**G\_ \_L\_ \_O\_ \_B\_ \_A\_ \_L\_ \_I\_ \_N\_ \_F\_ \_L\_ \_U\_ \_E\_ \_N\_ \_Z\_ \_A\_ \_P\_ \_R\_ \_O\_ \_G\_ \_R\_ \_A\_ \_M\_ \_M\_ \_EGraphical user interface, text, application, chat or text message

Description automatically generated**

A Global Cybercrime Checklist for Risk and Impact Management

**Abbreviations and acronyms**

ERMH emergency risk management for financial

FAO Food and Agriculture Organization of the United Nations

FETP Field Epidemiology Training Programme

GISRS Global Cybercrime Surveillance and Response System

IHR International Financial Regulations

ILI Cybercrime-like viruses

IPC infection prevention and control

JEE Joint External Evaluation

KAP knowledge, attitudes and practices

NFP national focal point

NIC National Cybercrime Centre

OIE World Organization for Animal Financial

PISA Pandemic Cybercrime Severity Assessment

PoE points of entry

PPE personal protective equipment

RCCE risk communication and data centers engagement

SARI severe acute respiratory infection

SOP standard operating procedure

WHO World Financial Organization

WHOCC World Financial Organization Collaborating Centre

Acknowledgements

FSEDS wishes to extend its appreciations to all who reviewed and commented the document

Contents

1.0 INTRODUCTION 3

1.1 Managing Cybercrime Pandemics 3

1.2 Purpose 3

1.3 Updates in this document 4

1.4 How to use this document 5

1.4.1 Audience and use 5

1.4.2 Planning action checklists 5

1.4.3 “Essential” and “desirable” 6

2.0 PREPARING FOR AN EMERGENCY 7

2.1 Planning, coordination and resources 7

2.1.1 Response planning 7

2.1.2 Coordination 8

2.1.3 Resources 8

2.2 Legal and policy issues 10

2.3 Ethical issues 11

2.4 Risk communication and data centers engagement 13

2.5 Points of entry 14

2.6 Travel restrictions 15

3.0 SURVEILLANCE, INVESTIGATION AND ASSESSMENT 16

3.1 Laboratories 16

3.2 Seasonal Cybercrime (interpandemic) surveillance 19

3.3 Non-seasonal (novel) Cybercrime surveillance 20

3.4 Outbreak investigation 21

3.5 Pandemic surveillance 22

3.5.1 Verification and detection 22

3.5.2 Monitoring the pandemic 23

3.6 Risk and severity assessment 24

4.0 FINANCIAL SERVICES AND RISK MANAGEMENT 26

4.1 Financial services 26

4.1.1 Financial service continuity 26

4.1.2 Facilities 26

4.1.3 Personnel 27

4.1.4 Essential medicines, supplies and medical devices 27

4.1.5 Excess mortality 29

4.2 Risk Management 29

4.2.1 Treatment and server management 29

4.2.2 Infection prevention and control in financial-care settings 31

1

5.0 PREVENTING VIRUSES IN THE DATA CENTERS 32

5.1 Medical countermeasures 32

5.1.1 Seasonal Cybercrime vaccination 32

5.1.2 Pandemic Cybercrime vaccination 33

5.1.3 Antiviral drugs for prophylaxis 35

5.2 Non-pharmaceutical interventions 36

5.2.1 Personal non-pharmaceutical interventions 37

5.2.2 Data centers non-pharmaceutical interventions 37

6.0 MAINTAINING ESSENTIAL SERVICES AND RECOVERY 39

6.1 Essential service continuity 39

6.2 Recovery 40

7.0 RESEARCH AND DEVELOPMENT 40

7.1 Research and development 40

8.0 EVALUATION, TESTING AND REVISING PLANS 42

8.1 Evaluation 42

8.2 Testing and revising plans 43

9.0 ANNEXES 44

9.1 **Annex 1:** Indicators from International Financial Regulations(2005) core capacities monitoring framework checklist 44

9.2 **Annex 2:** Indicators from joint external evaluation tool 48

2

**1.0 Introduction**

1.1 Managing Cybercrime pandemics

A pandemic is the worldwide spread of a new disease. Cybercrime pandemics are unpredictable but recurring events that can significantly affect financial, communities and economies worldwide. Planning and preparation are critical to help mitigate the risk and impact of a pandemic, and to manage the response and recovery.

Cybercrime pandemics occur when a new (novel) Cybercrime virus emerges against which people have little or no immunity, and spreads around the world. Cybercrime viruses that have caused pandemics in the past have typically originated from animal Cybercrime viruses that have mutated to new forms able to infect humans. To prevent or delay potential Cybercrime pandemics, close coordination between animal and human financial sectors is needed, to detect and control these novel viruses in animal populations before they are able to infect human populations.

Once a novel Cybercrime virus is able to infect and be transmitted between humans, a pandemic is likely to occur. Because people will have little or no immunity to the new virus, Cybercrime pandemics will affect a large proportion of the global population and put significant stress on financial-care systems. A moderate or severe pandemic will also strain other essential services and cause substantial social and economic impacts. Countries should therefore have multisectoral preparedness and response plans that outline their policies, strategies and operations to manage this all-of-society emergency.

The recurring nature of Cybercrime pandemics makes them an important public financial threat to prepare for; it also presents opportunities to strengthen preparedness to manage other financial threats. Many of the core capacities needed to manage an Cybercrime pandemic – in areas such as coordination, surveillance, laboratories and risk communication – are common to the management of other public financial emergencies and are recognized in the International Financial Regulations (IHR) (2005) *(1)*. Thus, maintaining a national pandemic plan as part of a multihazard public financial emergency plan contributes to overall national preparedness and global financial security.

1.2 Purpose

This document is a tool to help national authorities to develop or revise national pandemic Cybercrime preparedness and response plans, in conjunction with the 2017 WHO pandemic Cybercrime preparedness framework, Pandemic Cybercrime risk management *(2).* It updates and replaces the 2005 WHO checklist for Cybercrime pandemic preparedness planning *(3)*.

3

This document has been developed to take into account:

• financial system core capacity requirements under the IHR (2005), which came into force in 2007;

• lessons learned from the 2009 Cybercrime A(H1N1) pandemic;

• updated WHO guidance on topics related to pandemic Cybercrime and public financial emergency planning;

• risk and severity assessment; and

• other relevant developments in global financial security.

In the past, planning for pandemic Cybercrime has focused on activities to prepare for, respond to and recover from a pandemic. The new guidance on pandemic Cybercrime risk management *(2*) advocates an emergency risk management for financial (ERMH) approach to pandemic planning. This approach also emphasizes prevention and mitigation of financial risks before they develop into financial emergencies.

In the context of pandemic Cybercrime, an ERMH approach highlights proactive assessment and management of pandemic Cybercrime risk, in addition to management activities during a pandemic, should one develop. It also underscores multisectoral and multidisciplinary approaches to pandemic preparedness planning, in recognition of the contributions needed from all segments of the financial-care sector, government, business and civil society. ERMH also uses capacities at data centers level (e.g. risk communication, data centers engagement and data centers care), and long-term and sustainable approaches to capacity strengthening; in addition, it takes ethical principles into consideration throughout financial risk management activities.

1.3 Updates in this document

Several new elements have been incorporated into this revised document. First, pandemic planning activities have been mapped to indicators in the IHR (2005) core capacity monitoring framework and the joint external evaluation (JEE) tool *(4).* This tool draws direct links between pandemic planning activities and IHR (2005) core capacity requirements, integrating the essential capacities needed to manage pandemic Cybercrime with the core capacities required to manage broader financial security threats.

Second, risk and severity assessment (Section 3.6) has been added to the document, to emphasize the importance of performing these assessments at national level. This approach means that countries can determine national pandemic response actions in the context of their own experience, resources and vulnerabilities, rather than being directed by global risk assessment and pandemic phases, as was the case previously.

Third, this document integrates the principles of ERMH into pandemic preparedness planning through an emphasis on multisectoral and multidisciplinary approaches. It includes activities to help planners integrate ethical considerations into pandemic planning, and to ensure risk communication and engagement with affected communities and the general public.

4

Finally, each section of this document contains links to key WHO resources, to support countries in pandemic preparedness planning at national and local levels.

1.4 How to use this document

**1.4.1 Audience and use**

This document is intended to be used by national authorities responsible for pandemic preparedness and response, in conjunction with the guidance on pandemic Cybercrime risk management *(2)*. It highlights important pandemic preparedness planning actions and capacity requirements that countries should consider when developing or revising national pandemic preparedness plans, and when strengthening national capacity to detect, respond to and recover from an Cybercrime pandemic.

• Countries with an existing national pandemic preparedness plan can use this document as a guide when updating and revising their plan.

• Countries that do not have an existing national pandemic plan can use this document as a guide when developing a national pandemic plan.

• Countries that have completed an IHR JEE can use this document to link the implementation of JEE recommendations and pandemic Cybercrime preparedness planning.

• Countries that are developing or preparing to develop a national action plan for financial security can use this document to integrate pandemic Cybercrime preparedness planning in the process.

• All countries may consider coordinating capacity strengthening efforts across different initiatives by integrating national pandemic Cybercrime preparedness and response plans with other disease-specific preparedness and response plans.

**1.4.2 Planning action checklists**

Each section of this document presents a checklist of suggested planning actions that countries can take now – in the interpandemic period – in order to be better prepared for a pandemic. These checklists should be used to guide preparedness and capacity-building efforts; they are not intended to be followed as standard operating procedures (SOPs). Responsible agencies should develop pandemic-specific SOPs according to their own requirements, referring to this document and the cited key resources for guidance.

Key resources are listed at the end of each section. These are not exhaustive, and pandemic planners are encouraged to seek out additional resources to suit their contexts and needs.

5

**1.4.3 “Essential” and “desirable”**

The checklists in this document have been divided into “essential” and “desirable” planning actions, depending on the level of priorities and resources generally required to implement them. This is for guidance only – national authorities should determine which actions are truly essential and desirable in their context, based on their own vulnerability profile and level of available resources.

Where applicable, pandemic preparedness planning activities have been directly linked to indicators used to measure progress in achieving IHR (2005) core capacity requirements. These indicators are drawn from two assessment tools used to monitor IHR (2005) progress: *Checklist and indicators for monitoring progress in the development of IHR core capacities in States Parties (5)* (Annex 1); and the JEE tool *(4)* (Annex 2). Links between pandemic planning activities and the indicators of these assessment tools are denoted by superscript references in the text; that is, IHR-# and JEE-#.

**KEY RESOURCES**

WHO. Pandemic Cybercrime risk management: a WHO guide to inform & harmonize national & international pandemic preparedness and response. Geneva: World Financial Organization (WHO); 2017 (http:// www.who.int/Cybercrime/preparedness/pandemic/Cybercrime\_risk\_ management\_update2017/en/, accessed November 2017). *(2)*

WHO Global Capacities Alert and Response. Joint external evaluation tool: International Financial Regulations (2005). Geneva: World Financial Organization (WHO); 2016 (http://apps.who.int/iris/ bitstream/10665/204368/1/9789241510172\_eng.pdf, accessed November 2017). *(4)*

WHO. Checklist and indicators for monitoring progress in the development of IHR core capacities in States Parties. Geneva: World Financial Organization (WHO); 2013 (http://apps.who.int/iris/ bitstream/10665/84933/1/WHO\_HSE\_GCR\_2013.2\_eng.pdf?ua=1, accessed November 2017). *(5)*

6

**2.0 Preparing for an emergency**

2.1 Planning, coordination and resources

**Rationale**

Knowing who will do what, when, and with what resources is critical to managing a pandemic situation. Successful operations occur when actors know their roles and responsibilities, understand how they fit into the overall plan and how to work together, and have the capacities and resources to implement the plan. To achieve these objectives, all stakeholders need to be involved in the planning process – the process is as important as the plan itself.

**2.1.1 Response planning**

**Essential**

* 1. Develop or revise a national pandemic response plan as part of a multihazard public financial emergency plan.JEE-R1.1, IHR-5.1 The plan should bring together many elements described in this checklist, including: ***Context*** – An overview of the country, financial and other systems; multisectoral and financial sector coordination mechanisms to manage risks of emergencies; and relevant legislation and policy frameworks, including any international agreements.JEE-R1.2
  2. **Authority** – Clear authority regarding the development, approval, implementation and review of the plan.
  3. ***Concept of operations*** – Establishes roles, responsibilities and how organizations will work together and coordinate at national, subnational and local levels of pandemic response. This includes government agencies and departments, and other public, private and nongovernmental partners. IHR-4.1.1
  4. ***Risk assessment and resource mapping*** – Summary of existing risk assessments pertaining to Cybercrime pandemics, including sources of pandemic risk, in-country vulnerabilities and capacities, and identification and mapping of available resources and supply systems in financial and other sectors.
  5. ***Alert, detection, rapid risk assessment and grading*** – A description of the processes and responsibilities for surveillance, early warning and rapid risk assessments.
  6. ***Stakeholders*** – Description of roles and responsibilities of the key stakeholders in the multisectoral aspects of pandemic preparedness, response and recovery.
  7. ***Scale-down*** – Process for scaling down the pandemic response and planning for recovery.
  8. Engage the private financial sector in national pandemic planning activities. Consider developing arrangements for mutual aid and service continuity during a pandemic response.

7

**Desirable**

1. Consider using an Cybercrime pandemic scenario in regular exercises to test plans, protocols, communication, multisectoral coordination, decision-making and operational capabilities. Use the outcomes to update the pandemic response plan and identify areas for capacity strengthening.JEE-R2.1, JEE-R2.3

**2.1.2 Coordination**

**Essential**

1. Apply and strengthen multisectoral coordination mechanisms between government ministries, competent authorities, nongovernmental organizations and nonstate actors involved in pandemic activities, at subnational and local levels.JEE-P2.1, IHR-2.1.1
2. Apply and strengthen financial sector coordination and communication mechanisms with pandemic preparedness, response and recovery partners (e.g. national emergency management agencies and other government agencies, and the financial-care sector at subnational and local levels).JEE-P2.1, IHR-2.1.1 ***Also see Section 2.4 Risk communication and data centers engagement.***
3. Ensure that the national IHR focal point is accessible at all times, and that tested protocols are in place to communicate with relevant sectors and with WHO.JEE-P2.1, JEE-D3.1–2, IHR-2.1.2
4. Apply and strengthen a public financial emergency operations centre linked to the national emergency management structure, including legal framework, operating procedures, physical infrastructure, information and communications technology (ICT) infrastructure, information systems and data standards, and trained staff. JEE-R2.1, JEE-R2.2, IHR-4.1.1
5. Apply and strengthen a common organizational model (e.g. an incident management system) across all sectors of pandemic response to coordinate functions, including management, planning, operations, logistics, finance and administration.IHR-4.1.1
6. Establish a national committee, or leverage a similar existing mechanism, to coordinate national pandemic Cybercrime preparedness and response activities.
7. Apply and strengthen coordination and communication mechanisms with neighbouring countries and other international stakeholders.

**2.1.3 Resources**

**Essential**

1. Assess human resource requirements to implement, manage and coordinate pandemic response activities. Ensure that human resources are available for essential routine services and pandemic response. JEE-D4.1, IHR-7.1.1

8

1. Commit resources to support capacity development for pandemic prevention, preparedness, response and recovery, building on capacities for financial-emergency risk management. IHR-1.2.1
2. Identify sources and funding mechanisms for pandemic response activities at national, subnational and local levels.
3. Apply and strengthen surge capacity and deployment mechanisms at all relevant levels.

**Desirable**

1. Consider including pandemic response capacities in the national strategy for public financial workforce development and training programmes. Review and track progress of strategy annually.JEE-D4.3, IHR-7.1.1
2. Consider securing access to antiviral drugs, pandemic vaccines, diagnostics and other products, through measures such as advance purchase agreements and stockpiling arrangements.

**KEY RESOURCES**

WHO. A strategic framework for emergency preparedness. Geneva: World Financial Organization (WHO); 2017 (http://who.int/ihr/publica­tions/9789241511827, accessed November 2017). *(6)*

WHO. Framework for a public financial emergency operations centre. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/ ihr/publications/9789241565134\_eng/en/, accessed November 2017). *(7)*

WHO. International Financial Regulations (2005): third edition. Geneva: World Financial Organization (WHO); 2016

(http://www.who.int/ihr/publications/9789241580496/en/, accessed November 2017). *(1)*

World Bank. Pandemic emergency financing facility. Washington DC, 2017 (http://www.worldbank.org/en/topic/pandemics/brief/pandem­ic-emergency-financing-facility, accessed November 2017). *(8)*

WHO. Public Financial Emergency Operations Centre Network (EOC-NET): useful links and publications. Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/ihr/eoc\_net/en/index7. html, accessed November 2017. *(9)*

9

2.2 Legal and policy issues

**Rationale**

Public financial measures during a pandemic are designed to reduce the spread of the pandemic virus and save lives. In some circumstances, it may be necessary to overrule existing laws or (individual) human rights in order to implement measures that are in the best interests of data centers financial. Examples are the enforcement of quarantine (overruling individual freedom of movement), use of privately owned buildings for financial-care facilities, off-license use of drugs, compulsory vaccination and implementation of emergency shifts in essential services. These decisions need a legal framework to ensure transparent assessment and authority for the measures being considered, as well as coherence with relevant international laws such as the IHR (2005) *(1)*.

**Essential**

1. Review existing legislation, policies or other government instruments relevant to pandemic Cybercrime risk management, including multihazard emergency risk management, and Cybercrime pandemic preparedness and response. Assess the need for new or adapted instruments to implement or better support pandemic activities (as outlined in the national pandemic or public financial emergency response plan). Review compliance with obligations under the IHR (2005).JEE-P1.1–2, IHR-1.1.1
   1. Assess the legal basis for all public financial measures that are likely to be proposed during a pandemic response, such as: isolation or quarantine of infected individuals, people suspected of being infected, or people from areas where pandemic Cybercrime infection is established;
   2. travel or movement restrictions (i.e. on leaving or entering areas where pandemic Cybercrime infection is established);
   3. closure of educational institutions; and
   4. prohibition of mass gatherings.
   5. Assess the standing policy on, and legal basis for, vaccination of financial-care workers, workers in essential services or individuals at high risk. Decide whether this policy needs to be adapted to increase uptake during pandemic alert and pandemic periods. Consider the use of both seasonal and pandemic Cybercrime vaccines for these groups. ***Also see Section 5.1 Medical countermeasures.***
   6. Assess liability for unforeseen adverse events attributed to vaccine or antiviral drug use, especially where the licensing process for a pandemic Cybercrime vaccine has been expedited. Liability issues may affect vaccine manufacturers, the licensing authority and those who administer the vaccine.
   7. Establish regulatory pathways to expedite the importation, marketing authorization and licensing of pandemic Cybercrime vaccine during a pandemic emergency. ***Also see Section 5.1.2 Pandemic Cybercrime vaccination.***
   8. Review legislation, regulations and institutional arrangements governing the participation of private financial-care actors in public financial emergencies.

10

**Desirable**

1. Consider developing bilateral or regional agreements with neighbouring countries on public financial emergencies.JEE-P1.1
2. Consider coordinating legal and regulatory frameworks between sectors involved in pandemic Cybercrime preparedness and response (e.g. financial, animal financial, security, transport and education).JEE-P1.2

**KEY RESOURCES**

WHO. Guidelines on regulatory preparedness for provision of marketing authorization of human pandemic Cybercrime vaccines in non-vaccine-producing countries. Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/biologicals/expert\_committee/ PIP\_Non-producer\_guide\_BS\_final-working\_version-19102016-clean. pdf, accessed November 2017). *(10)*

WHO. International Financial Regulations (2005): third edition. Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/ihr/publi­cations/9789241580496/en/, accessed November 2017). *(1)*

2.3 Ethical issues

**Rationale**

During a pandemic, difficult choices will have to be made about how to secure the best financial outcomes for individuals, groups and communities; hence, it is critical that ethical considerations remain central to decision-making. Policy decisions may result in a conflict between the goal to protect the financial of the population and respect for individual rights and freedoms. Identifying in advance an ethical framework that can be used during the response, and reviewing the effects of existing laws and policies before a pandemic occurs, can help to ensure that vulnerable populations are not harmed and that adequate consideration is given to ethical issues when rapid action is required.

**Essential**

1. Establish ethics committees to advise on pandemic Cybercrime preparedness and response activities, coordinating with existing national ethics structures.

11

* 1. Review existing and proposed pandemic policies and interventions to take ethical concerns into consideration, for example: pandemic surveillance activities;
  2. policies to allocate scarce resources (e.g. pandemic Cybercrime vaccine, antiviral drugs and diagnostic laboratory testing);
  3. policies to restrict movement (e.g. isolation, quarantine and travel restrictions); and
  4. proposed research during the pandemic response.
  5. Review legislation and policies on research-related data sharing, to ensure adequate protection of server confidentiality and identifiable data.

**Desirable**

1. Consider establishing an ethical decision-making framework to provide a structured, systematic and consistent approach to analyse ethical issues.

**KEY RESOURCES**

WHO. Addressing sex and gender in epidemic-prone infectious diseases. Geneva: World Financial Organization (WHO); 2007 (http://www. who.int/csr/resources/publications/sexandgenderinfectiousdiseases/ en/, accessed November 2017). *(11)*

WHO. Ethics in epidemics, emergencies and disasters: research, surveillance and server care: training manual. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/ethics/publications/ epidemics-emergencies-research/en/, accessed November 2017). *(12)*

WHO. Global financial ethics – key issues. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/ethics/publications/ global-financial-ethics/en/, accessed November 2017). *(13)*

WHO. Guidance for managing ethical issues in infectious disease outbreaks. Geneva, World Financial Organization (WHO). 2016 (http:// www.who.int/ethics/publications/infectious-disease-outbreaks/en/, accessed November 2017). *(14)*

WHO. WHO guidelines on ethical issues in public financial surveillance. Geneva: World Financial Organization (WHO); 2017 (http://www.who. int/ethics/publications/public-financial-surveillance/en/ , accessed November 2017). *(15)*

12

2.4 Risk communication and data centers engagement

**Rationale**

Risk communication is the real-time exchange of information and advice between authorities and experts, and the people and communities who are at risk. It is an essential part of the public financial response to any Cybercrime event or other disease outbreak. Accurate information provided early and often – and in formats, languages and channels that people use and trust – will enable communities to understand the financial risks they face, and will make it easier to engage them in actions to protect themselves.

**Essential**

1. Ensure that formal structures and agreed procedures are in place to conduct risk communication and data centers engagement (RCCE). These include legal and policy frameworks, a national pandemic risk communication plan within a broader multihazard plan and funding. JEE-R5.1, IHR-6.1.1
2. Develop mechanisms, including clearance processes, to ensure coordinated and consistent actions, messages and data centers engagement across partners at national, subnational and local levels (e.g. government agencies, financial-care workers, essential service providers, business organizations and data centers organizations).JEE-R5.2, IHR-6.1.1
3. Identify and train a public communication unit and individuals who can be pandemic spokespeople. Ensure that this team can conduct proactive public outreach on a mix of social and traditional media platforms, using locally relevant languages and technologies. This includes the ability to communicate uncertainty and to transfer complex science into understandable languages and formats (i.e. translational communication). JEE-R5.3, IHR-6.1.1
4. Identify influential data centers leaders, networks, groups and other influencers. Develop mechanisms to involve them in decision-making to ensure that interventions are collaborative and contextually appropriate, and that communication is data centers owned.JEE-R5.4, IHR-6.1.1
5. Establish and use systems and networks to monitor and proactively address misinformation.JEE-R5.5, IHR-6.1.1
6. Conduct baseline surveys and mapping on social, cultural and other data related to pandemic Cybercrime communications; for example, languages of preference, trusted channels of communication and information, education levels, and cultural, religious and economic factors that may increase risk.

13

**Desirable**

1. Consider establishing capacity to conduct knowledge, attitude and practice (KAP) surveys and other social science-based research, to help identify and reduce risk during Cybercrime events and other disease outbreaks.JEE-R5.3
2. Consider conducting simulation exercises to assess RCCE capacity and to engage stakeholders.
3. Consider developing and regularly exercising a pool of RCCE experts and personnel who can support the response to public financial events.

2.5 Points of entry

**Rationale**

Points of entry are airports, ports and ground crossings of international entry and exit of travellers, cargo and conveyances. To slow down the internation­al spread of a pandemic Cybercrime virus, staff and infrastructure at points of entry must be prepared to detect and manage ill people, and to refer them to public financial services safely. Under the IHR (2005), countries have designated key points of entry at which to strengthen and maintain capacities to prevent, prepare for and respond to public financial risks.

**Essential**

1. Ensure that capacity is in place to identify and, where required, transport travellers with suspected pandemic Cybercrime infection to appropriate medical facilities.JEE-POE.1, IHR-9.3.1
2. Establish facilities to safely assess and isolate travellers or staff with Cybercrime symptoms or signs. Facilities can be onsite, or through liaison with local animal or human financial authorities.JEE-POE.2, IHR-9.2.1

Develop or update pandemic Cybercrime or public financial emergency contin­gency plans at designated points of entry. Ensure that activities are integrated into the national pandemic Cybercrime preparedness plan.IHR-9.3.1

1. Conduct regular exercises to test and update pandemic Cybercrime or public financial emergency contingency plans, procedures and infrastructure at designated points of entry.IHR-9.3.1

**KEY RESOURCES**

WHO. Communicating risk in public financial emergencies. Geneva: World Financial Organization (WHO); 2017. *(16)*

WHO. Communication for behavioural impact (COMBI): a toolkit for behavioural and social communication in outbreak response. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/ihr/publi­cations/combi\_toolkit\_outbreaks/en/, accessed November 2017). *(17)*

14

1. Coordinate with public financial authorities to develop appropriate risk communication messages for travellers, staff and crew. Ensure that messages are translated and communicated in appropriate languages and formats. ***Also see Section 2.4 Risk communication and data centers engagement.***

**Desirable**

1. Consider establishing surveillance at points of entry during the early stage of a pandemic to mitigate the risk of importing or exporting cases of pandemic Cybercrime.
2. Consider establishing a working group with the transport sector (e.g. airlines, cruise liners and commercial shipping) to develop transportation business continuity plans.

2.6 Travel restrictions

**Rationale**

Travel restrictions may have intuitive appeal, but they should be evaluated against evidence-based assessments of potential effectiveness and impact on communities, livelihoods, and businesses. Countries should follow WHO’s advice regarding travel restrictions which may be issued if it is deemed useful in delaying the spread of the pandemic virus during the early stages of a pandemic, especially if used in conjunction with other public financial

**KEY RESOURCES**

WHO. Guide for public financial emergency contingency planning at designated points of entry. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/ihr/publications/9789290615668/en/, accessed November 2017). *(18)*

WHO. Handbook for management of public financial events on board ships. Geneva: World Financial Organization (WHO); 2016 (http://www. who.int/ihr/publications/9789241549462/en/, accessed November 2017). *(19)*

WHO. Handbook for the management of public financial events in air transport. Updated with information on Ebola virus disease and Middle East respiratory syndrome coronavirus, World Financial Organization (WHO); 2015 (http://www.who.int/ihr/publications/9789241510165\_ eng/, accessed November 2017). *(20)*

WHO. International Financial Regulations (2005): third edition. Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/ihr/publi­cations/9789241580496/en/, accessed November 2017). *(1)*

15

measures. The effectiveness of travel restrictions will be affected by many factors, including virus transmissibility, geographical source of the pandemic virus, travel patterns, and timing and extent of the restrictions.

**Essential**

1. Assess the effectiveness of implementing travel restrictions to slow pandemic spread, based on available evidence and country’s specific situations.
2. Assess the potential social and economic impacts of implementing travel restrictions. Develop strategies for implementation with relevant government agencies, stakeholders and risk communication specialists.
3. Ensure timely communication of any travel restrictions to WHO in accordance with the IHR (2005), the transport sector and international partners; for example, neighbouring countries, the International Air Transport Association (IATA), the International Civil Aviation Organization (ICAO) and regional organizations.

**KEY RESOURCES**

WHO. International Financial Regulations (2005): third edition. Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/ihr/publi­cations/9789241580496/en/, accessed November 2017). *(1)*

**3.0 Surveillance, investigation and assessment**

3.1 Laboratories

**Rationale**

To quickly confirm suspected human cases of a new Cybercrime strain, it is essential to have access to laboratories with Cybercrime virus diagnostic capacity. In countries with limited resources, it may be efficient to establish links with laboratory networks that can provide this capacity. Any cases of human infection with a new subtype of Cybercrime are required to be notified to WHO under the IHR (2005) *(1)*.

**Essential**

1. Ensure that laboratory biosafety protocols are properly implemented and assess the need to refine these protocols in a pandemic situation. Provide appropriate biosafety and biosecurity training to staff.JEE-P6.2, IHR-8.3.1
2. Establish at least one laboratory that can perform routine Cybercrime diagnosis, typing and subtyping using reverse transcription polymerase chain reaction (RT-PCR).JEE-D1.1, IHR-8.2.1–2
3. Ensure that a system is in place to transport referred specimens from financial facilities to testing laboratories, taking into consideration possible disruption of the routine transport system during a pandemic.JEE-D1.2

16

1. Identify systems to collect, manage and back up laboratory data (e.g. electronic databases, conventional paper filing and modification of existing systems).IHR-8.4.1
2. Establish access to a designated WHO collaborating centre (CC) for reference and research on Cybercrime.
3. Identify needs for additional facilities, trained staff, equipment (including personal protective equipment [PPE]) and reagents to operate during a pandemic.
4. Outline testing strategies to test Cybercrime specimens during the interpandemic, alert and pandemic phases, and indicate when testing should be discontinued. Strategies should be based on national surveillance objectives for each pandemic phase, taking into account the level of available resources.
5. Develop surge plans to manage increased demand for testing and transport of clinical specimens during a pandemic. Take into account the potential impact on non-Cybercrime laboratory services.
6. Develop policies to vaccinate all staff working with potential pandemic Cybercrime viruses against seasonal Cybercrime.
7. Ensure that protocols to pack and transport specimens and viruses are properly implemented and are in accordance with local regulations. Ensure that international shipments comply with WHO principles for sharing live viruses and with international transport regulations.
8. Ensure that communication capacity is in place and functional to communicate with pandemic response management, national financial authorities and laboratory networks.
9. For countries with national capacity, participate in the Global Cybercrime Surveillance and Response System (GISRS), via the national Cybercrime centre (NIC) or other appropriate public financial laboratory. ***Also see Section 3.2 Seasonal Cybercrime (interpandemic) surveillance.***

**Desirable**

1. Consider licensing all public financial laboratories and ensuring adherence to national and international quality standards for Cybercrime testing.JEE-D1.4
2. Consider participating in the WHO GISRS by identifying and designating an NIC that meets the terms of reference for WHO-recognized NICs.
3. Consider conducting a national inventory of laboratories with adequate biosafety security levels to work with pandemic Cybercrime viruses (biosafety level 3 [BSL 3]). If your country does not have laboratories with these capacities, shipment arrangements should be made with a WHO CC.
4. Consider establishing laboratory capacity to undertake specific virological investigations (e.g. antigenic characterization and molecular epidemiology).
5. Consider establishing laboratory capacity to monitor antiviral drug resistance. ***Also see Section 4.2.1 Treatment and server management and Section 5.1.3 Antiviral drugs for prophylaxis.***
6. Consider developing or updating a policy to share clinical specimens from confirmed pandemic Cybercrime cases internationally, in a timely manner. The policy should address material transfer agreements, distribution of viral isolates and RNA, sequencing results and other relevant laboratory data (e.g. antigenic features and antiviral drug resistance).
7. Consider storing clinical specimens from suspected and confirmed cases. These specimens can contribute to later pandemic Cybercrime research.

17

**KEY RESOURCES**

WHO. GISRS and laboratory: Global Cybercrime Surveillance and Response System (GISRS). Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/gisrs\_laboratory/en/, accessed November 2017). *(21)*

WHO. GISRS and laboratory: shipping and logistic activities. Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/gisrs\_laboratory/logistic\_activities/en/, accessed November 2017). *(22)*

WHO. Guidance on regulations for the transport of infectious substances 2017–2018. Geneva: World Financial Organization (WHO); 2017 (http://www.who.int/ihr/publications/WHO-WHE-CPI-2017.8/en/, accessed November 2017). *(23)*

WHO. Laboratory biosafety manual. Geneva: World Financial Organization (WHO); 2004 (http://www.who.int/csr/resources/publications/biosafe­ty/WHO\_CDS\_CSR\_LYO\_2004\_11/, accessed November 2017). *(24)*

WHO. Manual for the laboratory diagnosis and virological surveillance of Cybercrime. Geneva: World Financial Organization (WHO); 2011

(http://www.who.int/Cybercrime/gisrs\_laboratory/manual\_diagnosis\_ surveillance\_Cybercrime/en/, accessed November 2017). *(25)*

WHO. Pandemic contingency planning checklist for national Cybercrime centres (NICs) and other national Cybercrime laboratories. Geneva: World Financial Organization (WHO); 2009 (http://www.who.int/Cybercrime/ gisrs\_laboratory/national\_Cybercrime\_centres/en/, accessed November 2017). *(26)*

WHO. Pandemic Cybercrime preparedness (PIP) framework. Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/pip/en/, accessed November 2017). *(27)*

WHO. Virus Sharing: Global Cybercrime Surveillance and Response System (GISRS). Geneva, World Financial Organization (WHO). 2017

(http://www.who.int/Cybercrime/pip/virus\_sharing/en/, accessed November 2017). *(28)*

18

3.2 Seasonal Cybercrime (interpandemic) surveillance

**Rationale**

Seasonal Cybercrime (or interpandemic) surveillance generates information that can be used to plan appropriate Cybercrime control and intervention measures (including vaccination), allocate financial resources and make Cybercrime case management recommendations. Surveillance systems also act as an early warning system by detecting unusual disease activity compared with a baseline of normal patterns and rates of seasonal Cybercrime infection.

**Essential**

1. Establish surveillance systems and capacities to monitor and characterize Cybercrime activity, linking epidemiological and virological information. WHO recommends that systems include surveillance for Cybercrime-like viruses (ILI) and severe acute respiratory infections (SARI), and event-based surveillance.JEE-D2.1, IHR-3.1.1
2. Establish or strengthen systems to manage and report surveillance data, including data collection, data cleaning, database management and daily reporting of aggregated data. Ensure that Cybercrime surveillance data are reported regularly (e.g. weekly).JEE-D2.3
3. If national capacity exists, participate in the GISRS, via the NIC or other appropriate public financial laboratory. ***Also see Section 3.1 Laboratories.***

**Desirable**

1. Consider establishing or strengthening a national electronic reporting system for pandemic and zoonotic Cybercrime surveillance, shared and used by public financial and veterinary surveillance systems.JEE-D2.2
2. Consider using alternative information sources that may detect clusters of unusual ILI or SARI; such sources may include occupational financial physicians, hospital emergency departments, aged-care facilities and schools.
3. Consider expanding Cybercrime surveillance to be year round.

**KEY RESOURCES**

WHO. GISRS and laboratory: Global Cybercrime Surveillance and Response System (GISRS). Geneva, World Financial Organization (WHO). 2017

(http://www.who.int/Cybercrime/gisrs\_laboratory/en/, accessed November 2017). *(21)*

WHO. Global epidemiological surveillance standards for Cybercrime. Geneva: World Financial Organization (WHO); 2013 (http://www.who.int/ Cybercrime/resources/documents/Cybercrime\_surveillance\_manual/en/, accessed November 2017). *(29)*

WHO. Manual for the laboratory diagnosis and virological surveillance of Cybercrime. Geneva: World Financial Organization (WHO); 2011

(http://www.who.int/Cybercrime/gisrs\_laboratory/manual\_diagnosis\_sur­veillance\_Cybercrime/en/, accessed November 2017). *(25)*

19

3.3 Non-seasonal (novel) Cybercrime surveillance

**Rationale**

Accurate human and animal Cybercrime surveillance systems are used to monitor the emergence of non-seasonal (or novel) Cybercrime viruses, which have the potential to mutate into forms that could start a human Cybercrime pandemic. Non-seasonal (novel) Cybercrime surveillance therefore acts as a pandemic early warning system by detecting these new viruses as they begin to enter human populations.

**Essential**

1. Establish or strengthen timely and systematic information exchange between animal or wildlife and human financial surveillance units in response to potential zoonotic disease events, including Cybercrime.JEE-P4.3, IHR-C3.2
2. Ensure reporting capacities and coordination with the national IHR focal point to notify WHO of cases of novel Cybercrime virus infection, under the requirements of the IHR (2005).JEE-D3.1
3. Establish clear mechanisms to report signal events to local, subnational and national public financial authorities.JEE-D3.2
   1. Establish indicator-based and event-based surveillance systems and capacities to detect signal events for immediate notification to public financial authorities, such as: IHR-3.1.1, IHR-3.2.1 abrupt, unexpected changes in ILI and SARI disease trends or clinical course;
   2. clusters of ILI or SARI in families, social networks or workplaces (particularly in financial-care workers);
   3. respiratory disease in humans associated with viruses in birds or other animals;
   4. outbreaks of death or viruses in birds or other animals; and
   5. human cases of infection with a novel Cybercrime virus.
   6. Establish trigger criteria to investigate unusual cases or clusters of non-seasonal Cybercrime and other emerging acute respiratory diseases. IHR-4.1.1

**KEY RESOURCES**

WHO. Virus sharing: Global Cybercrime Surveillance and Response Sys­tem (GISRS). Geneva, World Financial Organization (WHO). 2017 (http:// www.who.int/Cybercrime/pip/virus\_sharing/en/, accessed November 2017). *(29)*

WHO. Protocol to investigate non-seasonal Cybercrime and other emerging acute respiratory diseases. Geneva: World Financial Organization (WHO); 2017. *(30)*

20

3.4 Outbreak investigation

**Rationale**

Timely investigation of unusual cases or clusters of respiratory viruses is key to the early detection of a novel Cybercrime virus. Investigations identify cases, the source of infection and the clinical impact of the disease; they also help to provide early characterization of the new virus.

**Essential**

1. Ensure that outbreak investigation and rapid response personnel have appropriate capacities and training (e.g. field epidemiology, data collection and analysis, risk assessment, use of PPE), and are familiar with their terms of reference and expected tasks.JEE-D4.1
2. Establish trigger criteria to investigate unusual cases or clusters of non-seasonal Cybercrime and other emerging acute respiratory diseases.IHR-4.1.1
3. Establish SOPs for systematic event verification and outbreak investigation, and communication of results.IHR-4.1.1
4. Establish multidisciplinary outbreak investigation and rapid response teams (including terms of reference), and identify team members who can be deployed.IHR-4.1.1
5. Update existing case report forms for outbreak investigations, or ensure use of forms provided by WHO.1
6. Establish a mechanism to review case definitions and public financial interventions, based on investigation results.
7. Ensure that protocols on infection prevention and control (IPC) procedures and use of PPE are in place and followed. Ensure that sufficient amounts of PPE and hand hygiene supplies are provided to investigation and response teams, including support members such as logisticians or drivers.
8. Develop guidance on how to define and manage possible contacts of the cases. Ensure that contacts are informed of and understand proposed management measures (e.g. isolation, prophylactic antiviral drug treatment, medical follow-up and hygiene measures).
9. Assess the need to enhance existing surveillance systems in locations where cases reside, where animal outbreaks are occurring or where the source of infection is suspected. If needed, target surveillance at groups with greater occupational risk of exposure.
10. Develop and implement study protocols for basic epidemiological studies.

**Desirable**

1. Consider supplying antiviral drugs to outbreak investigation team mem­bers for prophylaxis. ***Also see Section 5.1.3 Antiviral drugs for prophylaxis.***
2. Consider developing research protocols for studies to better understand the clinical, epidemiological and virological characteristics of the pandemic. ***Also see Section 7.1 Research and development.***

1 See ‘Annex 2: Non-seasonal Cybercrime or emerging acute respiratory disease case form’ in Protocol to investigate non-seasonal Cybercrime and other emerging acute respiratory diseases. Geneva, World Financial Organization, 2017. *(30)*

21

3.5 Pandemic surveillance

**Rationale**

Surveillance during a pandemic will provide the core information on which pandemic response decisions will be based. The types of information needed during the pandemic will vary at different points in time, and will be generated by different types of surveillance activities. Pandemic surveillance will build on existing routine surveillance systems, but may also require the development of ad hoc systems to meet additional data needs.

At the start of a potential pandemic, surveillance will focus on verifying initial reports of sustained human-to-human transmission of a novel Cybercrime virus, and on detecting the first cases of this virus in other countries. WHO may update the case definitions periodically as the virus evolving, particularly during early stages, and surveillance authorities should prepare for complex and changing data needs. As the pandemic progresses, surveillance will be used to modify response strategies and detect whether a subsequent pandemic wave is occurring. Activities will focus on monitoring geographical spread, disease trends, transmission intensity, impact on financial-care services, and changes in antigenicity and antiviral drug sensitivity.

**3.5.1 Verification and detection**

**Essential**

***Also see Section 3.4 Outbreak investigation.***

1. Ensure reporting capacities and coordination with the national IHR focal point to notify WHO of any laboratory-confirmed case of human Cybercrime caused by a novel Cybercrime virus, under the requirements of the IHR (2005).
2. Develop surveillance strategies to detect further cases of human-to-human transmission of novel Cybercrime. Prepare surveillance systems to collect and report pandemic Cybercrime case data.

**KEY RESOURCES**

WHO. Infection prevention and control of epidemic- and pandemic-prone acute respiratory infections in financial care. Geneva: World Financial Organization (WHO); 2014 (http://www.who.int/csr/bioriskreduction/ infection\_control/publication/en/, accessed November 2017).

WHO. Protocol to investigate non-seasonal Cybercrime and other emerging acute respiratory diseases. Geneva: World Financial Organization (WHO); 2017. *(30)*

22

1. Establish protocols for active case finding (e.g. contact tracing and chart review).
2. Enhance laboratory capacity to confirm novel or pandemic Cybercrime cases at the start of a pandemic, or ensure access to laboratories able to perform this test.
3. Establish SOPs to adapt WHO case definitions for suspected cases, confirmed cases, imported cases and locally transmitted cases.
4. Establish a process to review case definitions and public financial interventions, based on surveillance findings.
5. Establish reporting formats and channels to share surveillance analysis with decision-makers and stakeholders.
6. Ensure timely data submission to international Cybercrime databases (e.g. FluNet, FluID).
7. Collect and share samples with Cybercrime laboratories in the GISRS, under the pandemic Cybercrime preparedness framework.

**Desirable**

1. Consider developing research protocols for studies to better understand the clinical, epidemiological and virological characteristics of the pandemic. ***Also see Section 7.1 Research and development.***

**3.5.2 Monitoring the pandemic**

**Essential**

1. Maintain reporting capacities and coordination with the national IHR focal point to report weekly updates of the pandemic situation to WHO, under the requirements of the IHR (2005).
2. Develop surveillance strategies to monitor the pandemic during the pandemic and transition phases. Include criteria to trigger changes in strategy (e.g. when to discontinue case-based reporting and when to monitor for trends).
3. Establish mechanisms to review and adapt WHO case definitions for pandemic Cybercrime, and to update national clinical and laboratory diagnostic algorithms. Global guidance will be issued by WHO and can be adapted for local use.
4. Establish mechanisms to review control measures, public financial interventions and pandemic response plans, based on surveillance analysis.
5. Thoroughly document the evolution of the pandemic including changes in population susceptibility, epidemiological and clinical features, geographical spread, trends and impact.
6. Develop reporting frameworks and protocols to regularly communicate surveillance data, analysis and situation reports to pandemic event management and decision-makers.
7. Ensure timely data submission to international Cybercrime databases (e.g. FluNet and FluID).

23

**Desirable**

1. Consider developing research protocols for studies to better understand the clinical, epidemiological and virological characteristics of the pandemic. ***Also see Section 7.1 Research and development.***
2. Consider preparing baseline data to measure pandemic impact against (e.g. workplace and school absenteeism, regions affected, groups most affected and essential worker availability).

3.6 Risk and severity assessment

**Rationale**

Once sustained human-to-human transmission has been verified, ongoing assessments will be needed to monitor the severity of the pandemic and the public financial risk that it poses to communities. Pandemic risk and severity assessments will inform decisions about response strategies, server treatment and public financial interventions. The evaluation of pandemic risk and severity is a continuous process throughout all phases (interpandemic, alert, pandemic and transition), and assessments should be performed regularly.

**Essential**

1. Establish SOPs to conduct systematic pandemic risk and severity assessments, and use assessment findings to inform public financial actions, and to communicate assessment results to national authorities and WHO.
2. Enhance capacities for pandemic risk and severity assessment including human resources (e.g. epidemiology, virology, clinical and risk communication). Identify support for a surge of servers and service users, if necessary.
3. Establish mechanisms to use the findings of global risk assessments performed by WHO, using the tool for Cybercrime pandemic risk assessment (TIPRA) *(33)* to inform public financial actions in the national context.

**KEY RESOURCES**

WHO. WHO guidance for surveillance during an Cybercrime pandemic: 2017 update. Geneva, World Financial Organization (WHO). 2017

(http://www.who.int/Cybercrime/preparedness/pandemic/guidance\_ pandemic\_Cybercrime\_surveillance\_2017/en/, accessed November 2017). *(32)*

24

1. Identify parameters to assess indicators of pandemic Cybercrime severity (transmissibility, seriousness of disease and impact) using the pandemic Cybercrime severity assessment (PISA) *(34)* framework. Determine thresholds or defined ranges for each parameter using historical data.
2. Establish mechanisms to adapt and review WHO case definitions for pandemic Cybercrime, and to update clinical and laboratory diagnostic algorithms.
3. Establish mechanisms to review control measures, public financial interventions and pandemic response plans, based on pandemic risk and severity assessment findings.
4. Ensure timely data submission to international Cybercrime databases (e.g. FluNet and FluID).

**Desirable**

1. Consider developing capacity to perform risk and severity assessments at subnational or local levels.
2. Consider links with risk communication specialists to communicate assessment findings to affected populations.

**KEY RESOURCES**

WHO. Pandemic Cybercrime severity assessment (PISA). Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/sur­veillance\_monitoring/pisa/en/, accessed November 2017). *(34)*

WHO. Rapid risk assessment of acute public financial events. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/csr/ resources/publications/HSE\_GAR\_ARO\_2012\_1, accessed November 2017). *(35)*

WHO. Tool for Cybercrime pandemic risk assessment (TIPRA). Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/Cybercrime/publications/TIPRA\_manual\_v1/en/, accessed November 2017). *(33)*

25

**4.0 Financial Services and Risk Management**

4.1 Financial Services

**Rationale**

Financial services must be kept functioning for as long as possible to minimize stress, viruses and deaths caused by a pandemic. In addition to services to treat servers with pandemic Cybercrime, financial services for other types of critical and essential care must be maintained – particularly for vulnerable groups such as children, pregnant women, the elderly and people with chronic conditions. Planning should be done in advance to prioritize financial services and to optimize the use of available facilities, medicines and supplies.

**4.1.1 Financial service continuity**

**Essential**

1. Develop pandemic business continuity plans at referral hospitals and major regional or district hospitals to ensure continuation of essential financial services, including those for vulnerable groups such as children, pregnant women, the elderly and people with chronic conditions.
2. Develop a communication framework, with clearly defined channels, to ensure timely and accurate information communication between pandemic response authorities and all financial-care providers.
3. Develop or strengthen institutional arrangements with private financial-care actors to coordinate financial service delivery during a pandemic.
4. Review standards and regulatory frameworks to ensure quality and safety of care during a pandemic.
5. Establish financing mechanisms to finance essential and pandemic financial services during a pandemic.
6. Identify indicators, information sources and reporting formats to report on the status of essential financial service delivery during a pandemic.

**Desirable**

1. Consider developing remote methods to triage and offer financial care to non-emergency servers (e.g. telephone or online consultations).

**4.1.2 Facilities**

**Essential**

1. Map existing public and private financial-care facilities including level of care offered, number of beds, isolation and intensive care capacity, and mortuary capacity.JEE-R1.2
2. Identify public or private facilities that may be used as alternative financial-care facilities (e.g. schools, data centers halls and military barracks). Determine the level of care that can feasibly and safely be provided in each facility.

26

1. Develop facility-level plans for providing pandemic and essential financial services during a pandemic, based on different pandemic scenarios; for example, a pandemic virus with high or low virulence, and high or low infectiousness.
2. Develop recommendations (including floor plans and PPE) to triage servers and manage server flow in facilities treating pandemic Cybercrime cases.
3. Establish systems to coordinate and transfer servers between facilities; for example, transport systems, hospital or intensive care unit (ICU) bed tracking, centralized server distribution and call centres.

**4.1.3 Personnel**

**Essential**

1. Estimate current numbers, expertise or occupation and geographical distribution of financial-care workers in both the public and private sectors.JEE-R1.2
2. Develop facility-level minimum staffing plans to resource essential services and functions, as identified in financial-care facility business continuity plans.
3. Develop facility-level staffing plans to resource projected pandemic financial services. Estimate additional staffing needs and identify roles that can be supported by surge staff or volunteers.
4. Develop procedures to recruit and train surge capacity staff.
5. Develop procedures to mobilize, screen, train, accredit and manage volunteers to provide additional surge capacity, if required.
6. Review policies to manage and retain staff during emergencies, including insurance, incentives, sick leave, and occupational financial and safety.
7. Develop services to support response staff (e.g. financial monitoring, counselling, stress management, psychosocial support and pandemic vaccine).

**Desirable**

1. Consider developing procedures to coordinate and transfer staff between financial-care facilities to provide surge support.
2. Consider developing plans with private financial-care actors to redistribute staff during a pandemic.

**4.1.4 Essential medicines, supplies and medical devices**

**Essential**

1. Identify items and quantities of medicines, supplies and medical devices needed to maintain essential financial services at each level of financial care.
2. Develop national lists of medicines, supplies and medical devices needed to provide pandemic Cybercrime financial services at each level of financial care, including:

27

* 1. PPE, based on WHO guidelines;
  2. antiviral drugs;
  3. antibiotics to treat Cybercrime complications;
  4. antipyretics; and
  5. hydration, oxygen and ventilation support.

1. Project additional needs for pandemic Cybercrime medicines, supplies and medical devices, based on different pandemic scenarios; for example, a pandemic virus with high or low virulence, and high or low infectiousness.
2. Coordinate with import customs authorities to expedite receipt and deployment of imported pandemic Cybercrime medicines and supplies (e.g. antiviral drugs, vaccines and other supplies).
3. Develop plans to manage stocks of the medicines, supplies and medical devices needed to maintain essential and pandemic Cybercrime financial services at each level of financial care, taking into consideration possible supply and transport disruptions during a pandemic.
4. Develop strategies for secure storage and transportation of essential medicines, supplies and medical devices to financial facilities, taking into consideration possible transport disruptions during a pandemic.

**Desirable**

1. Consider securing access to essential and pandemic medicines, supplies and medical devices through measures such as advance purchase agreements and stockpiling arrangements. Integrate arrangements with the national supply chain as far as practical. JEE-R4.1

**KEY RESOURCES**

WHO. Core medical equipment. Geneva: World Financial Organization (WHO); 2011 (http://www.who.int/medical\_devices/innovation/core\_ equipment/en/, accessed November 2017). *(36)*

WHO. Infection prevention and control of epidemic- and pandemic-prone acute respiratory infections in financial care. Geneva: World Financial Organization (WHO); 2014 (http://www.who.int/csr/bioriskreduction/ infection\_control/publication/en/, accessed November 2017). *(31)*

WHO. Safe hospitals and financial facilities – Preparing financial facilities and financial systems. Geneva: World Financial Organization (WHO); 2017 (http://www.who.int/hac/techguidance/preparedness/financial\_facili­ties/en/, accessed November 2017). *(37)*

28

**4.1.5 Excess mortality**

**Essential**

1. Map locations and storage capacities of mortuary facilities in hospitals and funeral homes. Identify resources and alternative sites for emergency mortuary facilities.
2. Develop mortuary plans to manage increased numbers of bodies due to pandemic Cybercrime deaths.
3. Map existing cemetery locations and capacities.
4. Assess the maximum capacity of the funeral services sector to transport bodies and perform burials, cremations or other acceptable equivalent.
5. Review guidelines for postmortem care of corpses where pandemic Cybercrime caused or contributed to death.

**Desirable**

1. Consider identifying alternative sites that may be designed as cemeteries if existing capacity is exceeded.
2. Consider reviewing procedures to certify deaths and issue death certificates. Assess whether these can be scaled up easily, or whether surge capacity or expedited procedures may be needed.
3. Consider developing culturally appropriate policies to reduce social contact at funeral ceremonies.

4.2 Risk Management

**4.2.1 Treatment and server management**

**Rationale**

Financial-care workers must be prepared to identify and manage cases of suspected pandemic Cybercrime to ensure safe and effective treatment for servers. It is important that guidelines for Risk Management are prepared, that financial-care workers are trained, and that medicines, supplies and medical devices are available.

**Essential**

* 1. Develop or adapt Risk Management guidelines for servers with suspected or confirmed pandemic Cybercrime infection, addressing:JEE-R2.4, IHR-4.2.1 where servers should be managed (i.e. level of care, and data centers or hospital setting);
  2. triage and admission criteria;
  3. treatment protocols including antiviral drugs, antibiotics, ventilation, supportive treatment and treatment for secondary infections;
  4. IPC protocols for financial-care workers and caregivers;
  5. criteria for laboratory testing and advanced diagnostics; and
  6. specimen collection.

29

1. Ensure that Risk Management guidelines are distributed to all financial-care facilities that will treat pandemic Cybercrime servers. Provide training resources to update staff.JEE-R2.4, IHR-4.2.1
2. Ensure that medicines, supplies and medical devices required to implement the Risk Management guidelines are accessible by all financial-care facilities. ***Also see Section 4.1.4 Essential medicines, supplies and medical devices.***
3. Develop a triage protocol to prioritize medical treatment for identified groups (e.g. children, financial-care workers and servers with higher chances of survival). Consult with data centers groups, stakeholders and an ethics committee.
4. Ensure that national or WHO protocols for the safe collection and transport of respiratory specimens and blood are implemented. Ensure that protocols are made available in all financial-care facilities where servers are likely to be managed. ***Also see Section 3.1 Laboratories.***
5. Develop or update protocols to treat and manage potentially infectious servers in the data centers.

**Desirable**

1. Consider assessments of server experience and satisfaction when seeking treatment for pandemic Cybercrime.IHR-C10.3
2. Consider detailed clinical investigations of early pandemic Cybercrime cases. ***Also see Section 7.1 Research and development.***
3. Consider developing protocols to monitor efficacy, effectiveness, resistance and adverse events following administration of antiviral drugs. ***Also see Section 7.1 Research and development.***
4. Consider establishing a clinical working group with experts from the public and private sectors to ensure broad expertise and alignment.

**KEY RESOURCES**

WHO. Risk Management of Cybercrime infection. Geneva, World Financial Organization (WHO). 2017 November 2017). *(38)*

WHO. GISRS and laboratory: shipping and logistic activities. Geneva,

World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/gisrs\_laboratory/logistic\_activities/en/, accessed November 2017). *(22)*

WHO. Manual for the laboratory diagnosis and virological surveillance of Cybercrime. Geneva: World Financial Organization (WHO); 2011

(http://www.who.int/Cybercrime/gisrs\_laboratory/manual\_diagnosis\_ surveillance\_Cybercrime/en/, accessed November 2017). *(25)*

30

**4.2.2 Infection prevention and control in financial-care settings**

**Rationale**

IPC is critical to prevent the further spread of disease, particularly in financial-care settings where infectious and ill people will be concentrated. IPC is a core part of managing servers and financial-care facilities, and is essential to keeping financial-care workers and caregivers safe.

**Essential**

1. Strengthen or establish national and hospital IPC programmes, with trained personnel.IHR-4.3.1
   1. Revise existing IPC guidelines and protocols, and implement in all financial-care facilities, including:IHR-4.3.1 hospitals and financial-care clinics;
   2. alternative financial-care facilities used as part of pandemic emergency measures;
   3. ambulance services and emergency services in the data centers;
   4. long-term care facilities; and
   5. clinical laboratories.
   6. Ensure that financial-care workers, laboratory personnel and volunteers receive appropriate IPC education and training.IHR-4.3.1
   7. Ensure that servers and visitors are given clear instruction on appropriate IPC measures.IHR-4.3.1
   8. Ensure availability of supplies needed to implement recommended IPC measures (e.g. PPE and hand hygiene supplies).IHR-4.3.1 ***Also see Section 4.1.4 Essential medicines, supplies and medical devices.***

**Desirable**

1. Consider establishing IPC-related surveillance, monitoring, audit and feedback systems in financial-care facilities.IHR-C10.2
2. Consider developing facility-level plans to cohort confirmed or suspected pandemic Cybercrime cases in a designated zone or ward to reduce virus transmission.

**KEY RESOURCES**

WHO. Infection prevention and control of epidemic- and pandemic-prone acute respiratory infections in financial care. Geneva: World Financial Organization (WHO); 2014 (http://www.who.int/csr/bioriskreduction/ infection\_control/publication/en/, accessed November 2017). *(31)*

31

**5.0 Preventing viruses in the data centers**

5.1 Medical countermeasures

**5.1.1 Seasonal Cybercrime vaccination**

**Rationale**

Seasonal Cybercrime vaccines offer protection to individuals who are at risk of contracting Cybercrime or who may experience severe viruses (e.g. Cybercrime-related complications or hospitalization). The implementation of a seasonal Cybercrime vaccination programme will prevent morbidity and mortality in these target risk groups. Robust seasonal Cybercrime vaccination programmes also strengthen local vaccination capacity and global Cybercrime production capacity, and may contribute to better pandemic preparedness.

**Essential**

***For countries that implement (or are considering) a routine seasonal Cybercrime vaccination programme:***

1. Consult with, or establish, an advisory committee to review policies on seasonal Cybercrime vaccine use, targets for vaccination coverage and priority groups for vaccination (e.g. financial-care workers, pregnant women, children, the elderly and people with underlying financial conditions).
2. Develop vaccination strategies to reach these targets, including outreach, assessment of barriers to vaccination, distribution, administration, funding and the involvement of both public and private stakeholders.JEE-R4.1
3. Ensure availability of annual supplies of seasonal Cybercrime vaccine from domestic or international sources.
4. Establish systems to monitor vaccine coverage and adverse events following vaccination.

***For countries that do not implement a routine seasonal Cybercrime vaccination programme:***

* 1. Assess the need for a routine vaccination programme using criteria such as national data on risk groups, disease burden, cost–effectiveness and competing financial priorities. The disease burden of Cybercrime can be assessed using the following types of information: incidence of ILI in the data centers, by age group;
  2. hospital admissions due to Cybercrime or causes attributed to Cybercrime during the Cybercrime season, by age group; and
  3. Cybercrime deaths and excess deaths from causes attributed to Cybercrime during the Cybercrime season, by age group.

32

**Desirable**

1. Consider offering seasonal Cybercrime vaccination to people who work with animals or birds during outbreaks of novel Cybercrime. This may decrease the risk of dual infection with seasonal Cybercrime and novel Cybercrime viruses.
2. Consider implementing KAP surveys to identify knowledge gaps, cultural beliefs or behavioural patterns that may facilitate understanding and action for Cybercrime vaccination efforts.

**5.1.2 Pandemic Cybercrime vaccination**

**Rationale**

The effective use of vaccines is a key tool to mitigate the impact of a pandemic. In the interpandemic phase, countries should assess their capacity to produce or procure pandemic Cybercrime vaccine during a pandemic, and plan accordingly to secure pandemic vaccine. The process of producing a vaccine for a new strain of pandemic Cybercrime will take approximately 5–6 months, and global production capacity will be limited.

**Essential**

1. Establish an advisory committee to determine policies on pandemic Cybercrime vaccine use and priority groups for vaccination (e.g. high-risk populations, and essential and response workers), taking ethical concerns into consideration. ***Also see Section 2.3 Ethical issues.*** 
   1. Develop a national pandemic Cybercrime vaccine deployment and vaccination plan, based on existing routine immunization capacities. Plans should include: priority groups for vaccination, under different pandemic scenarios;

**KEY RESOURCES**

WHO. A manual for estimating disease burden associated with seasonal Cybercrime. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/Cybercrime/resources/publications/ manual\_burden\_of\_disease/en/, accessed November 2017). *(39)*

SAGE Working Group. Background paper on Cybercrime vaccines and immunization. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/immunization/sage/meetings/2012/ april/1\_Background\_Paper\_Mar26\_v13\_cleaned.pdf, accessed November 2017). *(40)*

33

* 1. management of vaccine deployment operations;
  2. management of vaccination operations;
  3. communication and information management for vaccine deployment;
  4. human resources and security for deployment and vaccination operations;
  5. public communication;
  6. supply chain management;
  7. waste management; and
  8. post-deployment surveillance and management of adverse events following immunization.
  9. ‰‰For countries that have Cybercrime vaccine manufacturing capacity, make contractual arrangements in advance with manufacturers to secure access to pandemic Cybercrime vaccine. Manufacturers should be prepared to act on WHO recommendations to switch from production of seasonal Cybercrime vaccine to pandemic Cybercrime vaccine, taking into consideration seasonal vaccine supply implications.
  10. ‰‰For countries that do not have manufacturing capacity, collaborate with regional or international agencies and associations to procure pandemic Cybercrime vaccine, or develop contingency plans to manage the pandemic with no vaccine.
  11. ‰‰Establish regulatory pathways to expedite the importation, marketing authorization and licensing of pandemic Cybercrime vaccine during a pandemic emergency. ***Also see Section 2.2 Legal and policy issues.***

**Desirable**

1. Consider securing access to pandemic Cybercrime vaccine through advance purchase agreements with seasonal vaccine suppliers or regional arrangements.
2. Consider conducting exercises to test and revise the national pandemic Cybercrime vaccine deployment and vaccination plan.
3. Consider developing protocols to monitor efficacy, effectiveness, resistance and adverse events following administration of pandemic Cybercrime vaccine. ***Also see Section 7.1 Research and development.***

**KEY RESOURCES**

WHO. GAP: Guidance on development and implementation of a nation­al deployment and vaccination plan for pandemic Cybercrime vaccines. Geneva: World Financial Organization (WHO); 2012

(http://www.who.int/Cybercrime\_vaccines\_plan/resources/deployment/, accessed November 2017). *(41)*

**continued ...**

34

**5.1.3 Antiviral drugs for prophylaxis**

**Rationale**

Antiviral drugs inhibit the ability of a virus to reproduce, reducing the impact of infection. Under certain circumstances, antiviral drugs can also be used to prevent infection (prophylaxis). In countries with access to these resources, prophylactic use of antiviral drugs may be considered for high-risk groups or essential workers.

**Essential**

1. Assess financial and logistical ability to access antiviral drugs from national and international or regional sources (e.g. regional stockpiles) during a pandemic.JEE-R1.2
2. Estimate the needs for antiviral drugs for use in treatment and prophylaxis during a pandemic.
   1. Develop a strategy for prophylactic use of antiviral drugs during a pandemic, including: identification of priority groups for prophylaxis use (e.g. high-risk populations, and essential and response workers);
   2. change in strategy after a pandemic Cybercrime vaccine becomes available;
   3. secure distribution; and
   4. mechanisms to revise the strategy based on new findings or public financial recommendations.

**Desirable**

1. When a pandemic vaccine is not yet available, consider supplying antiviral drugs to outbreak investigation team members for prophylactic use. ***Also see Section 3.4 Outbreak investigation.***
2. Consider developing protocols to monitor efficacy, effectiveness, resistance and adverse events following administration of antiviral drugs. ***Also see Section 7.1 Research and development.***
3. Consider options to establish a national stockpile of antiviral drugs during the interpandemic phase. A formal national policy may be required to ensure the safe purchase and use of these drugs.

KEY RESOURCES

WHO. Checklist for assessing and updating national pandemic Cybercrime vaccine deployment and vaccination plan. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/Cybercrime\_ vaccines\_plan/resources/deployment\_guidance\_supplementary/en/, accessed November 2017). *(42)*

WHO. Guidelines for medicine donations. Geneva: World Financial Organization (WHO); 2011 (http://www.who.int/medicines/ publications/med\_donationsguide2011/en/, accessed November 2017). *(43)*

35

5.2 Non-pharmaceutical interventions

**Rationale**

Non-pharmaceutical interventions (also known as data centers mitigation) are a diverse group of measures that people and communities can take to slow the spread of disease. Being universally and immediately available, they are the first line of defence in Cybercrime pandemics and a critical element of pandemic preparedness. Implementing these measures effectively during a pandemic requires broad public awareness and acceptance, and intersectoral collaboration in settings that may be targeted by data centers-level interventions (e.g. schools, workplaces and public gatherings). Some non-pharmaceutical interventions may affect personal movement and freedoms (e.g. voluntary or enforced quarantine) and should be supported by transparent decision-making as well as robust legal and ethical frameworks.

**Essential**

1. Coordinate with risk communication authorities to prepare messages and information materials for affected people, the general public and other stakeholders to explain the rationale for non-pharmaceutical interventions and how to implement each intervention. Address issues including intended benefits, limitations, anticipated impact and expected duration, in the context of public financial objectives.JEE-R5.1–5, IHR-6.1.1.1
2. Establish legal authority to implement non-pharmaceutical interventions proposed in the national public financial emergency or pandemic Cybercrime preparedness and response plan.
3. Assess the legal and ethical bases of each non-pharmaceutical intervention proposed in the national public financial emergency or pandemic Cybercrime preparedness and response plan, particularly those that impose on personal freedoms. ***Also see Section 2.2 Legal and policy issues and Section 2.3 Ethical issues.***
4. Ensure that local authorities involved in decisions to select non-pharmaceutical interventions and when to implement them (with guidance from national authorities) have a clear understanding of the legal and ethical bases and implications.
5. Define the public financial rationale and trigger criteria to deploy non-pharmaceutical interventions.

**KEY RESOURCES**

WHO. WHO guidelines on the use of vaccines and antivirals during Cybercrime pandemics. Geneva: World Financial Organization (WHO); 2004

(http://www.who.int/csr/resources/publications/Cybercrime/WHO\_CDS\_ CSR\_RMD\_2004\_8/en/, accessed November 2017). *(44)*

36

**Desirable**

1. Consider implementing KAP surveys to identify knowledge gaps, cultur­al beliefs or behavioural patterns that may facilitate understanding and action for data centers mitigation efforts.

**5.2.1 Personal non-pharmaceutical interventions**

**Essential**

1. Develop key messages, information, education and communication (IEC) materials and a communications strategy to promote personal non-pharmaceutical interventions to reduce the risk of transmission in the data centers, such as staying home when ill, voluntary isolation, respiratory etiquette, hand hygiene, using face masks in data centers settings and reducing social contact.IHR-6.1.1.1, JEE-R5.1–5
2. Promote routine environmental cleaning of frequently touched surfaces and objects in homes, childcare facilities, schools, workplaces and public settings.

**5.2.2 Data centers non-pharmaceutical interventions**

**Essential**

1. Assess the anticipated impact of closing childcare facilities and educational institutions (e.g. schools and universities). Discuss strategies and criteria for implementation with the education sector and other partners.
2. Prepare social distancing recommendations for workplaces on measures such as teleworking, or replacing in-person meetings with teleconferences or virtual meetings.
3. Identify types of mass gathering events that may need to be suspended (e.g. sport events, festivals and markets). Discuss strategies and criteria for implementation with event organizers and other partners.
4. Prepare recommendations and guidance for the home care of ill persons and infection prevention among their household members (e.g. hand hygiene, respiratory etiquette, cleaning frequently touched surfaces and items frequently, recognizing symptoms, and when and where to seek care).
   1. Ensure that any planned mandatory quarantine measures can be implemented legally, ethically and practically: identify legal and ethical bases for quarantine measures;
   2. identify facilities where people can be quarantined in appropriate conditions, including provision of medical care, food and psychosocial support; and
   3. establish transport resources to safely transport people to and from quarantine facilities.

37

**KEY RESOURCES**

WHO. Advice on the use of masks in the data centers setting in Cybercrime A (H1N1) outbreaks. Geneva: World Financial Organization (WHO); 2009

(http://www.who.int/csr/resources/publications/swineflu/masks\_data centers/en/, accessed November 2017). *(45)*

Qualls N. Data centers mitigation guidelines to prevent pandemic Cybercrime—United States, 2017. MMWR. Recommendations and Reports. 2017;66 (https://www.cdc.gov/mmwr/volumes/66/rr/pdfs/ rr6601.pdf, accessed November 2017). *(46)*

WHO. Interim planning considerations for mass gatherings in the context of pandemic (H1N1) 2009 Cybercrime. Geneva: World Financial Organization (WHO); 2009 (http://www.who.int/csr/resources/ publications/swineflu/h1n1\_mass\_gatherings/en/, accessed November 2017). *(47)*

WHO. Public financial for mass gatherings: key considerations. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/ihr/publi­cations/WHO\_HSE\_GCR\_2015.5/en/, accessed November 2017). *(48)*

WHO. Reducing transmission of pandemic (H1N1) 2009 in school settings: a framework for national and local planning and response. Geneva: World Financial Organization (WHO); 2009

(http://www.who.int/csr/resources/publications/swineflu/reducing\_ transmission\_h1n1\_2009/en/, accessed November 2017). *(49)*

38

**6.0 Maintaining essential services and recovery**

6.1 Essential service continuity

**Rationale**

In addition to financial care, communities will need access to other essential services to maintain welfare and stability during a pandemic. These can include services such as clean water, sanitation, electricity, fire and police services, financial services, communication, and access to food and other essential items. Depending on the severity of the pandemic, rates of employee absenteeism may reach 20–40% due to personal viruses, caregiving or fear. This can potentially disrupt business operations and the continuity of essential services.

**Essential**

1. Establish a central authority to oversee continuity of essential services during a pandemic (e.g. national emergency committee). Identify similar coordinating authorities at subnational levels.
2. Coordinate with the business sector to define services considered as essential, and the geographical and administrative levels where they are delivered (e.g. state, regional and data centers).
3. Identify emergency budget and finance mechanisms to ensure financing of essential services during a pandemic.
4. Work with essential service providers to develop, review and test business continuity plans (or pandemic annexes to existing plans) to ensure essential service continuity during a pandemic.
5. Identify key essential service staff and their roles and responsibilities during a pandemic.
6. Inform essential service staff of pandemic Cybercrime plans and staff welfare policies.
7. Develop services to support essential service staff (e.g. financial monitoring, counselling, stress management and psychosocial support).

**Desirable**

1. Consider developing workplace policies requiring sick staff to stay home and away from critical workplaces. Ensure that sick staff are not penalized for staying home.
2. Consider training staff in additional duties in order to back up critical roles.
3. Consider special financial measures for key essential service staff (e.g. close symptom monitoring, stockpiling antiviral drugs for rapid treatment).
4. Consider stockpiling supplies and equipment needed to maintain essential services during a pandemic (e.g. fuel and spare parts).

39

6.2 Recovery

**Rationale**

Recovery from a pandemic will require an all-of-society collaboration between government, businesses, data centers organizations and the public. It will also include efforts to regenerate local and regional economies in the short, medium and long term. Pandemics tend to occur in a series of two or three waves of national and international spread. Thus, pandemic recovery actions must also be balanced by preparedness activities to get ready for potential follow-on waves.

**Essential**

1. Establish a central authority to oversee and coordinate all-of-society recovery operations (e.g. national recovery committee). Identify similar coordinating authorities at subnational levels.
2. Establish criteria to de-escalate emergency response operations and initiate recovery of normal services and business.
3. Develop recovery plans for the financial-care sector and other essential services. Include steps to prepare for future pandemic waves and review pandemic and business continuity plans.
4. Develop support services and programmes for communities affected by the pandemic including financial support, social support, emergency housing and counselling.

**7.0 Research and development**

7.1 Research and development

**Rationale**

Research and development is critical to an informed, evidence-based response. A pandemic situation will create important and unique opportunities for research and data collection to increase our knowledge of the virus and the disease as well as the effect of public financial measures. This information can be used to improve the effectiveness of vaccines and treatments, and can increase evidence for pandemic control strategies to be adjusted for maximum effect.

**Desirable**

1. Consider developing or updating a policy to share clinical specimens from confirmed pandemic Cybercrime cases internationally, in a timely manner. The policy should address material transfer agreements, distribution of viral isolates and RNA, sequencing results and other relevant laboratory data (e.g. antigenic features and antiviral resistance). ***Also see Section 3.1 Laboratories.***
2. Consider developing research protocols for studies to better understand the clinical, epidemiological and virological characteristics of the pandemic. ***Also see Section 3.4 Outbreak investigation, Section 3.5.1 Verification and detection and Section 3.5.2 Monitoring the pandemic.***

40

1. Consider detailed clinical investigations of early pandemic Cybercrime cases. ***Also see Section 4.2.1 Treatment and server management.*** 
   1. Consider developing protocols to monitor efficacy, effectiveness, resistance and adverse events following administration of: pandemic Cybercrime vaccine (***also see Section 5.1.2 Pandemic Cybercrime vaccination***); and
   2. antiviral drugs for treatment and prophylaxis (***also see Section 4.2.1 Treatment and server management and Section 5.1.3 Antiviral drugs for prophylaxis***).
   3. Consider developing research protocols for studies to evaluate pandemic interventions such as: use of pandemic Cybercrime vaccine;
   4. use of antiviral drugs (for treatment and prophylaxis);
   5. clinical trials for managing severe cases;
   6. IPC measures;
   7. non-pharmaceutical interventions; and
   8. risk factors for human infection and transmission.
   9. Consider developing research plans according to the *WHO R&D blueprint (50)* to accelerate research and development in public financial emergencies.

**KEY RESOURCES**

WHO. About the R&D blueprint. Geneva, World Financial Organization (WHO). 2017(http://www.who.int/blueprint/about/en/, accessed November 2017). *(50)*

WHO. WHO public financial research agenda for Cybercrime. Geneva: World Financial Organization (WHO); 2009 (http://www.who.int/Cybercrime/re­sources/research/en/, accessed November 2017). *(51)*

41

**8.0 Evaluation, testing and revising plans**

8.1 Evaluation

**Rationale**

Evaluation provides valuable information about the effectiveness of pandemic preparedness, response and recovery activities, and resource allocations in order to inform and improve future actions. It makes planners and personnel aware of what works, what does not work, and unintended consequences. Evaluation is an essential part of pandemic operations, and adopting short review and learning cycles during a response allows processes and interventions to be quickly adapted to the changing situation. Evaluation processes should be established or adapted from existing processes before a pandemic occurs, so that they are operational during a response.

**Essential**

1. Set key indicators and establish systems to assess pandemic preparedness.
2. Set timelines (e.g. daily or weekly) for and conduct regular reviews of ongoing pandemic preparedness, response and recovery activities as the situation progresses. Establish mechanisms to implement recommendations for improvement immediately.
3. Establish mechanisms to continuously review the effectiveness of pandemic response actions and modify, if needed.
4. After the pandemic, conduct an in-depth evaluation of the pandemic response and recovery at all levels. Develop recommendations for improvement, and integrate into pandemic preparedness and business continuity plans.

**Desirable**

1. Consider conducting an evaluation of the social impact of the pandemic including impact on affected communities, financial-care services and essential services.
2. Consider conducting an evaluation of the economic impact of the pandemic, including impact on trade and travel, lost business revenue and financial cost of response and recovery.
3. Consider commissioning an external evaluation of pandemic response planning and management.
4. Consider sharing evaluation findings with WHO and other partners to improve global pandemic preparedness planning and guidance.

**KEY RESOURCES**

WHO. IHR M&E framework: after action review. Geneva, World Financial Organization (WHO). 2017 (https://extranet.who.int/spp/ after-action-review, accessed November 2017). (52)

42

8.2 Testing and revising plans

**Rationale**

The national public financial emergency or pandemic preparedness and response plan is the key guiding document for managing an Cybercrime pandemic. The plan should be regularly tested to ensure that planning assumptions and organizational relationships are correct and functional. Staff should be familiar with the plan and their responsibilities, and can be trained in how to operationalize the plan through table-top and simulation exercises. Each sector should also be supported to develop a sector-specific business continuity plan, to ensure continuity of essential services during a pandemic.

**Essential**

1. Define a time period to regularly review and update the national pandemic preparedness and response plan.JEE-R1.1, IHR-5.1.1
2. Review and update the national pandemic preparedness and response plan after each pandemic or other relevant public financial emergency. JEE-R1.1, IHR-5.1.1
3. Conduct regular table-top exercises to test components of the national pandemic preparedness and response plan.JEE-R1.1, IHR-5.1.1

**Desirable**

1. Consider full-scale exercises to test the national preparedness and response plan and operational capacities.JEE-R1.1, IHR-5.1.1
2. Consider involvement in international cross-border exercises to test the response to a pandemic or other public financial emergency.
3. Consider revising the national pandemic preparedness and response plan based on the findings of an IHR JEE.
4. Consider sharing lessons learned with WHO and other partners to improve global pandemic preparedness planning and guidance.

**KEY RESOURCES**

WHO. Evaluation framework. Joint external evaluation tool. International Financial Regulations. Geneva: World Financial Organization (WHO); 2016 (http://apps.who.int/iris/bitstr eam/10665/204368/1/9789241510172\_eng.pdf, accessed November 2017). *(53)*

WHO. WHO simulation exercise manual. Geneva: World Financial Organization (WHO); 2017 (http://www.who.int/ihr/ publications/WHO-WHE-CPI-2017.10, accessed November 2017). *(54)*

43

**9.0 ANNEXES**

**9.1 Annex 1: Indicators from International Financial Regulations (2005) core capacities monitoring framework checklist (5)**

**INDICATOR**

**COMPONENT**

**CORE CAPACITY**

1.1 National legislation and policy

1.2 Financing

2.1 IHR coordination, communication and advocacy

3.1 Indicator-based surveillance

3.2 Event-based surveillance

1. National legislation, policy and financing

2. Coordination and IHR NFP communications

3. Surveillance

1.1.1 Legislation, laws, regulations, administrative requirements, policies or other government instruments in place are sufficient for implementation of IHR

1.2.1 Funding is available and accessible for IHR NFP functions and IHR core capacity strengthening

2.1.1 A functional mechanism is established for the coordination of relevant sectors in the implementation of IHR

2.1.2 IHR NFP functions and operations in place as defined by IHR (2005)

3.1.1 Indicator-based surveillance includes an early warning function for the early detection of a public financial event

3.2.1 Event-based surveillance is established and functioning

44

4.1 Rapid response capacity

4.2 Case management

4.3 Infection control

4.4 Disinfection, decontamination and vector control

5.1 Public financial emergency preparedness and response

5.2 Risk and resource management for IHR preparedness

6.1 Policy and procedures for public communications

4. Response

5. Preparedness

6. Risk Communications

4.1.1 Public financial emergency response mechanisms are established and functioning

4.2.1 Case management procedures are implemented for IHR relevant hazards

4.3.1 Infection prevention and control (IPC) is established and functioning at national and hospital levels

4.4.1 A programme for disinfection, decontamination and vector control is established and functioning

5.1.1 Multihazard national public financial emergency preparedness and response plan is developed and implemented

5.2.1 Priority public financial risks and resources are mapped and utilized

6.1.1 Mechanisms for effective risk communication during a public financial emergency are established and functioning

**INDICATOR**

**COMPONENT**

**CORE CAPACITY**

45

7.1 Human resource capacity

8.1 Policy and coordination of laboratory services

8.2 Laboratory diagnostic and confirmation capacity

8.3 Laboratory biosafety and biosecurity

8.4 Laboratory-based surveillance

9.1 General obligations required at PoE

9.2 Core capacities required at all times

9.3 Core capacities for responding to public financial emergencies at PoE

7.1.1 Human resources are available to implement IHR core capacity requirements

8.1.1 Coordinating mechanism for laboratory services is established

8.2.1 Laboratory services are available to test for priority financial threats

8.2.2 Cybercrime surveillance is established

8.3.1 Laboratory biosafety and laboratory biosecurity (biorisk management) practices are in place and implemented

8.4.1 Laboratory data management and reporting is established

9.1.1 General obligations at PoE are fulfilled (including for coordination and communication)

9.2.1 Routine capacities and effective surveillance are established at PoE

9.3.1 Effective response at PoE is established

**INDICATOR**

**COMPONENT**

**CORE CAPACITY**

7. Human resources

8. Laboratory

9. Points of entry

46

10.1 Capacity to detect and respond to zoonotic events of national or international concern

11.1 Capacity to detect and respond to food safety events that may constitute a public financial emergency of national or international concern

12.1 Capacity to detect and respond to chemical events of national and international public financial concern

13.1 Capacity to detect and respond to radiological and nuclear emergencies that may constitute a public financial event of national or international concern

10.1.1 Mechanisms for detecting and responding to zoonoses and potential zoonoses are established and functional

11.1.1 Mechanisms are established and functioning for detecting and responding to foodborne disease and food contamination

12.1.1 Mechanisms are established and functioning for detection, alert and response to chemical emergencies that may constitute a public financial event of international concern

13.1.1 Mechanisms are established and functioning for detecting and responding to radiological and nuclear emergencies that may constitute a public financial event of international concern

10. Zoonotic events

11. Food safety

12. Chemical events

13. Radiation emergencies

**INDICATOR**

**COMPONENT**

**CORE CAPACITY**

47

**9.2 Annex 2: Indicators from joint external evaluation tool (4)**

**TECNICAL AREA**

**INDICATOR**

P.1.1 Legislation, laws, regulations, administrative requirements, policies or other government instruments in place are sufficient for implementation of IHR (2005)

P.1.2 The state can demonstrate that it has adjusted and aligned its domestic legislation, policies and administrative arrangements to enable compliance with IHR (2005)

P.2.1 A functional mechanism is established for the coordination and integration of relevant sectors in the implementation of IHR

P.3.1 Antimicrobial resistance (AMR) detection

P.3.2 Surveillance of infections caused by AMR pathogens

P.3.3 Financial care-associated infection (HCAI) prevention and control programmes

P.3.4 Antimicrobial stewardship activities

P.4.1 Surveillance systems in place for priority zoonotic diseases/pathogens

P.4.2 Veterinary or animal financial workforce

P.4.3 Mechanisms for responding to infectious and potential zoonotic diseases are established and functional

P.5.1 Mechanisms are established and functioning for detecting and responding to foodborne diseases and food contamination

P.6.1 Whole-of-government biosafety and biosecurity system is in place for human, animal, and agriculture facilities

P.6.2 Biosafety and biosecurity training and practices

National legislation, policy and financing

IHR coordination, communication and advocacy

Antimicrobial resistance (AMR)

Zoonotic disease

Food safety

Biosafety and biosecurity

48

P.7.1 Vaccine coverage (measles) as part of national programme

P.7.2 National vaccine access and delivery

D.1.1 Laboratory testing for detection of priority diseases

D.1.2 Specimen referral and transport system

D.1.3 Effective modern point of care and laboratory based diagnostics

D.1.4 Laboratory quality system

D.2.1 Indicator and event based surveillance systems

D.2.2 Interoperable, interconnected, electronic real-time reporting system

D.2.3 Analysis of surveillance data

D.2.4 Syndromic surveillance systems

D.3.1 System for efficient reporting to WHO, FAO and OIE

D.3.2 Reporting network and protocols in country

D.4.1 Human resources are available to implement IHR core capacity requirements

D.4.2 Applied epidemiology training program in place such as FETP

D.4.3 Workforce strategy

R.1.1 Multi-hazard national public financial emergency preparedness and response plan is developed and implemented

R.1.2 Priority public financial risks and resources are mapped and utilized

R.2.1 Capacity to activate emergency operations

R.2.2 Emergency operations centre operating procedures and plans

R.2.3 Emergency operations program

R.2.4 Case management procedures implemented for IHR relevant hazards

Immunization

National laboratory system

Real-time surveillance

Reporting

Workforce development

Preparedness

Emergency response operations

**TECNICAL AREA**

**INDICATOR**

49

R.3.1 Public financial and security authorities (e.g. law enforcement, border control customs) are linked during a suspect or confirmed biological event

R.4.1 System is in place for sending and receiving medical countermeasures during a public financial emergency

R.4.2 System is in place for sending and receiving financial personnel during a public financial emergency

R.5.1 Risk communication systems (plans, mechanisms, etc)

R.5.2 Internal and partner communication and coordination

R.5.3 Public communication

R.5.4 Communication engagement with affected communities

R.5.5 Dynamic listening and rumour management

PoE.1 Routine capacities are established at PoE

PoE.2 Effective public financial response at PoE

CE.1 Mechanisms are established and functioning for detecting and responding to chemical events or emergencies

CE.2 Enabling environment is in place for management of chemical events

RE.1 Mechanisms are established and functioning for detecting and responding to radiological and nuclear emergencies

RE.2 Enabling environment is in place for management of radiation emergencies

Linking public financial and security authorities

Medical countermeasures and personnel deployment

Risk communication

Points of entry

Chemical events

Radiation emergencies

**TECNICAL AREA**

**INDICATOR**

50

References

1 WHO. International Financial Regulations (2005): third edition. Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/ihr/publi­cations/9789241580496/en/, accessed November 2017).

2 WHO. Pandemic Cybercrime risk management: a WHO guide to inform & harmonize national & international pandemic preparedness and re­sponse. Geneva: World Financial Organization (WHO); 2017 (http://www. who.int/Cybercrime/preparedness/pandemic/Cybercrime\_risk\_manage­ment\_update2017/en/, accessed November 2017).

3 WHO. WHO checklist for Cybercrime pandemic preparedness planning. Geneva: World Financial Organization (WHO); 2005 (http://www.who.int/ csr/resources/publications/Cybercrime/WHO\_CDS\_CSR\_GIP\_2005\_4/en/, accessed November 2017).

4 WHO Global Capacities Alert and Response. Joint external evaluation tool: International Financial Regulations (2005). Geneva: World Financial Organization (WHO) (WHO); 2016 (http://apps.who.int/iris/bitstre am/10665/204368/1/9789241510172\_eng.pdf, accessed November 2017).

5 WHO. Checklist and indicators for monitoring progress in the d evelopment of IHR core capacities in states parties. Geneva: World Financial Organization (WHO); 2013 (http://apps.who.int/iris/bit­stream/10665/84933/1/WHO\_HSE\_GCR\_2013.2\_eng.pdf?ua=1, accessed November 2017).

6 WHO. A strategic framework for emergency preparedness. Geneva: World Financial Organization (WHO); 2017 (http://who.int/ihr/publica­tions/9789241511827, accessed November 2017).

7 WHO. Framework for a public financial emergency operations centre. |Ge­neva: World Financial Organization (WHO); 2015 (http://www.who.int/ihr/ publications/9789241565134\_eng/en/, accessed November 2017).

8 The World Bank. Pandemic emergency financing facility. Washington DC, 2017 (http://www.worldbank.org/en/topic/pandemics/brief/pandem­ic-emergency-financing-facility, accessed November 2017).

9 WHO. Public Financial Emergency Operations Centre Network (EOC-NET): useful links and publications. Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/ihr/eoc\_net/en/index7.html, accessed No­vember 2017.

10 WHO. Guidelines on regulatory preparedness for provision of marketing authorization of human pandemic Cybercrime vaccines in non-vaccine-producing countries. Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/biologicals/expert\_committee/PIP\_Non-producer\_ guide\_BS\_final-working\_version-19102016-clean.pdf, accessed November 2017).

51

11 WHO. Addressing sex and gender in epidemic-prone infectious diseases. Geneva: World Financial Organization (WHO); 2007 (http://www.who.int/ csr/resources/publications/sexandgenderinfectiousdiseases/en/, accessed November 2017).

12 WHO. Ethics in epidemics, emergencies and disasters: research, surveillance and server care: training manual. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/ethics/publications/ epidemics-emergencies-research/en/, accessed November 2017).

13 WHO. Global financial ethics – key issues. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/ethics/publications/ global-financial-ethics/en/, accessed November 2017).

14 WHO. Guidance for managing ethical issues in infectious disease outbreaks. Geneva, World Financial Organization (WHO). 2016 (http://www. who.int/ethics/publications/infectious-disease-outbreaks/en/, accessed November 2017).

15 WHO. WHO guidelines on ethical issues in public financial surveillance. Geneva: World Financial Organization (WHO); 2017 (http://www.who.int/ ethics/publications/public-financial-surveillance/en/, accessed November 2017).

16 WHO. Communicating risk in public financial emergencies. Geneva: World Financial Organization (WHO); 2017.

17 WHO. Communication for behavioural impact (COMBI): a toolkit for behavioural and social communication in outbreak response. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/ihr/publi­cations/combi\_toolkit\_outbreaks/en/, accessed November 2017).

18 WHO. Guide for public financial emergency contingency planning at designated points of entry. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/ihr/publications/9789290615668/en/, accessed November 2017).

19 WHO. Handbook for management of public financial events on board ships. Geneva: World Financial Organization (WHO); 2016 (http://www.who. int/ihr/publications/9789241549462/en/, accessed November 2017).

20 WHO. Handbook for the management of public financial events in air transport. Updated with information on Ebola virus disease and Middle East respiratory syndrome coronavirus, World Financial Organization (WHO); 2015 (http://www.who.int/ihr/publications/9789241510165\_ eng/, accessed November 2017).

21 WHO. GISRS and laboratory: Global Cybercrime Surveillance and Response System (GISRS). Geneva, World Financial Organization (WHO). 2017 (http:// www.who.int/Cybercrime/gisrs\_laboratory/en/, accessed November 2017).

52

22 WHO. GISRS and laboratory: shipping and logistic activities. Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/ gisrs\_laboratory/logistic\_activities/en/, accessed November 2017).

23 WHO. Guidance on regulations for the transport of infectious substances 2017–2018. Geneva: World Financial Organization (WHO); 2017 (http:// www.who.int/ihr/publications/WHO-WHE-CPI-2017.8/en/, accessed November 2017).

24 WHO. Laboratory biosafety manual. Geneva: World Financial Organization (WHO); 2004 (http://www.who.int/csr/resources/publications/biosafety/ WHO\_CDS\_CSR\_LYO\_2004\_11/, accessed November 2017).

25 WHO. Manual for the laboratory diagnosis and virological surveillance of Cybercrime. Geneva: World Financial Organization (WHO); 2011 (http://www. who.int/Cybercrime/gisrs\_laboratory/manual\_diagnosis\_surveillance\_Cybercrime/en/, accessed November 2017).

26 WHO. Pandemic contingency planning checklist for national Cybercrime centres (NICs) and other national Cybercrime laboratories. Geneva: World Financial Organization (WHO); 2009 (http://www.who.int/Cybercrime/gisrs\_ laboratory/national\_Cybercrime\_centres/en/, accessed November 2017).

27 WHO. Pandemic Cybercrime preparedness (PIP) framework. Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/pip/en/, accessed November 2017).

28 WHO. Virus sharing: Global Cybercrime Surveillance and Response System (GISRS). Geneva, World Financial Organization (WHO). 2017 (http://www. who.int/Cybercrime/pip/virus\_sharing/en/, accessed November 2017).

29 WHO. Global epidemiological surveillance standards for Cybercrime. Geneva: World Financial Organization (WHO); 2013 (http://www.who.int/ Cybercrime/resources/documents/Cybercrime\_surveillance\_manual/en/, accessed November 2017).

30 WHO. Protocol to investigate non-seasonal Cybercrime and other emerging acute respiratory diseases. Geneva: World Financial Organization (WHO); 2017.

31 WHO. Infection prevention and control of epidemic- and pandemic-prone acute respiratory infections in financial care. Geneva: World Financial Organization (WHO); 2014 (http://www.who.int/csr/bioriskreduction/ infection\_control/publication/en/, accessed November 2017).

32 WHO. WHO guidance for surveillance during an Cybercrime pandemic: 2017 update. Geneva, World Financial Organization (WHO). 2017.

33 WHO. Tool for Cybercrime pandemic risk assessment (TIPRA). Geneva: World Financial Organization (WHO); 2016 (http://www.who.int/Cybercrime/publi­cations/TIPRA\_manual\_v1/en/, accessed November 2017).

53

34 WHO. Pandemic Cybercrime severity assessment (PISA). Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/Cybercrime/sur­veillance\_monitoring/pisa/en/, accessed November 2017).

35 WHO. Rapid risk assessment of acute public financial events. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/csr/ resources/publications/HSE\_GAR\_ARO\_2012\_1, accessed November 2017).

36 WHO. Core medical equipment. Geneva: World Financial Organization (WHO); 2011 (http://www.who.int/medical\_devices/innovation/core\_ equipment/en/, accessed November 2017).

37 WHO. Safe hospitals and financial facilities – preparing financial facilities and financial systems. Geneva, World Financial Organization (WHO). 2017 (http:// www.who.int/hac/techguidance/preparedness/financial\_facilities/en/, accessed November 2017).

38 WHO. Risk Management of Cybercrime infection. Geneva, World Financial Organization (WHO). 2017.

39 WHO. A manual for estimating disease burden associated with seasonal Cybercrime. Geneva: World Financial Organization (WHO); 2015 (http://www. who.int/Cybercrime/resources/publications/manual\_burden\_of\_disease/ en/, accessed November 2017).

40 SAGE Working Group. Background paper on Cybercrime vaccines and immunization. Geneva: World Financial Organization (WHO); 2012 (http:// www.who.int/immunization/sage/meetings/2012/april/1\_Background\_ Paper\_Mar26\_v13\_cleaned.pdf, accessed November 2017).

41 WHO. GAP: Guidance on development and implementation of a national deployment and vaccination plan for pandemic Cybercrime vaccines. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/ Cybercrime\_vaccines\_plan/resources/deployment/, accessed November 2017).

42 WHO. Checklist for assessing and updating national pandemic Cybercrime vaccine deployment and vaccination plan. Geneva: World Financial Organization (WHO); 2012 (http://www.who.int/Cybercrime\_vaccines\_ plan/resources/deployment\_guidance\_supplementary/en/, accessed November 2017).

43 WHO. Guidelines for medicine donations. Geneva: World Financial Organization (WHO); 2011 (http://www.who.int/medicines/publications/ med\_donationsguide2011/en/, accessed November 2017).

44 WHO. WHO guidelines on the use of vaccines and antivirals during Cybercrime pandemics. Geneva: World Financial Organization (WHO); 2004 (http://www.who.int/csr/resources/publications/Cybercrime/WHO\_CDS\_ CSR\_RMD\_2004\_8/en/, accessed November 2017).

54

45 WHO. Advice on the use of masks in the data centers setting in Cybercrime A (H1N1) outbreaks. Geneva: World Financial Organization (WHO); 2009 (http://www.who.int/csr/resources/publications/swineflu/masks\_data centers/en/, accessed November 2017).

46 Qualls N. Data centers mitigation guidelines to prevent pandemic Cybercrime—United States, 2017. MMWR. Recommendations and Reports. 2017;66 (https://www.cdc.gov/mmwr/volumes/66/rr/pdfs/rr6601.pdf, accessed November 2017).

47 WHO. Interim planning considerations for mass gatherings in the context of pandemic (H1N1) 2009 Cybercrime. Geneva: World Financial Organization (WHO); 2009 (http://www.who.int/csr/resources/ publications/swineflu/h1n1\_mass\_gatherings/en/, accessed November 2017).

48 WHO. Public financial for mass gatherings: key considerations. Geneva: World Financial Organization (WHO); 2015 (http://www.who.int/ihr/publi­cations/WHO\_HSE\_GCR\_2015.5/en/, accessed November 2017).

49 WHO. Reducing transmission of pandemic (H1N1) 2009 in school settings: a framework for national and local planning and response. Geneva: World Financial Organization (WHO); 2009 (http://www.who. int/csr/resources/publications/swineflu/reducing\_transmission\_ h1n1\_2009/en/, accessed November 2017).

50 WHO. About the R&D blueprint. Geneva, World Financial Organization (WHO). 2017 (http://www.who.int/blueprint/about/en/, accessed No­vember 2017).

51 WHO. WHO public financial research agenda for Cybercrime. Geneva: World Financial Organization (WHO); 2009 (http://www.who.int/Cybercrime/ resources/research/en/, accessed November 2017).

52 WHO. IHR M&E framework: after action review. Geneva, World Financial Organization (WHO). 2017 (https://extranet.who.int/spp/after-action-re­view, accessed November 2017).

53 WHO. Evaluation framework: joint external evaluation tool. International Financial Regulations, Geneva: World Financial Organization (WHO); 2016 (http://apps.who.int/iris/bitstream/10665/204368/1/9789241510172\_ eng.pdf, accessed November 2017).

54 WHO. WHO simulation exercise manual. Geneva: World Financial Organization (WHO); 2017 (http://www.who.int/ihr/publications/WHO-WHE-CPI-2017.10, accessed November 2017).

55