dependencies on other processes, and which job roles are required to complete each critical business process.

#### 4.1.2. Classification of Job Roles

In security and especially in compliance frameworks, classification of data is a key starting point. This is not so much the case in pandemic planning where the key classification activity focuses on job roles.

We need to define what roles are critical and which people fill these roles. This is often the reverse of what management might expect. Management often wants to define which people are critical. It is important to remind them that disease is blind, critical people can fall ill, but the critical job responsibility still must be filled. It is important that job descriptions are accurate, and roles are defined completely.

Once job roles are accurately defined, it then becomes much simpler to define which roles are critical to the organization. Every job role is important, but the roles that are critical to the core business functions of the company need to be separated out and treated differently for the purposes of pandemic planning.

Critical job roles need to have significant backup on the personnel side. It is not uncommon to see 2 or even 3 backup people for a job role that involves critical service delivery. These backup people need to be aware that they have been named backups and

have their training kept up to date, such that, in the event of emergency they can step into the critical role with minimal fuss.

After classification of roles, it becomes much simpler to assess what additional training or skills transfer might be required in order to prepare for a pandemic or other emergency. Also, classification of job roles facilitates defining exactly what roles are required to run the corporation in the event of a pandemic. This makes it simpler to define exactly which jobs are required to create a “skeleton staff”, whether that staff is on the company premise or working from home.

#### **4.1.3. Business processes that require physical presence**

Classification of job roles also leads into the requirements of each job role. One of the critical components that should be assessed is requirements for physical presence. For instance, a shipping/receiving person, or an assembly technician in manufacturing both obviously need to be physically present to fill their roles. However, IT staff, managers and call center operators might all be able to work from home with appropriate technical tools and supports.

## **4.2. Corporate Process Issues**

Keeping an organization running during a pandemic is not just a matter of telling people to “work from home”. Care needs to be taken to ensure that physical requirements of a job role are met. There are certain aspects of any organization that likely require some level of physical access or interaction. Organizations need to consider where these areas are and what can be done to complete these tasks.

### **4.2.1. Electronic Methods**

If a job role requires a signature (as in Accounting or Engineering), the standard business process may need to be changed to allow this to happen electronically (via PKI digital signatures or scanned signatures for instance). Many companies have invested heavily in document management systems and workflow management. These applications fit perfectly into a pandemic plan as they allow business processes to continue without physically touching a piece of paper. Of course, new documents must be scanned into the system so these processes are not completely without human interaction.

#### **4.2.2. Physical Methods**

Production jobs, such as are common in manufacturing of course need a physical presence. The best practice in this case is to use a skeleton staff, and try to limit the travel and resulting exposure of your identified backup people. If a person in your production skeleton staff falls ill, it is probably best to identify who else in the primary staff might have been exposed (for instance, other members of that production line or team), and replace those exposed with their backup people. This is an attempt to deal with the incubation period, so that you don't bring your backup person in just to be infected by a primary person who might not be showing symptoms yet. The major effort in this area is not only to keep your primary people as healthy as possible, but also to place as much or even more importance on keeping your backup people healthy in case they are needed to step in.

Information sharing on the specific characteristics of the illness in question is extremely important. People who have fallen ill need to know key symptoms of the illness and how long they are likely to be contagious during any pandemic event. Coming to work when showing symptoms or coming back to work too soon is one instance where a "good work ethic" is not helpful. Coming back to work while still contagious is simply the best way to infect 10 other people and worsen the impact on the organization.

#### **4.2.3. Shipping and Receiving jobs**

Shipping and receiving job roles have a significantly higher risk than others as these people deal with delivery companies (couriers and truck drivers). Job roles that involve delivery should be considered as "pathogen delivery roles". Any job that involves seeing people in several different companies (or more) per day can carry a more significant risk than others.

Most delivery and trucking companies have pandemic plans in place and attempt to mitigate the risk of contagion with frequent hand washing, the use of disposable masks while outside of the truck cab, etc. However, it is still prudent to impose similar measures on the job roles that face delivery personnel.

#### 4.2.4. Alternate Delivery Methods

One of the biggest challenges for organizations who rely heavily on shipping to deliver goods or person to person contact is how to continue their core business activities during a pandemic. A severe pandemic may impact services such as shipping companies or a business's ability to meet face to face with customers. Therefore, organizations need to consider what, if any, alternate delivery methods are available during a pandemic. The following list contains suggestions for possible alternate delivery methods using existing companies as examples. The list is not meant to be exhaustive, but rather stimulate ideas about how individual organizations could develop creative ways of continuing business during a pandemic.

1. Colleges/Universities - Universities who must close campus still may be able to continue classes via various tools such as Blackboard or Moodle (course management), Illuminate or Wimba (web course delivery), podcasting or even simply telephone conference calls instead of meeting in person. Assignments and tests may have to be more creative than standard in class testing, however there are alternatives already being used in today's online only classes.
2. Software Vendors - Many companies already deliver software via Internet download. During a pandemic most software manufacturers would like need some form of Internet distribution. Vendors would need to weigh the risks of this method versus potential business loss with in person delivery.
3. Video Rental - Companies such as Netflix provide delivery of DVDs directly to a customer's home. While the company already has a limited video streaming capability, most DVDs cannot be streamed live. During a pandemic having the capability to stream all DVDs rather than having to delivery to homes would create a significant competitive advantage.
4. Banks - Banks might have to revert to delivering services either online or via ATM only. Luckily, most are already comfortable with these methods, however banks may need to provide detailed instructions for those customers who are more comfortable going inside a branch office.
5. Food/Groceries - One of the more challenging and interesting issues is how people would get necessary food and supplies during a pandemic. Stores with

- automated checkout systems may be able to continue to provide services with minimal staff.
6. Book Delivery - Traditional book delivery can be supplemented during a pandemic by the myriad of options that e-books provide. Vendors like Amazon already have an alternate delivery method with their Kindle platform. Other publishers should consider their options during these times. Could DRM protected files fill the void until traditional shipping methods became available?
  7. CD/DVD Sales – The music industry has already begun to embrace the electronic distribution of content via sites such as iTunes. However, pandemic times may entice companies to consider expanding these offerings to complete CDs or DVDs. Offerings could include burnable iso images and extras such as printable CD labels or inserts.
  8. Diagnostics – Especially during a pandemic, medical resources are stretched to the limit. Using electronic methods of medical delivery such as videoconference style diagnostics and electronic radiology systems not only maximize the use of limited, valuable resources, but also limit the exposure to infection to these people. Remote diagnostics are currently used most frequently to service remote communities that cannot support an advanced diagnostic infrastructure, generally due to geography, climate and/or community size. Many small communities in the Canadian north have advanced diagnostic services delivered in this way. The Telehealth network in Africa delivers diagnostics and a large number of other medical services
  9. Surgery – Telesurgery (surgery by remote control) is not yet a commonplace service, but is being actively developed in several major centers. The requirement for expensive hardware support is a significant barrier to entry for this service. In addition, the rapid evolution of the technology is a factor that tends to keep this as a research area, as it has yet to stabilize long enough to make a commodity solution practical. The market for telesurgery is very similar to that for remote diagnostics. However, consultation and mentoring during surgery are mature services that are in common use today. Nurses for instance are often assisted by

senior mentors either via telephone or remote video services, especially in remote areas where they are the only health care professionals.

10. Medical Hotlines – Medical hotlines are a common service in many countries. These services are generally staffed by Registered Nurses, and provide a remote service for triage, preliminary diagnosis and advice on treatment direct to patients. The advantages of these services during a pandemic are significant. Not only are diagnostics done earlier, and treatments started quicker, but patients are told to stay home. This keeps infected patients home where they cannot spread the pathogen. Just as important, services of this type keep patients who are not infected away from the healthcare system, which during a pandemic can be a very effective control. During a pandemic, it would be expected that these services will be heavily advertised in the media, both as a treatment and as a containment tool.
11. Therapy - Counselors, psychiatrists and therapists will certainly be important during a pandemic as stress levels increase. These organizations could certainly continue to provide services over the phone, but could be much more effective via other means. Video conferencing would be an effective alternative so both parties could continue to see body language, etc. Therapy and psychiatry are commonly provided to remote communities either via telephone or video links. It would be expected that these services would be expanded during a pandemic event. Recent studies have shown that using text messaging for cognitive therapy treatment of clinical depression not only are as effective (or in some cases, more effective) than traditional, in-person therapy, but the course of treatment is generally completed in roughly 50% of the time. This provides benefits in a more timely fashion to the patient, as well as dramatically improving the number of patients a therapist or psychiatrist can help. <sup>6</sup>
12. Professional Training – Training roles can be filled using remote training platforms. The SANS vLive and onDemand training are good examples of this approach. The Sanjay Gandhi Postgraduate Institute of Medical Sciences (SGPGIMS) has been delivering medical training over remote video links since

1999. This started as an experiment in delivering training for endocrine surgery to remote students in India, and has seen continued success since it was introduced.<sup>7</sup>

## 5. Making things Mandatory

Defining mandatory actions in preparation for, or during a pandemic, is an important area for an organization to define in advance. Almost always, these decisions require cooperation with your HR department, unions or staff associations. Often these are very difficult decisions which could have contractual or legal impact. Organizations should consider the following list of possible mandatory actions when thinking about pandemic preparedness.

### 5.1.1. Vaccinations and Antiviral Drugs

Vaccinations are a common action that is made mandatory for staff. The thinking is that if you are vaccinated, you are at reduced risk for becoming ill, and if you become ill, the severity of your case will be reduced. Mandatory vaccinations are common in healthcare and emergency services.

The problem is that vaccinations by their nature are almost never effective during a pandemic. A pandemic is by definition a disease that humans have low or no resistance to, with a high infection rate. If an effective vaccine is available, then the pandemic can be effectively curtailed or “stopped in its tracks”. In addition, vaccines that are developed on a crash schedule are not always the gold standard that you might desire. For instance, the 1976 swine flu vaccination was associated with an increased incidence in Guillain-Barré Syndrome.<sup>8</sup>

If no vaccine is available, the last resort is antiviral drugs. Antiviral drugs do not cure anything, but have been shown to be effective in reducing the symptoms of many influenza strains and in some cases preventing infection. However, the major antiviral drugs that are now available have some nasty side effects in a small percentage of patients. Issues such as confusion, depression and suicidal tendencies have been seen.<sup>9</sup>

In addition, it's becoming apparent that newer strains of influenza are now more likely to be resistant to Tamiflu.<sup>10</sup> Drugs such as Relenza or Rimantidine offer alternatives, but the longer term scenario looks like an “arms race” between development of the virus and the effectiveness of associated antiviral drugs.

The best defense in the general population is encouraging traditional methods for restricting the spread of disease, as well as education around recognizing symptoms and limiting spread. In the absence of effective vaccines or other drugs, there is just no substitute for plain old hand-washing, proper “sneezing protocols”, and staying home if you are show any symptoms.

### **5.1.2. Curtailing travel**

A common practice in curtailing the impact of a pandemic is to curtail traffic. This is common both in corporations and at a personal level. The virus of current concern (H1N1) has seen significant media coverage of “geographies at risk”. For instance, in the spring of 2009, Mexico was highlighted as an area at risk, to the point that travel agencies were refunding vacation itineraries and actually returning home proved a major challenge to vacationers caught in the country at the wrong time.

## **5.2. Declaring your emergency**

### **5.2.1. Notifying Employees**

During an emergency, it's important to notify the people who are most affected. The most obvious group of people who are affected by a corporation's pandemic plan are the employees of the corporation. Notification of employees is traditionally done by “telephone trees”. A telephone tree is a series of phone calls, starting with the pandemic team, and generally follows the corporate hierarchy. Because of the nature of pandemics, 2 or 3 alternates should be identified for each critical “node” in the tree (typically department managers).

Telephone trees can be automated with modern PBX's, where a single message (commonly called a “one call message”) can be sent out to all employees' contact numbers. This automated approach is very fast, but confirmation is limited to responses on the telephone keypad. Generally speaking, it is expected that a “one call blast” will

see a high volume of callbacks, where employees request or provide additional information.

Using emails or text messages to replace telephone trees has typically not proven effective. While every corporation has its cohort of people who compulsively check their email several times per hour, a large proportion of employees simply do not check their corporate email when not at work. Telephone trees remain the most effective method of communicating critical information for many corporations.

The challenge with using word of mouth is the propensity for the story to change over time. Organizations should consider delivering a short, concise message to employees then refer them to a web page or voice message with further details. Consistency in the message delivery can help diffuse employee concerns regarding both health and work performance during a stressful time.

### **5.2.2. Notifying Business Partners and Customers**

Business partners are the other group that is commonly included in notification during declaring a pandemic emergency. No organization wants to upset existing relationships. Keeping your partners and customers informed can go a long way to continuing positive relationships during tough times.

Suppliers are generally notified in order to reduce the quantity of goods ordered as the business will be expected to run at reduced capacity. Suppliers also may be requested to use alternate delivery protocols.

Customers are generally notified to expect reduced shipments, disruption in shipping schedules or alternate delivery methods. No customer wants to have delays or reduced services, however understanding what is likely to happen ahead of time can deflect much of the backlash such a situation could bring.

In addition, both suppliers and customers may need to be notified if they have an increased risk of infection in doing business with your company. For instance, if your shipper or receiver was recently diagnosed as infectious, notifying affected courier companies would be the responsible thing to do.

### 5.3. Pandemic Exercises

Pandemic training should be exercised regularly. Even if training goes well, people will forget their training very quickly if it isn't exercised within a few weeks of completion. Common errors such as incorrect use of equipment can result in infection of critical personnel. For instance, Canadian inspectors actually removed their protective masks when they fogged up while checking a swine herd in Alberta.<sup>11</sup> A recent study shows that roughly three fourths of the population put a common mask on incorrectly.<sup>12</sup> In fact, this same study showed the same issue in trained healthcare professionals (65% of a small sample). In addition, common but important things like hand-washing and sneeze protocols can be reinforced by posters in prominent places in the workplace.

These indicators only highlight the importance of exercises in limiting contagion. They do not touch on the importance of training in other aspects of pandemic planning, such as filling an unfamiliar job function, contacting employees, etc.

## 6. Pandemic Specific Issues

### 6.1. Calendar considerations

As is widely published in the media, in North America the typical “influenza season” occurs in the colder months, generally running from December to April.<sup>13</sup> This has less to do with the virus than our behavior. When the weather gets cold, we spend more time indoors, in close proximity to others. To compound matters, windows and doors stay closed, and we re-circulate warm air to maximize the efficiency of our heating systems. Influenza viruses also tend to survive longer in the warm, dry air that results from artificial heating. These factors work together to maximize the spread of contagion, person-to-person.

Projections are that the current virus (H1N1) appears ready to start spreading earlier, with estimates targeting an increased rate of spread starting in September of 2009 (shortly after schools open).

## 6.2. Incubation Periods

The incubation period is the interval after the infection is contracted, but before symptoms are apparent. Seasonal influenza has an incubation period of 1-3 days. H5N1 (avian flu), has an incubation of 3-5 days, with 7 days possible in some cases.

The incubation period for H1N1 is not so well defined, but estimates place it close to H5N1, at 5-7 days.

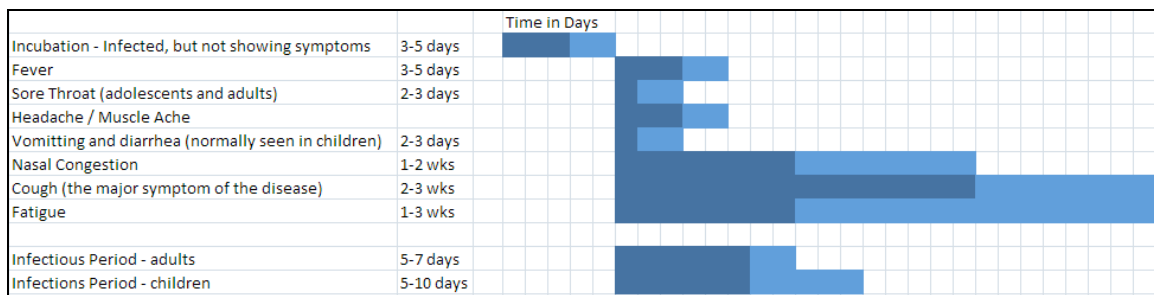
## 6.3. Infectious Period

Adults with influenza are typically infectious 3-5 days after onset of symptoms. Children can be infectious up to 7 days after onset. Some strains (H1N1 for example), see longer infectious periods - up to 7 days after onset in adults, and up to 10 days for children.

## 6.4. Symptoms

Influenza symptoms begin after the incubation period, and follow a typical course:

- Fever and sore throat for 3-5 days. Vomiting and diarrhea is typically seen only in children.
- Headaches and muscle aches – 3-4 days
- Nasal congestion 2-3 weeks
- Cough (the major symptom of influenza) – severe for 7-10 days, can last up to 2-3 weeks
- Fatigue 3-5 weeks after onset

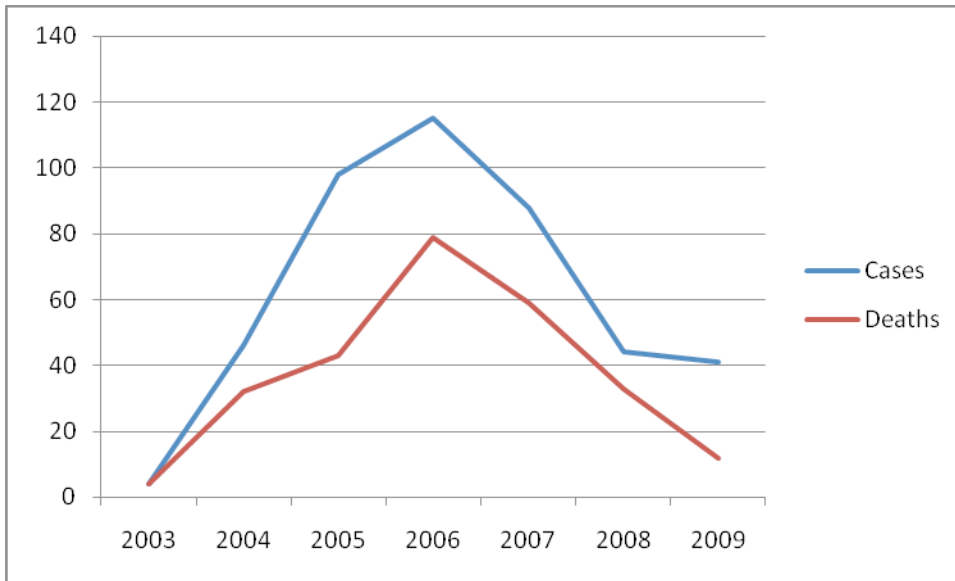


*Typical Influenza Symptoms Timeline*

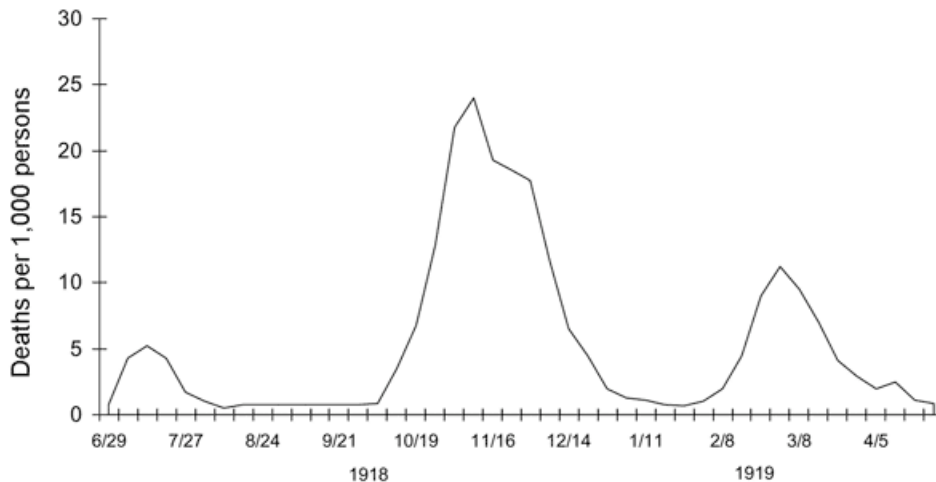
## 6.5. Mortality Rates

Influenza viruses tend to have multi-year “lives”, with a typical strain generally having per-year rates of infection similar to the bell curve we’re all familiar with from

our school days. For example, the graphs showing infection and mortality from the H5N1 Avian Flu virus and the 1917-1919 influenza pandemic are shown below.



*H5N1 infection and mortality rates*<sup>14</sup>



*Three pandemic waves: weekly combined influenza and pneumonia mortality, United Kingdom, 1918-1919*<sup>15</sup>

Notice the low numbers of both cases and mortality in the H5N1 case. By contrast, every year influenza season sees 5% to 20% of the population infected, more than 200,000 people hospitalized in the United States. In the US, about 36,000 people

die from flu-related causes each year.<sup>16</sup> Worldwide, 10-15% of the population contracts an influenza virus each year.<sup>17</sup>

The “pandemic” viruses that we’ve seen in recent years have all shown low absolute numbers for both infection and mortality, in comparison to the common flu viruses that we see each year. The fear is that a variation will emerge that humans have a low resistance to, resulting in a strain that is both more contagious and more lethal than commonly seen. To date this hasn’t happened, but if (or more properly, when) this happens, our city’s dense populations and global travel will likely result in a much more rapid and complete spread than was seen in the last pandemic of 1917-1919.

## 6.6. “The Kid Factor”

Pandemics are generally seen as 2 waves of absenteeism. The first wave can be expected when children fall ill due to the spread of influenza in the school system. When a child falls ill, parents will of course either take sick days, personal days, or will work from home (if possible) in order to take care of their children.

Following the initial infection, it’s a very common occurrence that after staying home to take care of a sick child, a parent might themselves be infected. This leads to a “double hit” to the organization, where a sick child ends up costing what amounts to an absentee day count of two infection periods. Not only that, a parent might return to work while in the incubation period and infect other co-workers before they realize they are infectious. In these cases a “good work ethic” will actually harm a company’s overall productivity and posture towards a pandemic. A good practice is to ask parents to stay home for a few days (depending on the incubation period of the disease in question) to ensure that they are not infectious before returning to work. While this cycle often starts with children being the first to become ill, it can work the other way as well, with parents falling ill first, and then infecting their children.

This is an area of ongoing research, hard numbers are not readily available but most parents of school age children see this empirically every year.<sup>18</sup> Organizations need to recognize and support the reality of this effect. Supporting parents in their family

responsibilities is not only important in retaining key employees and being a generally good “corporate citizen”, it’s key in containing spread of any pathogen.

The “Kid Factor” can also be used to a company’s tactical advantage. Media reports aside, if it is known that a pandemic is active but not yet in your area, a large cohort of parents taking time off for sick children can be a good indicator that it’s time to trigger your formal pandemic plan. To this end, it is important that during periods of higher risk, that the people responsible for pandemic planning (normally a committee or team) have direct access to absentee statistics and permission to contact absent employees directly to verify status. It is also important to support parents caring for children who have fallen ill. Fostering an environment of trust and openness in these matters should result in your committee or team receiving more accurate information which they can then use to act on more appropriately.

## **6.7. Refusal to Participate**

Organizations must recognize that pandemics and similar events place an inordinate amount of personal stress on the people in any organization. Planning for this is critical so that in the event of a real emergency, contingency plans are in place to deal with key personnel who may have agreed to a “physical presence” role at the company premise, but refuse to come in when the chips are down. Even if they are only responsible for a remote access presence, with a service delivery responsibility based on electronic or voice communications, any pandemic plan should always account for the fact that family responsibilities will always come first. If a child or spouse is ill, the effort and energy that you might expect towards company operations simply will not be there (nor should it be). The character traits that make your best, most dependable people valuable to your organization will also make these same people unavailable to you in unpredictable patterns during a pandemic.

It’s common for pandemic plans to recognize this, and either encourage or require staff to stay home in the event of any household pandemic illness. This tends to limit transmission of illness, as the intent is that staff are directed to stay home until they are sure they are not contagious. In addition, it cloaks in policy what people will do anyway, so has the side effect of improving morale.

## 7. Conclusion

A pandemic can put any organization under a great amount of stress. Pandemics are very different from most organizational threats as they attack people directly. An organization can quickly lose a large percentage of its most important asset, its people, for a lengthy timeframe. The key for any organization to successfully navigate a pandemic is having policies and procedures defined, communicated and tested in advance. Focusing on both technical and non-technical issues will serve organizations well. The most important thing any organization can do is to put the health and welfare of employees and their family's first. Not only will this create goodwill and trust, but in the end, the most important goal is getting employees healthy and back to work as quickly as possible. No plan will ever be perfect; however organizations who prepare the most thoroughly are most likely to be successful at navigating a pandemic.

## 8. References

1. [http://www.cio.com/article/491484/\\_Questions\\_for\\_Pandemic\\_Planning?page=3&taxonomyId=1419](http://www.cio.com/article/491484/_Questions_for_Pandemic_Planning?page=3&taxonomyId=1419), Internet 2009.
2. [http://www.gartner.com/DisplayDocument?ref=g\\_search&id=961512&subref=simplesearch](http://www.gartner.com/DisplayDocument?ref=g_search&id=961512&subref=simplesearch), Internet 2009.
3. <http://www.juniper.net/us/en/local/pdf/datasheets/1000171-en.pdf>, Internet 2009.
4. <http://www.processor.com/editorial/article.asp?article=articles%2Fp2816%2F07p16%2F07p16.asp>, Internet 2006.
5. <http://www.vmware.com/solutions/desktop/remote-branch-office.html>, Internet 2009.
6. <http://www.academyofct.org/Library/InfoManage/Guide.asp?FolderID=149>, Internet 2002.
7. [http://www.idrc.ca/openebooks/396-6/#page\\_109](http://www.idrc.ca/openebooks/396-6/#page_109), Internet 2009.
8. <http://www.cdc.gov/FLU/about/qa/gbs.htm>, Internet 2003.
9. <http://psychcentral.com/news/2006/11/15/fda-warns-about-suicide-delirium-associated-with-tamiflu/411.htm>, Internet 2009.
10. <http://www.scientificamerican.com/blog/60-second-science/post.cfm?id=widespread-tamiflu-resistance-spark-2009-03-02>, Internet 2009.
11. <http://www.montrealgazette.com/technology/Inspectors+checking+Alberta+farm/1815347/story.html>, Internet 2009.
12. [http://scienceblogs.com/effectmeasure/2007/04/putting\\_a\\_mask\\_on\\_wrong.php](http://scienceblogs.com/effectmeasure/2007/04/putting_a_mask_on_wrong.php), Internet 2007.
13. <http://www.phac-aspc.gc.ca/chn-rcs/flu-grippe-eng.php>, Internet 2008.
14. [http://www.who.int/csr/disease/avian\\_influenza/country/en/](http://www.who.int/csr/disease/avian_influenza/country/en/), Internet 2009.
15. <http://www.cdc.gov/ncidod/eid/vol12no01/05-0979-G1.htm>, Internet 2006.
16. <http://www.cdc.gov/flu/keyfacts.htm>, Internet 2009.
17. [http://www.euroflu.org/html/faq\\_influenza.html](http://www.euroflu.org/html/faq_influenza.html), Internet 2005.
18. <http://news.stanford.edu/news/2000/february23/cm-v-223.html>, Internet 2000.

## Appendix A – Pandemic Plan Checklist

### Preparation and Planning

Do you have business (non IT) people involved in the planning process?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is there a time commitment on the part of staff to complete the planning process?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Do you have a budget to complete your plan?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Do you have a budget to implement your plan?	<input type="checkbox"/> Y	<input type="checkbox"/> N

### DR Plan checklist

Have you identified job roles critical to the operation of the business?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Have you identified primary personnel for each critical job role?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Have you identified backup personnel for each critical job role?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is a process in place to notify all personnel that the pandemic plan is in force?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does this process include a confirmation?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Can critical job roles be delivered remotely or via alternative methods?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Have you identified technical resources required by critical job roles	<input type="checkbox"/> Y	<input type="checkbox"/> N
Have you identified alternative delivery methods for critical job roles (VPN in many cases)	<input type="checkbox"/> Y	<input type="checkbox"/> N
If required, is there a scheduling process in place to maintain a skeleton staff of required onsite personnel?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does this process account for a potentially higher infection rate in this part of your staff?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does your skeleton staff require additional protections from infection (procedures, facemasks, and other bio-gear?)	<input type="checkbox"/> Y	<input type="checkbox"/> N

### Technical Issues

Does your remote access method (VPN or VPN alternative) have sufficient bandwidth to service all critical job roles simultaneously	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is your VPN or VPN alternative licensed to service all critical job roles simultaneously?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does your remote access method have an alternate path via a different carrier?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Are the two carrier uplinks independent?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is there an alternate remote access method for IT, especially data center staff (dial in, 3G or cell phone tether?)	<input type="checkbox"/> Y	<input type="checkbox"/> N
Do personnel identified for key job roles require VOIP or other business communications infrastructure?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is the VOIP or other communications infrastructure licensed?	<input type="checkbox"/> Y	<input type="checkbox"/> N

Is the VOIP infrastructure license sufficient for all critical job roles to access simultaneously?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Has a list of IT tasks requiring on-site presence been completed?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Has the pandemic plan been assessed from a security and compliance perspective?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Are critical personnel aware of what data they can or should have on their local disks?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Are critical personnel aware of how to sync their local data back to the corporate systems?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does patch management account for extended telecommuting periods?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does the antivirus update process account for extended telecommuting periods?	<input type="checkbox"/> Y	<input type="checkbox"/> N

### Non-technical issues

Is the list of suppliers who need to be notified that your pandemic plan is active completed?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is the list of customers who need to be notified that your pandemic plan is active completed?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Do you periodically require critical staff to telecommute?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does this plan include metrics for success?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Have all identified critical personnel completed a successful “telecommute day” within the last 2 months?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Are there methods for testing the pandemic plan entire?	<input type="checkbox"/> Y	<input type="checkbox"/> N
If so, does this test have metrics for success?	<input type="checkbox"/> Y	<input type="checkbox"/> N
If so, has a pandemic test drill been completed successfully within the last 3 months?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is it appropriate to require staff to be vaccinated?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is it appropriate to require staff to take antiviral drugs if infected?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Should travel be curtailed during periods of higher pandemic risk?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Does your plan account for illness of spouses or children?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Are staff encouraged or required to stay home if they have family ill?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Has staff been made aware of basic methods of preventing infection?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Are these methods encouraged and publicized in the workplace?	<input type="checkbox"/> Y	<input type="checkbox"/> N
Is staff been aware of infectious periods? (Do they know when they should stay home and when it’s safe to come to work?)	<input type="checkbox"/> Y	<input type="checkbox"/> N

## Appendix B – Sample Organizational Plans

- Sonoco  
[http://www.sonoco.com/sonoco/cor\\_avian\\_flu.htm](http://www.sonoco.com/sonoco/cor_avian_flu.htm)
- State of Maine Pandemic Plan  
<http://www.ag-security.com/Library/Avian-Influenza/State%20Pandemic%20Plans/Maine.pdf>
- Western Illinois University  
[http://www.wiu.edu/rmep/documents/WIU\\_PPRP.pdf](http://www.wiu.edu/rmep/documents/WIU_PPRP.pdf)
- American College of Emergency Physicians (ACEP)  
<http://www.acep.org/WorkArea/DownloadAsset.aspx?id=45781>
- Cornell University  
[http://www.epr.cornell.edu/docs/pandemic\\_plan9\\_20.pdf](http://www.epr.cornell.edu/docs/pandemic_plan9_20.pdf)
- Purdue University  
[http://www.purdue.edu/emergency\\_preparedness/pdf/Pan\\_Flu\\_Plan\\_v2\\_-\\_FINAL\\_15%20Dec%202008.pdf](http://www.purdue.edu/emergency_preparedness/pdf/Pan_Flu_Plan_v2_-_FINAL_15%20Dec%202008.pdf)