have become corrupted or unintentionally deleted. These systems must be backed up periodically, usually every night. Failover systems minimize disruptions in patient care and loss of data and are usually on the premises and switched over within a few seconds or minutes of the primary system becoming unavailable due to planned or unplanned downtime. In hospitals that use a cloud-based system for data backup, the vendor must have adequate backup systems in place to minimize disruptions to care, prevent loss of data, and maintain data integrity.

Hospitals that plan for maintaining access to electronic information systems by using various backup and recovery processes are likely to experience seamless continuity of patient care and minimal data loss.

The way information is communicated to staff depends on the system that is down. For example, if the hospital's network goes down, communication to staff via telephone may be required. Multiple communication strategies should be developed to address the different systems that may be affected. In addition to internal communication strategies, it may be necessary to develop strategies for external communication. For example, if the hospital has an interfacing application with outside/contracted laboratory or radiology services and it becomes unavailable due to downtime, there needs to be a process for obtaining the results during downtime and a plan to have results reported back via the interface when the downtime is over.

One approach to managing downtime is the practice of having a packet of hard-copy downtime forms or a downtime binder available to continue care if unplanned downtime exceeds a certain time threshold (typically greater than 30 minutes). Another approach is to maintain a downtime computer that allows read-only access to patient data.

Hospitals need to define what data may need to be reentered in a discreet format (for example, all medications prescribed during downtime, select orders, allergies, problem lists), what data may need to be scanned in, and what data may need to be transcribed from hard copy to soft copy. To ensure confidentiality and security of information, the hospital should have a documented process for the management of any paper documentation used during downtime.

Many tools are available for backing up data. The optimal backup solutions for each hospital depend on many factors, including the amount of data requiring backup, the speed at which data can be backed up and recovered, the location of recovery systems, costs, and other factors.

Measurable Elements of HCT.01.04

1. Ⓓ The hospital maintains, and tests at least annually, a written program for response to planned and unplanned downtime of data systems. (*See also* FMS.08.00, ME 1; HCT.01.05, ME 1)
2. The hospital identifies the probable impact that planned and unplanned downtime of data systems will have on all aspects of care and services.
3. The program includes continuity strategies for the provision of ongoing safe, high-quality patient care and services, including services provided by outside vendors, during planned and unplanned downtime of data systems.
4. The program identifies internal and, when applicable, external communication strategies for planned and unplanned downtime.
5. The hospital implements downtime recovery tactics and ongoing data backup processes to recover and maintain data and ensure data integrity and maintain confidentiality and security of patient information.
6. Staff are trained in the strategies and tactics used for planned and unplanned downtime of data systems.

Standard HCT.01.05

The hospital develops and maintains processes and procedures for cybersecurity and cyber risk management.

Intent of HCT.01.05

Cyberattacks in health care carry more risk due to the type and widespread use of information and can be detrimental to patient safety and hospital operations if not properly managed.

Cyberattacks have the potential to interrupt and delay a variety of services throughout a hospital system, including ambulance transport, surgeries, medication delivery, and system operations (HVAC) to name a few. Information technology, whether in the form of the electronic health record (EHR) or that used throughout the hospital system, is susceptible to cyberattacks. As technology advances within the system, cybersecurity advancements need to be made as well to ensure patient safety and prevent operational delays. Areas that are vulnerable to cyberattacks include but are not limited to the following:

- EHR
- E-prescribing software
- Remote patient monitoring
- Laboratory information systems
- Medical billing software
- Scheduling software
- Communication systems

Measures and procedures for cybersecurity are necessary to protect valuable patient information during attacks. For example, penetration testing can be used to simulate a variety of attacks using similar tools that cyberattackers would use to find weaknesses within the system. From these test results, a response program could be constructed.

Downtime related to cyberattacks requires a differentiated plan from the standard planned or unplanned downtime for hospitals that use an electronic health record and communication system. In the event of a cyberattack, there must be a process to report details to the information technology (IT) department, hospital leaders, and a cyber team if applicable.

Most departments in the hospital handle information that is highly sensitive and valuable to cyber hackers. Staff, including providers of care, billing agents, administrative staff, and scheduling agents, manage this information daily and require specialized training to understand safe practices and consequences of a cyberattack or breach. Initial and ongoing training should be conducted and documented for completion.

In many hospitals, resources allocated to the IT department may be limited due to a number of constraints. Leaders must consider all the medical devices that are interconnected throughout the system, the thousands of people using those devices, and inconsistent business/user processes.

In the event downtime occurs because of a cyberattack, there must be downtime recovery procedures for backing up, maintaining, and potentially recovering system data. There is no single correct way to manage a cyberattack, but having plans in place beforehand can reduce the impact. Both the US National Institute of Standards and Technology (NIST) and European Union Cybersecurity Agency (ENISA) have frameworks for establishing a risk-based approach.

A strong posture for security includes the following:

- Having a high-quality, stable application base and infrastructure (for example, hardware, software applications, operating systems, networking tools, and telecommunication tools)
- Having IT infrastructure with configuration management, change management, logging, and monitoring
- Having a proactive stance and security measures in place (for example, resources and budgeting)
- Having training and awareness for all employees who interact in any way with hospital technology

Strategies for reducing exposure to a cyberattack include but are not limited to the following:

- Filtering e-mail and checking suspicious content
- Updating security configurations on devices, servers, and systems
- Installing antivirus software

- Running penetration tests
- Limiting control of physical access
- Maintaining regularly scheduled backups, which are stored in a physical, offline location

Provisions should be made for communicating a security breach internally and notifying any affected party externally. For example, the General Data Protection Regulation (GDPR), in the European Union, implemented regulations for breach notification and penalties when not adhered to.

Measurable Elements of HCT.01.05

1. Ⓓ The hospital maintains, and tests at least annually, a written incident response program that includes the following:
   - Identifying the probable impact a cyberattack on data systems will have on all aspects of care and operations (*See also* HCT.01.04, ME 1)
   - Identifying strategies for the provision of ongoing safe and high-quality care and services
2. The program identifies internal and external communication strategies for those affected by cyberattacks or events.
3. The hospital implements recovery tactics and ongoing data backup processes to recover and maintain data, ensuring data integrity, confidentiality, and security.

Management of Lasers, Electrosurgical, and Other Optical Radiation Devices

Standard HCT.02.00

The hospital establishes and implements a program for the safe use of lasers, electrosurgical, and other optical radiation devices used for performing procedures and treatments.

Intent of HCT.02.00

Nearly all lasers, electrosurgical, and other optical radiation devices that are used in the clinical setting pose potential hazards for patients and staff if safety procedures and guidelines are not established and followed.

Lasers are a source of optical radiation, which includes ultraviolet radiation, high-intensity visible light, and infrared radiation. The narrow beam of high-intensity light from a laser can be targeted and focused for precise surgical procedures. As technology evolves, the use of lasers is becoming more common with surgical procedures, and their clinical use is broadening.

Laser surgeries are generally minimally invasive with less blood loss than conventional surgery, and patients typically experience shorter recovery times. Lasers are also used in noninvasive procedures providing safer alternatives for treating conditions without surgical intervention.

Lasers and other optical radiation devices can generate intense concentrations of heat, light, and reflected light. When the skin and eyes are exposed to the heat and light without adequate protection, skin burns and eye injuries, such as retinal burns, cataracts, and macular degeneration, may result. Injuries can come from direct contact with the light or with the reflected light from the laser.

Plumes are another potential hazard. These are the vapors, smoke, and particles produced during some surgical procedures. Plumes produced by lasers and electrosurgical devices (for example, cautery units) introduce a potential respiratory hazard for patients and staff, as they may contain irritants, toxins, tissue, bacteria, viruses, blood fragments, and other particles, depending on the type of procedure.