Policy Cover	
Title: Contingency Plan Policy and Procedures	**Effective Date:** March 20, 2018
	Adoption/Revision Date: March 20, 2018
Custodian: Services Director	**Approving Body:** Executive Committee

1. **Authority**
    a. Executive Committee
2. **References**
    a. Various IT Steering Committee minutes.
3. **Purpose**
    1) To limit the amount of time Information Technology may be inaccessible.
    2) To respond to emergencies that damage Information Technology that create, receive, maintain, and transmit Electronic Protected Health Information (ePHI), as well as other restricted and sensitive information, and other information in critical systems.
    3) To anticipate worst-case threat sources, emergency situation, and/or Disaster scenarios and decide how best to react to them and recover Information Technology while ensuring the confidentiality, integrity, and availability of ePHI, as well as other restricted and sensitive information.
    4) To determine what could happen if the organization's ePHI, as well as other restricted and sensitive information (or other significant portions of an organization's infrastructure external or internal to the organization) is partially or totally destroyed or otherwise unavailable and what the organization does to recover from that.
4. **Scope**
    a. Applies to all Clark County Government employees.
5. **Policy Overview**
    a. This sets expectations and guidelines for all Clark County employees who use and manage resources and services including, but not limited to, computing, networking, communications and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, and any related materials and services.
6. **Policy Performance**
    a. The quantifiable performance indicator for this policy is one-hundred percent (100%) compliance by Clark County personnel.
7. **Clark County Mission Statement**

The mission of Clark County and its employees is to provide cost effective services, with equal access to all citizens; to continue and enhance partnerships; to responsibly manage our resources and prepare for the future.

CLARK COUNTY
CONTINGENCY PLAN POLICY AND PROCEDURES

RESPONSIBLE FOR IMPLEMENTATION

The Contingency Plan is developed, overseen, activated, and maintained by the Information Technology Department. The Information Technology Director is responsible for implementing and overseeing this P&P.

POLICY

1. It is the policy of Clark County to have systems, especially those containing Electronic Protected Health Information (ePHI), as well as other restricted and sensitive information, collectively "Confidential Information", available at all times as well as during an emergency or a Disaster as needed and feasible to provide critical services. Critical services include, but are not limited to the following:
   A. Clark County access to the practice management / billing systems.
   B. Sheriff's department critical systems.
   C. Critical systems as defined by other departments and agreed upon by the Information Technology department.
2. To provide the organization with a current information system Contingency Plan and Disaster Recovery Plan that supports timely restoration and recovery of interrupted critical clinical and business operations during an emergency or Disaster situation.
3. To minimize possible adverse clinical outcomes, as well as financial and business impacts, to the organization as a result of an interruption of normal business operations through manual and automated methods of accessing needed information during an emergency.
4. To meet the needs of the organization's patients, workforce members, customers, and other stakeholders reliant on the organization's ability to provide necessary services during and following an emergency or Disaster situation.
5. To continue to protect Confidential Information to the extent possible even during emergencies and Disasters.
6. To protect the public image and credibility of the organization.

DEFINITIONS

Contingency Planning: The process of developing procedures that enable an organization to respond to emergencies so that critical business functions continue with planned levels of interruption or essential change, while continuing to protect Confidential Information.

Disaster (Information System): An event that makes the continuation of normal information system functions impossible; an event which would render the information system unusable or inaccessible for a prolonged period of time (may be departmental or organization-wide).

Disaster Recovery Plan: Defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated Disaster recovery goals.

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or maintained in electronic media.

Security Incident: An Occurrence that exercises a significant adverse effect on people, process, technology, Confidential Information data or facilities. Security incidents include, but are not limited to:

- A system or network Breach accomplished by an internal or external entity; this Breach can be inadvertent or malicious
- Unauthorized or unintentional acquisition, Access, use, or Disclosure of Confidential Information (a Breach)
- Unauthorized change or destruction of Confidential Information
- Physical or biological threat to staff members or external entities at the site
- Disaster or enacted threat to business continuity
- Information Security Incident: A violation or imminent threat of violation of the Clark County General Technology Policy. Examples of information Security Incidents may include, but are not limited to, the following:
  - **Denial of Service:** An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
  - **Malicious Code**: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host
  - **Unauthorized Access/System Hijacking:** A person gains logical or physical access without permission to a network, system, application, Confidential Information data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations.
  - **Inappropriate Usage:** A person violates acceptable computing use policies
  - **Unplanned Downtime:** The network, system, and/or applications are not accessible due to any unexplainable circumstance causing downtime more than identified recovery point objectives and recovery time objectives (due to system failure, utility failure, disaster situation, etc.)
  - **Multiple Component:** A single incident that encompasses two or more incidents (e.g., a malicious code infection leads to unauthorized Access to a host, which is then used to gain unauthorized Access to additional hosts).
- Other examples of observable information Security Incidents may include, but are not limited to:
  - Use of another person's individual password and/or account to login to a system
  - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment)
  - Leaving workstations unattended while actively signed on
  - Installation of unauthorized software
  - Falsification of information
  - Lost or stolen workstations (including personal devices that connect to the network and/or Information Technologies)
  - Theft of software
  - Destruction of tampering with equipment or software

- Posting / storing of Confidential Information to applications, websites, devices, etc.
- Discarding of PC hard drives, CDs or other devices including Confidential Information without following approved destruction/disposal guidelines
- Files mysteriously increasing in size
- Terminated workforce member accessing applications, systems, or network

Privacy Officer which is designated as Clark County Corporation Counsel and is defined as:
The **Privacy Officer** oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the **privacy** of, and access to, patient health information in compliance with federal and state laws and the healthcare.

Security Officer which is designated as Clark County Services Director and is defined as:
The **Security Officer** is responsible for the ongoing management of information **security** policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all patient health Information Technology.

PROCEDURES

1. **Environmental controls**.
   A. The Information Technology Director and Security Officer make all reasonable efforts to have security controls and contingency plans in place that minimize the amount of time systems may be down to the least possible, but no more than identified recovery time objectives for critical systems, as long as it does not unduly hinder operational performance, jeopardize security, or increase costs.
   B. Critical Confidential Information Technology:
      i) Are on an uninterrupted power supply (UPS) with warning lights or alarms.
         (1) UPS powers this equipment for up to 24 minutes
         (2) UPS are tested monthly
      ii) For the sheriff's department are on a generator
   C. The following are in each server room/wiring closet. Exceptions are approved and documented by the Information Technology Director and Security Officer:
      i) A cooling system
      ii) A backup cooling system
      iii) Fire suppression system
      iv) Electrical fire rated fire extinguisher
      v) Temperature, humidity, and fire alarms/paging
      vi) Located away from any water source
      vii) Locked room with access limited to the minimum necessary needed to maintain/recover systems.
   D. All reasonable efforts are made to ensure organizations/vendors that Vendors/business associates that create, receive, maintain, transmit, and backup Confidential Information have sound security controls that minimize downtimes and allow them to recover systems within identified recovery times, such as the above stated controls. Exceptions are approved and documented by the Information Technology Director and Security Officer.

2. **Facility Security**
   A. Only those individuals (that are able to assist in restoring access to Confidential Information) may have access to and be in the server and data wiring rooms as well as have access to backups, even during emergencies and Disaster situation.
      i) In the event of an emergency situation that renders the server and data wiring rooms uninhabitable (e.g. fire, chemical spill, tornado, etc.), appropriate emergency personnel will control access to the site during the entire course of the emergency.
      ii) Priority will be given to the safety of people and to evacuating as much equipment as possible to a safe indoor location, or a safe and guarded outdoor location, until it can be moved to a better location. If necessary, on site Information Technology staff will direct the effort and work with other agencies to secure help to move and transport equipment.
      iii) Movement, repair, and restoring of service will be prioritized. Equipment will be secured in accordance with the level of security of the information that remains.
   B. These authorized individual also have ID badge access and/or keys to enter the primary and secondary sites to assist in efforts to restore access to Confidential Information.
3. **Contingency Plans.** The Information Technology Department oversees and has the authority and overall responsibility for facilitating the implementation, activation, coordination, and documentation of the contingency plan and Disaster recovery operations, including the following:
   A. Maintains a contact list for each system with the current Contingency Plan/DRP (refer to the Vendor Emergency Contact Information form, Attachment B).
      i) The contact list includes key workforce members and key vendors and other individuals that help support and recover systems such as: business associates, stakeholders, utilities management (e.g. electric, water, gas), telecommunications/phone, internet services provider(s), emergency government and law enforcement/government agencies, radio and TV stations, etc.
      ii) The contact information for each includes name(s), company name(s), address, main and backup telephone numbers, email address, and web site address, as applicable.
   B. Obtains Contingency Plans/DRPs from vendors and other business associates when they are necessary to be incorporated into the organization's contingency and Disaster recovery plans.
   C. Maintains an Inventory Asset List for each system, application, server, hardware, IT equipment (workstations, portable devices, etc.), network information/specifications, etc. purchased or leased by Clark County that are used to access, create, receive, maintain, or transmit Confidential Information. This list includes, at a minimum and as applicable:
      i) Critical functions which help determine how important each system is to business needs.
      ii) Indication of the critical systems that are supported at alternate sites.
      iii) Location and who uses each Confidential Information system, workstation, and portable device.
      iv) Model and serial numbers, manufacturer, operating systems, where to purchase, warranty information, etc. so items can easily be replaced, as applicable.
      v) Interdependencies/interoperability on other systems, applications, servers, etc., with a recovery plan for each.
      vi) Expected date of retirement.
      vii) Retired assets
   D. Assigns a Data Criticality Level for each system, application, server, hardware, IT equipment, network information/specifications, etc.
      i) Applications, systems, and/or networks that need to be available at all times and need to be recovered/restored first are prioritized; they are ranked in order of critical functions and recovery order.

E. Maintains a current network diagram of all servers, systems, interfaces, etc.
F. Creates and maintains a list of most significant types of Threat sources that are the most likely to damage systems containing or affect the availability of Confidential Information and/or critical systems.
G. Maintains a list of Disaster recovery supplies needed and ensures that they are readily available (refer to the Disaster Recovery Supply Checklist, Attachment A).
H. Makes arrangements for a Recovery facility(s) for the IT Disaster Recovery Command Center, as needed to provide critical services.
   i) The Command Center functions as the centralized location for IT Disaster recovery processes and has the necessary critical resources and equipment required for Disaster recovery.
   ii) Recovery facility Locations.
      (1) Onsite location: basement of the Clark County Courthouse
      (2) Off-site location: RLC.
   iii) Maintains documentation of the steps and resources needed to bring the recovery facility locations on-line while maintaining the security of Confidential Information.
   iv) During emergencies, Workforce may work from their homes, as assigned by Department Heads and needed to provide critical services. Workforce are required to continue to adhere to the organization's information security policies and procedures.

4. **Emergencies: Activation of the Contingency Plan.**
   A. Contact the Information Technology Department when a system(s) and/or network is down.
   B. The Information Technology Department activates the Contingency Plan/DRP, as appropriate. In situations that affect single systems, the Information Technology Department restores the system.
   C. The Information Technology Department contacts the appropriate vendor to report the issue and obtain a status, as applicable to the situation.
   D. Protect Confidential Information
      i) During emergencies, all users must continue to protect Confidential Information to the extent possible, to prevent a breach of confidentiality
      ii) Users may not share passwords or allow others to utilize systems logged in by the user, unless instructed to do so by the Security Officer or Information Technology Director.
   E. Notifications
      i) The Information Technology Director or Security Officer notifies Department Heads with a summary of the emergency and potential outage times and alternative processes in place.
         (1) Department Heads notify Workforce of the situation and work responsibilities.
         (2) Department Heads notify appropriate clients and business partners in the event of a disaster.
   F. System Recovery: The Information Technology Department recovers Information Technology.
      i) DRP procedures to each recover system, based on each type of significant threat source, Disaster, and/or emergency scenario are located in a folder on the SharePoint site that is accessible to the Information Technology Department and Legal Counsel.
      ii) DRP procedures to restore lost Confidential Information for each type of system which stores Confidential Information, including what data to restore are located in in a folder on the SharePoint site that is accessible to the Information Technology Department and Legal Counsel.

5. **Contingency Plan Testing and Maintenance**
   A. Testing
      i) Contingency Plan/DRP testing is done annually when possible, but at a minimum every two years.
         (1) A scenario-based walk-through or "mock" drill is done to examine the plans and determine the need for changes.
         (2) The alternative sites are also reviewed to verify they support Contingency Plan/DRP needs (with backed-up Confidential Information), should the main facility be compromised.
      ii) During the normal use of any system, components fail. Document why the system was down and how the system was recovered. Maintain this documentation as a part of the Contingency Plan/DRP testing files.
   B. Maintenance and Revision
      i) The Information Technology Department is responsible for maintenance and revision of the Contingency Plans/DRP.
         (a) The Contingency Plans/DRP are reviewed and revised annually when possible, but at a minimum every two years and when needed to ensure that the information it contains is current.
         (b) The Contingency Plans/DRP is reviewed and revised to address issues identified after each Disaster incident, whether a planned drill or actual Disaster.
      ii) All revisions are provided to those that need to follow the plans.
6. **Education and Training**
   A. Users of critical systems are trained on how to access necessary Confidential Information during an emergency and continue to protect Confidential Information during emergencies, as applicable to their roles.
   B. Workforce members are provided education and training in emergency preparedness and the contingency plans upon hire, annually, and when significant changes to the organization's contingency plans, emergency preparedness, and Disaster recovery plans are made that impact them.
   C. Workforce members with specific responsibilities for IT Disaster recovery receive specific training so that they can carry out their assigned duties.
7. **Documentation**
   A. Copies of the Contingency Plan and Disaster Recovery Plans are maintained on and offsite and are readily available in the event of an emergency.
      i) Copies are maintained are accessible to the Information Technology Department and Legal Counsel in the following locations:
         (1) In a SharePoint site folder
         (2) Hard copy, and
         (3) Encrypted USB drive.
      ii) Copies are in a safe location and only accessible by these individuals (e.g. in a locked fire safe, in a bank safety deposit box, encrypted or password protected flash drive, etc.).
   B. Contingency Plans/DRP information, including the controls in place, testing, and revisions are maintained for 6 years from the last date in effect.

Policy Attachments

ATTACHMENT A

DISASTER RECOVERY SUPPLY CHECKLIST

Disaster Recovery Resources Supply Checklist	
Workspace □ Desk, Chairs, Tables, Lights □ Electrical Support □ Telecommunications Support	**Documentation** □ Hardware Inventory Lists and Serial Numbers □ Software Inventory Lists and License Numbers □ Network Schematic Diagrams □ Equipment Room Floor Grid Diagrams for Each Facility, Alternate Sites, and Command Center □ Contract and Maintenance Agreements □ Steps to recover systems/applications/networks □ Steps to recover ePHI □ Steps to restore lost data
Hardware □ PC's/Laptops □ Printers □ Scanners □ Server □ Wiring □ Secondary Power Sources □ Flash drives (encrypted)	**Forms** (Each department is responsible for determining what forms to stock in the event any/all systems are unavailable, the power is out, or there is a nature disaster. Below are some examples). □ Clinical forms to track/monitor patient care □ Patient registration forms □ Invoices □ Human Resources forms (payroll, workers compensation, etc.) □ Maintenance Forms □ Message Pads
Software **Back-Up Copies of Data Files**	**Other Supplies** □ Office Supplies (pens, paper, folders, paper clips, scissors, staplers, tape, etc.)

Disaster Recovery Resources Supply Checklist	
Communications (Identify Location of Each) □ Telephones □ Cellular Phones With Chargers □ Fax and Backup Fax □ Dedicated Telephone Line(s) □ Radios (Walkie-Talkie, Weather) as Required □ Organizational Contact Information/Directories □ Telephone Directories □ Telephone Log	□ Office Equipment (shredder, copiers, etc.) □ Camera/Video Recorder □ Film/Blank Recoding Media □ Duct Tape □ Backup Media □ Flashlights and Spare Batteries □ Area Maps/Site Maps of Each Facility, Including Alternate Sites and Command Centers
Other	

Attachment B

CLARK COUNTY
Vendor Emergency Contact Information

Vendor/System Name	Brief Description	Contact	Phone #	Other Phone #	Email Address	Website Link	Contract Number	Address	Other

Attachment C

Policy Review Form

Completed by Policy Custodian

Policy Title	IT Services Director
Overview of Adoption/Revision	03 08 2018
Policy Submitted By	Cindy Currier
Policy Submitted To	IT Steering Committee and Executive Committee
Anticipated Date of Policy Final Approval	March 8, 2018

Completed by IT Steering Committee

Policy Received On	February 27, 2018
Policy Approved/Denied On w/ Reason	Approved
Policy Approved/Denied By	IT Steering Committee
Policy Storage Location	J:\Everyone\Policies\IT Policies
Policy Forwarded to Corporation Counsel	03 07 2018

Completed by Corporation Counsel

Policy Received On	03 07 2018
Policy Approved/Denied On w/Reason	Approved with changes
Policy Approved/Denied By	Jacob Brunette
Policy Forwarded to Executive Committee	03 08 2018

Completed by Executive Committee

Policy Received On	03 08 2018
Policy Approved/Denied On w/Reason	Approved
Policy Approved/Denied By	Executive Committee

Revision History		
Adoption/Revision Date	**Overview of Adoption/Revision**	**Adoption/Revision Reference**
March 20, 2018	Original	Resolution 13-3-18