Davis County HOSPITAL & CLINICS | An Affiliate of MERCYONE.

Board of Trustees

October 18, 2021

Policies / Plans / Annual Reviews / Biennial Reviews **Action**

New Policy

- **Employee Health**
  - **Flu Vaccination Policy**
- **Information Technology**
  - **Vulnerability Management**

Revised Policy Statements

- **Employee Health**
  - **Employee Health Program**
- **Infection Prevention**
  - **Antibiotic Guidelines**
- **Information Technology**
  - **Asset Decommission Procedure**
  - **Asset Management Policy**
  - **Authentication Standard Procedure**
  - **Contingency Planning**
  - **Disaster Recovery Planning**
  - **Identity and Access Management Policy**
  - **Information Classification and Management Policy**
  - **Information Security Policy**
  - **Physical and Environmental Security**
  - **Risk Assessment Procedures**
  - **Sanctions**
  - **Security Training and Awareness Policy**
  - **Server Backup**
  - **Social Networking Procedure**

Biennial Reviews

- **Accounting**
- **Infection Prevention and Plans**
- **Information Technology**
- **Medical Associates**
- **Senior Life Solutions**
- **Trauma**

Current Status: *Pending* **PolicyStat ID:** *10391977*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE

Origination:	*N/A*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*N/A*
Next Review:	*2 years after approval*
Owner:	*Lynn Fellinger: Public Health Manager*
Policy Area:	*Employee Health*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Flu Vaccination Policy

Flu Vaccination Policy for Davis County Hospital & Clinics

PURPOSE:

The purpose of this policy is to protect staff, non-employees, patients, and families from acquiring seasonal influenza and to help prevent the unnecessary spread of the influenza virus between employees, non-employees, patients, and families. This is accomplished through the requirement that all health care personnel at Davis Co Hospital & Clinics (DCHC) receive annual influenza vaccination unless an excemption is granted.

POLICY:

Participation in Davis County Hospital and Clinic's (DCHC) influenza immunization program is **mandatory**. All contractors, students or other individual serving at DCHC will be required to provide the proof listed below prior to October 31st, or date determined by DCHC administration team each year. All providers, staff and volunteers employed by DCHC will be required to do one of the following:

- Receive a flu vaccination offered by DCHC free of charge
- Provide proof of immunization if received outside of our program. This may be a signed physician's note, immunization record that is dated and signed or a medical record document.
- Submit a medical or religious exemption Form. (see attachment). Take the form to your provider or your religious leader (Paster, Minister, Rabbi, Clergy, Priest, etc.) to complete and return to Employee Health.

PROCEDURE:

Individuals may request a Medical or Religious exemption to this requirement based on:

- Medical contraindication to the flu vaccine, which requires a signed statement from the individual's healthcare provider and identification of the reason
- Religious practice or creed that prohibits immunization, which requires a signed statement from the individual's minister/religious leader and must be renewed annually.

Medical exemption examples include life threatening allergy, sensitivity to thimerosal, history of Guillain-Barre' Syndrome, and pregnancy (until the point of pregnancy when the provider gives documented approval to safely vaccinate). Acute fever, acute respiratory infections or active illness must be resolved prior to receiving influenza vaccination.

All reasonable submitted exemption requests must be submitted to Employee Health by October 15th and are reviewed and processed by Employee Health, Infection Control, and HR.

The individual requesting the exemption will be notified in writing as to whether his/her request for exemption has been granted. If an exemption request is denied, the individual will be required to be immunized pursuant to this policy.

Medical or Religious exemption does not exempt the individual from the annual influenza prevention program, but rather is an alternate method of compliance in place of the influenza vaccine.

All individuals not receiving the flu vaccine and granted an exemption will be required to wear respiratory protection in the form of a hospital provided surgical mask which must be always worn with exceptions of breaks and mealtimes. Individuals will be required to wear the mask for the duration of the influenza season which ends March 31st. The mask should fit snugly and be secured to the face. The mask should be discarded and changed, at a minimum, at the end of the shift and immediately if it becomes soiled or moist.

Documentation

Employee Health will oversee receiving completed flu consent forms and completed exemption forms. All department leaders are responsible for making sure their staff are allowed adequate time to get their flu vaccinations. Employee Health will track all vaccinations and exemption documents.

All new employees will receive the flu vaccine or provide documentation of their immunization or exemption prior to the start of employment.

Employee Health will notify managers of staff that will not receive the flu vaccine due to medical or religious exemption. Managers will ensure that staff not receiving vaccine will comply with always wearing masks during flu season.

All flu vaccine will require employee written consent, consent forms are kept in the employee's Employee Health file, vaccinations are recorded electronically in IRIS (Iowa Registry of Immunization Services)

Vaccine Shortages

In the event of an influenza vaccine shortage, the situation will be evaluated by DCHC administration, relying of the expertise of Employee Health, Infection Prevention, Human Resources, Pharmacy, and medical leadership. Influenza vaccinations will be offered to personnel based on job function and risk of exposure to influenza. Priority will be established in accordance with recommendations by the Iowa Department of Public Health.

Attachments

DCH Influenza Vaccination Relgious Exemption Request-updated 9-8-2021 (002) (2).docx
Certificate of Immunization Exemption - Medical 12-21-16 Final (1).pdf

Approval Signatures

Step Description	Approver	Date
	Lynn Fellinger: Public Health Manager	pending

Applicability

Davis County Hospital

Davis County
HOSPITAL & CLINICS

An Affiliate of MERCYONE

Influenza Vaccination Religious Exemption Request From

Name: ________________________________ Dept:_______________ Date: ___________________

□ **I request a religious exemption to the seasonal influenza vaccine offered by Davis County Hospital.**

I understand that my failure to submit acceptable documentation describing my religious belief may result in my request for an exemption being denied. In making a request for religious exemption, my signature on this form is my testimony that my religious beliefs are sincerely held.

I understand that my request for an exemption may be reviewed by employee health/Infection Prevention staff who can assist in the evaluation of my request. I understand that to maintain a safer work environment for patients and staff, my director and/or supervisor will be notified of my exemption and that I must follow the guidelines in the employee health policy.

I consent to the release of this request including any supporting documentation to all such representatives of Davis County Hospital and Clinics, for the representatives to carry out their duties and to act on my request for an exemption.

To be completed by employee:

I request an exemption from the influenza immunization based on a sincerely held religious belief that prohibits me from receiving the influenza vaccine. State in the space below, your personal statement that describes your religious belief that prevents you from receiving the influenza vaccine.

____

____

____

____

Documentation from religious/spiritual leader, (Paster, Minister, Rabbi, Clergy, Priest etc.) is required and must be attached to this document.

Signature: ____ Date: _____________________

RETURN THIS FORM TO EMPLOYEE HEALTH NO LATER THAN OCTOBER 15TH.

Office Use Only:

Exemption Review Date: ____________

Approval Date: ___________ Denial Date: __________ Reason for Denial: __________________________

Signature: ______________________________________ Date: _____________________

Signature: ______________________________________ Date: _____________________

Iowa Department of Public Health
Certificate of Immunization Exemption

Medical Exemption

Name Last: ______________________________ First: __________________________ Middle: _________________________ Date of Birth: ___________

The above named applicant qualifies for a medical exemption to immunization for the following reason (select one):

□ In the opinion of a physician, nurse practitioner, or physician assistant the following required immunization(s) would be injurious to the health and well-being of the applicant or any member of the applicant's family or household (contraindication due to contact with family or household member applies only to MMR and Varicella vaccine). Check only those immunizations which are medically contraindicated:

- □ Hep B (Hepatitis B)
- □ DTaP (Diphtheria, Tetanus, Pertussis)
- □ IPV (Polio)
- □ Hib (*haemophilus influenza* type b)
- □ PCV (Pneumococcal)
- □ MMR (Measles/Rubella)
- □ Varicella (Chickenpox)
- □ Tdap (Tetanus, Diphtheria, Pertussis)
- □ Meningococcal (A, C, W, Y)

If, in the opinion of the physician, nurse practitioner, or physician assistant issuing the medical exemption, the exemption should be terminated or reviewed at a future date, an expiration date shall be recorded on the Certificate of Immunization Exemption.

□ Administration of the following required vaccine(s) would violate minimum interval spacing of at least 28 days from a dose of a previously received live vaccine. In this circumstance, the exemption shall apply only to an applicant who has not received prior doses of exempted vaccine. An expiration date, not to exceed 60 days, shall be recorded on the certificate. Check only the immunizations which are medically contraindicated:

- □ MMR (Measles/Rubella)
- □ Varicella (Chickenpox)

Certificate Expiration Date: __________________

A child granted a medical exemption may be excluded from child care or school during a disease outbreak. The length of time a child is excluded from child care or school will vary depending on the type of disease and the circumstances surrounding the outbreak, and could range from several days to over a month. A Certificate of Immunization Exemption for medical reasons is valid only when signed by an Iowa licensed physician, nurse practitioner, or physician assistant.

By signing this certificate, I certify the immunizations specified on this certificate would be injurious to the health of the applicant, to a member of the applicant's family or household or the required vaccine would violate the minimum interval spacing.

Name (Print): ____
Physician (MD or DO), Physician Assistant, or Nurse Practitioner

Iowa License Number: ____
Physician (MD or DO), Physician Assistant, or Nurse Practitioner

Signature: ____ Date: ____________________
Physician (MD or DO), Physician Assistant, or Nurse Practitioner

January 2017

Current Status: *Pending* **PolicyStat ID:** *10512454*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*N/A*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*N/A*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Vulnerability Management

Policy:

The purpose of the Davis County Hospital & Clinics (DCHC) Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them. This is needed in order to protect the confidentiality, integrity and availability of information created, collected and maintained, to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Department of Health and Human Services ("DHHS") security and privacy regulations.

Audience

The Davis County Hospital & Clinics Acceptable Use Policy Vulnerability Management Policy applies to individuals who are responsible for **Information Resource** management.

Contents

Procedure:

Endpoint Protection (Anti-Virus & Malware)

- All DCHC owned and/or managed **Information Resources** must use the DCHC IT management approved endpoint protection software and configuration.
- All non-DCHC owned workstations and laptops must use DCHC IT management approved endpoint protection software and configuration, prior to any connection to a DCHC **Information Resource.**
- The endpoint protection software must not be altered, bypassed, or disabled.
- Each email gateway must utilize DCHC IT management approved email virus protection software and

must adhere to the DCHC rules for the setup and use of this software, which includes, but is not limited to, scanning of all inbound and outbound emails.

- Controls to prevent or detect the use of known or suspected malicious websites must be implemented.
- All files received over networks or from any external storage device must be scanned for malware before use.
- Every virus that is not automatically cleaned by the virus protection software constitutes a potential security incident and should be handled following DCHC Security Incident procedures/playbooks.

Logging & Alerting

- Documented baseline configurations for **Information Resources** must include log settings to record actions that may affect, or are relevant to, information security.
- Event logs must be produced based on the DCHC **Logging Standard** and sent to a central log management solution.
- A review of log files must be conducted periodically.
- All exceptions and anomalies identified during the log file reviews should be documented and reviewed.
- DCHC will use file integrity monitoring or change detection software on critical system logs and critical files to alert personnel to unauthorized modification.
- Log files should be protected from tampering or unauthorized access whenever possible.
- All servers and network equipment must retrieve time information from a single reference time source on a regular basis so that timestamps in logs are consistent.
- All log files should be maintained for a minimum of 90 days wherever possible.

Patch Management

- The DCHC IT team maintains overall responsibility for patch management implementation, operations, and procedures.
- All **Information Resources** must be scanned on a regular basis to identify missing updates.
- All missing software updates must be evaluated according to the risk they pose to DCHC.
- Missing software updates that pose an unacceptable risk to DCHC **Information Resources** must be implemented within a time period that is commensurate with the risk as determined by the DCHC **Vulnerability Management Standard**.
- Major software updates and configuration changes applied to **Information Resources** should be tested prior to widespread implementation whenever feasible and the ability exists to do so.
- Verification of successful software update deployment will be conducted within a reasonable time period as defined in the DCHC **Vulnerability Management Standard**.

Penetration Testing

- **Penetration testing** of the internal network, external network, and applicable hosted applications should be conducted perodically.
- Any exploitable vulnerabilities found during a **penetration test** will be corrected and re-evaluated to verify the vulnerability was corrected.

Vulnerability Scanning

- **Vulnerability scans** of the internal and external network must be conducted at least quarterly or after any significant change to the network.
- Failed **vulnerability scan** results rated at Critical or High will be remediated and re-scanned until all

Critical and High risks are resolved.
- Any evidence of a compromised or exploited **Information Resource** found during **vulnerability scanning** must be reported to the DCHC Information Security Officer and IT support.
- Upon identification of new vulnerability issues, configuration standards will be updated accordingly.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 12, 18
- NIST CSF: PR.IP, PR.PT, DE.AE, DE.CM, RS.MI
- IT Security Incident Response Plan/Procedure
- Logging Standard
- Vulnerability Management Standard

Waivers

Waivers from certain policy provisions may be sought following the Davis County Hospital & Clinics Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Attachments

Vulnerability_Management_Standard.docx
Logging_Standard.docx

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *9795504*

Davis County
HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*08/2020*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*09/2021*
Next Review:	*2 years after approval*
Owner:	*Lynn Fellinger: Public Health Manager*
Policy Area:	*Employee Health*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Employee Health Program

POLICY:

~~DCH~~DCHC will administratively support an effective Employee Health Program. Guidelines and standards from the CDC, the Iowa Department of Public Health, and the Iowa Department of Inspection and Appeals are used for all Employee Health Policies. In those cases in which the standards of the Department of Inspection and Appeals (DIA) are more stringent, DIA standards will be adhered to.

PROCEDURE

~~Annually, the organization will conduct a TB risk assessment to evaluate the risk for transmission of M. Tuberculosis, regardless of whether a person with suspected or confirmed TB disease is expected to be encountered in the facility.~~
~~This assessment shall include:~~

~~A. The community rate of TB~~

~~B. The number of persons with infectious TB encountered in the hospital, and~~

~~C. The speed with which persons with infectious TB disease are suspected, isolated, and evaluated to determine if such persons exposed staff or others in the facility.~~

~~If the hospital has fewer than three TB patients for the preceding year, the hospital shall be classified as low risk, and the TB standards (IAC, Chapter 51.24(3) and Chapter 59) in this policy apply.~~

~~If the hospital has three or more TB patients in a preceding year, the hospital will require annual TB testing of all hospital staff.~~

~~STANDARD OF CARE~~

An effective Employee Health Program will be established and interlinked with Infection Prevention. The Medical Director of Infection Prevention and Employee Health will be an active member~~ of the DCH~~(s) of the DCHC Medical Staff.

DESIGNATED PERSONNEL

All hospital paid employees and hospital-employed medical staff; all contracted employees, volunteers, students, interns, clergy and others who work or serve in all divisions of the hospital operations are covered in this policy. Vaccinations and other employee health services will be recommended and offered to medical staff who are not employees; however, any failure to follow employee health policy by these individuals will be addressed by Administration.

The Employee Health Program will be presented to all new employees~~ during new employee orientation and to all employees during annual in-service education~~.

CONFIDENTIALITY OF EMPLOYEE HEALTH RECORDS

The employee health record is a confidential document, access to which shall be restricted to the employee, the medical director of employee health, infection prevention nurse, and employee health staff members. All employee health personnel are responsible for controlling and enforcing the principle that the information contained in the record is private and confidential. The record is the property of ~~DCH~~DCHC and the original record shall not be removed from ~~DCH~~DCHC except in accordance with a subpoena or a court order.

Separate confidential files for employee health information shall be established and maintained in a locked cabinet in the Employee Health Department, apart from employee personnel files. After termination of employment, employee health files are maintained a minimum of 30 years, per OSHA regulations, in locked storage. The employee may request a copy of any, or all, of their employee health records at any time, during or after their employment. All requests will require a release of information.

EMPLOYEE HEALTH/INFECTION PREVENTION~~/EMPLOYEE SAFETY LINK~~ COORDINATION

Employee Health activity is linked closely to both Infection Prevention and Employee Safety Programs. Employee Health personnel will coordinate with these departments regarding the following issues.

A. The Infection Prevention Coordinator shall promptly report any Employee Health-related infection control concerns to the Employee Health Nurse and vice Versa, as needed.

B. The Infection Prevention Nurse shall share all bloodborne pathogen exposure data and reports with Employee Health as needed.

C. Employee health, Infection Prevention, and safety and workers' compensation personnel will be in close communication concerning:

    1. Regular environmental rounds
    2. Health and safety education
    3. Work injuries
    4. Sharps injuries
    5. Ergonomic issues

D. The Infection Prevention Nurse shall maintain responsibility for Employee Health Surveillance data. Every employee, contracted staff member, or volunteer who reports as unable to attend work as scheduled because of illness shall also report symptoms to supervisor for surveillance tracking. The employee's supervisor will be responsible to ensure that symptoms are presented as part of absence notification. The Infection Prevention Coordinator will have full access to all surveillance data and will share with

PRE-PLACEMENT/ONGOING HEALTH REQUIREMENTS

The following are immunization recommendations. Please note: These recommendations may temporarily change in response to the most recent CDC, IDPH, or hospital/employee health guidelines as necessary to handle outbreaks, epidemics, or other health issues without instigating a change in the formal policy.

DCHC will adhere to the immunization recommendations made by the Centers for Disease Control and Prevention (CDC) and the Advisory Committee on Immunization Practices (ACIP) and adopted by the Iowa Department of Public Health, with one exception. Generally, employee health will not give employees vaccinations during pregnancy. Instead, the employee will be referred to their OB provider to determine if the vaccination should be done while pregnant (by the provider or Employee Health with signed approval from provider), or can be delayed to postpartum. Signed consents to receive the immunizations will signify that information concerning the precautions and contraindications has been received (including the Vaccination Information Sheet (VIS) if appropriate) and that the employee releases DCHC from any liability or claims. When provided by DCHC, vaccines will be administered at no cost to the employee.

In the event of an exposure to any of the diseases for which DCHC recommends immunization,and an employee has signed declination, the non-immune individual may not be allowed to work in the environment. They will not be compensated for their time off (unless they have available PTO) and will not be allowed to return to work until they are cleared by the employee health coordinator, per state and/or federal guidelines.

Employee and ~~DCH~~DCHC-Employed Medical Staff:

Post-offer and prior to beginning employment, the following will be completed at no cost to the employee:

A. Medical history inquiry and physical exam by Employee Health RN or designee.

B. Documentation of immune status of measles (rubeola), mumps, rubella, and varicella by titer, physician documentation of disease, or documented vaccination, "History of disease" will not be accepted if hired after 1/1/2020. If MMR and/or varicella titer is negative the employee will receive two MMR and/or varicella vaccines at least 28 days apart (unless signed declination by employee).

C. New employees will be asked to submit documentation of their tetanus/diptheria/pertussis (Tdap) vaccination status. Those who have not received a Tdap booster within the preceding 5-10 years will be given Tdap vaccine (unless signed declination by employee).

D. New employees will be asked to submit documentation of Hepatitis B vaccine. If no documentation available a series of three Hepatitis B vaccines will be offered free of charge to all personnel. (Unless signed declination by employee).

E. urine drug screen

F. Blood work as required by the employee's health or vaccine history. These may include but not be limited to rubella titer, mumps titer, rubeola titer, varicella titer, hepatitis titer, or other serologic testing in accord with the CDC guidelines at the direction of the Employee Health Nurse or designee.

G. Baseline Tb screening according to Iowa Code Chapter 59, which consists of two components: (1) assessing for current symptoms of active TB disease and (2) testing using the two-step TST procedure or a single IGRA to screen for infection with *M. tuberculosis*

1. *Reactivity to the Tuberculin skin tests may be depressed for 5-7 weeks following administration of live virus vaccines, including MMR and varicella. Therefore, the TB test should be administered before or concurrently with the live vaccine. If not, the TB test should be delayed for 8 weeks to allow for normal reactivity.*
2. A newly hired employee with proof of properly received baseline TB screening at another low risk health care facility does not have to receive serial testing to ~~RB~~TB as long as the employee was continuously employed at that facility up to the time of employment at ~~Davis Co Hospital~~DCHC. Proof of the baseline TB test does have to be provided to ~~Davis Co Hospital~~DCHC (IAC 59.5).

H. Employee will be asked about Latex allergy/sensitivity during Employee Health assessment (this will also be required of all volunteers, students, interns, clergy, or others working in patient care areas)

Prior to reporting to the home department following orientation, all new employees must receive or decline any recommended vaccines or tests (excluding those tests or vaccines that require a time interval prior to full completion). Any other employee health issues must be successfully completed prior to reporting to the home department.

Every four years, per Iowa Administrative Code 51.24 sec 3, every employee will undergo an employee health ~~appraisal~~assessment and immunization review. These exams will be performed by the Employee Health RN or designee. Employees wishing to have their physical performed by their personal physician shall have the hospital approved form completed by the physician and returned to employee health. The employee is responsible for the full cost if going to his/her personal physician for the exam.
~~Employees~~The employee will be ~~given a~~notified by Employee health when health assessment is due. Health assessment needs to be completed within 2 weeks after first notification.If second ~~written~~ notice ~~through their manager if the physical has not been done by the beginning of the month following their birthday month and administration~~is needed this will be ~~notified~~sent to employee and supervisor.

Contracted Employees, Volunteers, Students, and Interns:

A. Contracted employees, in addition to any pre-employment requirements, will be required to have an initial IGRA (Interferon-Gamma Release Assays) Quantiferon Gold TB test and a health ~~maintenance evaluation~~assessment upon entrance to ~~DCH~~DCHC; the health ~~appraisal~~assessment will be repeated every four years thereafter. (IAC 51.24)

B.Volunteers who work in the hospital or healthcare facility in patient care areas on a consistent and regularly scheduled basis for five or more hours per week will complete a health questionnaire and IGRA (Interferon-Gamma Release Assays) Quantiferon Gold TB test upon entrance to program and the questionnaire every 4 years. (IAC 59.2(135C.1) The questionnaires will be reviewed by the Employee Health RN as needed and will be stored in the volunteer health file.
~~College student/volunteers: student volunteer will obtain a copy of their college health records that documents TB status (and BCG vaccination with a negative chest x-ray if applicable). If the student has been out of the country since completing the college health records, an IGRA (Interferon-Gamma Release Assays) Quantiferon Gold TB test will be performed at student cost.~~

C. College student will obtain a copy of their college health records that documents TB status (and BCG vaccination with a negative chest x-ray if applicable). If the student has been out of the country since completing the college health records, an IGRA (Interferon-Gamma Release Assays) Quantiferon Gold TB test will be performed at student cost.

All college students and interns will be required to provide documentation and education as per attached matrix.

~~C~~D. Anyone in section B above who have a positive TB or other health abnormality discovered as part of required ~~DCH~~DCHC testing will be referred back to his/her personal medical provider for follow-up testing or care; entrance into the volunteer program will be deferred until that provider has provided clearance that active disease is not present. ~~DCH~~DCHC will not provide care or reimbursement for such care.

~~D~~E. ~~Unpaid clinical~~Clinical students/interns are covered by the requirements outlined in the legal agreement between their school and ~~DCH~~DCHC. ~~Unpaid medical~~Medical students doing clinical rotations at ~~DCH~~DCHC will be required to show proof of adequate immunizations and TB testing from their school. Clinical students/ interns will be required to provide documentation and education as per attached matrix.

~~E~~F. Failure by those in these categories to complete the required testing or documentation will results in them not being allowed to volunteer or work until the requirements have been completed.

It will be the responsibility of each hospital department manager to notify human resources and employee health, and infection prevention when someone in any of the above mentioned categories is providing services (and the dates of active service) so that appropriate actions can be taken.

Medical Staff and Allied Health Professionals- Non-DCH Employed:
As part of an ongoing communicable disease prevention program, upon initial credentialing the medical staff (excluding telemedicine physicians) will:

A. Provide proof of immunity to Rubella, Mumps, Measles, and Varicella by blood test or vaccination history or sign declination. “History of disease” is not acceptable.

B. Provide proof of Tetanus/diptheria/pertussis (Tdap) vaccination within the past 10 years or sign declination.

C. Provide proof of three doses of Hepatitis B vaccine, positive titer or sign declination.

D. Receive appropriate vaccinations and immunizations (at their expense) if desired.

E. Provide Tb screening according to Iowa Code Chapter 59, which consists of two components: (1) assessing for current symptoms of active TB disease and (2) testing using the two-step TST procedure or a single IGRA to screen for infection with *M. tuberculosis.*

~~Receive latex sensitivity screening as done for regular employees.~~

Upon initial credentialing of a medical staff member, The Medical Staff Services office will document the above. The employee health department will provide vaccinations, administration of vaccinations and other required services to the medical staff and allied health professionals as desired, at staff member's expense. Adherence issues regarding non-compliance with employee health policy will be the responsibility of the Medical Staff Services staff.

~~IMMUNIZATIONS~~

~~DCH will adhere to the immunization recommendations made by the Centers for Disease Control and Prevention (CDC) and the Advisory Committee on Immunization Practices (ACIP) and adopted by the Iowa Department of Public Health, with one exception. Generally, employee health will not give employees vaccinations during pregnancy. Instead, the employee will be referred to their OB provider to determine if the vaccination should be done while pregnant (by the provider or Employee Health with signed approval from provider), or can be delayed to postpartum. Signed consents to receive the immunizations will signify that information concerning the precautions and contraindications has been received (including the Vaccination Information Sheet (VIS) if appropriate) and that the employee releases DCH from any liability or claims. When provided by DCH, vaccines will be administered at no cost to the employee.~~

~~**Declination of vaccine**: Employees and other personnel may refuse immunizations for any reason. Vaccinations that are recommended (as described below), but declined by the employee requires the employee to sign the declination acknowledging that the information described below has been provided, but the employee wishes to decline. If the employee changes his/her mind and wishes to have the vaccine at a later date, it will be provided by DCH at no cost to the employee.~~

~~In the event of an exposure to any of the diseases for which DCH recommends immunization, the non-immune individual may not be allowed to work in the environment. They will not be compensated for their time off (unless they have available PTO) and will not be allowed to return to work until they are cleared by the employee health coordinator, per state and/or federal guidelines.~~

~~RECOMMENDED IMMUNIZATIONS~~

~~The following are immunization recommendations. Please note: These recommendations may temporarily change in response to the most recent CDC, IDPH, or hospital/employee health guidelines as necessary to handle outbreaks, epidemics, or other health issues without instigating a change in the formal policy.~~

~~A. **Rubeola (measles), Mumps, and Rubella (German measles):**~~
~~All employees must provide documentation of immune status to these three diseases. If immunity cannot be proven, DCH will provide serologic testing for evidence of immunity, and if found to be not immune, will provide free vaccination in the form of MMR immunization. The employee must prove immune status documentation (at the pre-employment physical) by:~~

1. ~~Physician diagnosed measles/rubella/mumps written documentation~~
2. ~~Laboratory evidence of immunity~~
3. ~~Documentation of receipt of two live virus MMR vaccinations on or after their first birthday~~
4. ~~Presumptive Immunity according to CDC, born prior to 1957.~~
5. ~~"History of Disease" is not an acceptable form of immunity documentation.~~

~~If the employee cannot prove immunity as stated above, a serologic test will be performed (to determine immunity) for mumps, rubeola, and rubella, prior to being allowed to work in their home department. If the serologic test is negative, vaccine will be provided to employee at no cost.~~

~~A. **Hepatitis B:**~~
~~Persons with known past positive antibody titers are considered immune (protected) and do not need further vaccine or testing. If titer documentation for Hep B is available, it should be provided by the employee at the time of hire. Employees who have anticipated exposure to bloodborne pathogens will be offered the Hepatitis B vaccine (if they have not had the vaccine previously) prior to being allowed to work in their home department. Employees who decline Hep B vaccine will be required to sign a declination. If they decide at a later date, to receive vaccination it will be provided at no charge to the employee. Re-vaccination or the administration of booster doses will be done following a bloodborne exposure if the employee's hepatitis B titer is negative. The regular immunization schedule includes:~~

1. ~~First dose~~
2. ~~Second dose - one month later~~
3. ~~Third dose - 6 months after the first dose~~
4. ~~Late doses will be administered according to CDC recommendations~~

5. ~~Follow-up titers - done 1 - 2 months after completing the vaccine series~~
6. ~~Repeat the vaccine series and follow-up titer testing for persons who did not respond to the first 3-dose series~~
7. ~~Persons not responding to the vaccine series after two rounds are considered vaccine non-responders.~~
8. ~~New employees who have completed the Hepatitis B vaccine series elsewhere and have not received post-vaccine titer testing may be offered serologic testing to verify vaccine effectiveness given the following considerations:~~
    a. ~~if the vaccine series has been completed within the past 6 months, testing will be performed.~~
    b. ~~if the vaccine series has been completed at least 6 months from the time of employment, no serology will be drawn to avoid possible confusion from "false" negative results.~~

B. ~~**Influenza:**~~

~~Flu vaccine will be offered to all employees each fall. It is ***mandated*** that all employees, contracted staff, and medical providers receive the influenza vaccine each year so that the hospital can maintain personnel to care for patients during the peak of the flu season and prevent the spread of flu. In the event the CDC/IDPH states that influenza is "widespread" in Iowa, those unable to be vaccinated will be required to be evaluated prior to each shift in the ER to see if fever, cough or sore throat are present. This will be tracked on a log sheet by ER staff. Employees screening positive for temp of 100.4 degrees F or higher and/or sore throat or cough will be sent to Lab for flu testing, and ER staff will notify House Supervisor and Employee Health. Any staff with a positive flu test will not be allowed to work until symptoms, including fever, have been resolved at least 24 hours (without the use of fever-reducing medication). Generally, 7 days from onset of symptoms will be considered the minimum time period for reduction of infectivity to allow return to work. Relief of symptoms will drive the ability to return to work, regardless of Tamiflu use.~~

1. ~~All employees, contracted staff, and medical providers, including new hires, will be given the influenza vaccine annually in the fall 1) until March 31st or 2) until the supply is depleted and no more can be obtained for that season or 3) after March 31st if influenza activity remains rated as "widespread" by the Iowa Department of Public Health.~~

C. ~~**Varicella [chickenpox] / Herpes Zoster [shingles]:**~~

~~All employees must provide documentation of immune status to chickenpox. If immunity cannot be proven, DCH will provide free serologic test and/or vaccination in the form of a varicella vaccination. The employee must prove immune status documentation (at the pre-employment physical) by:~~

1. ~~History of chickenpox disease (physician documented)~~
2. ~~Laboratory (serological) evidence of immunity~~
3. ~~Documentation of receipt of varicella vaccination as age-appropriate~~
4. ~~"History of disease" is not an acceptable form of immunity documentation.~~
5. ~~If the employee cannot prove immunity as stated above, a serologic test must be performed (to determine immunity) for chickenpox prior to being allowed to work in their home department. If the serologic test is negative, vaccine will be provided to employee at no cost.Vaccination of all non-immune employees will be strongly encouraged, or a form will be signed declining the vaccine. If they decide at a later date, to receive vaccination it will be provided at no cost to the employee.~~
6. ~~**IMPORTANT NOTE:** Per the Varicella, package insert, transmission of vaccine virus may occur~~

~~rarely between healthy vaccinees who develop a chickenpox-like rash and healthy susceptible contacts. Transmission of vaccine virus from vaccinees without a chickenpox-like rash has been reported but has not been confirmed.~~ ~~***Therefore, vaccine recipients should avoid, whenever possible, close association with susceptible high-risk individuals for up to six weeks including immunocompromised individuals, pregnant women without documented history of chickenpox or laboratory evidence of prior infection, and newborn infants of mothers without documented history of chickenpox or laboratory evidence of prior infection, unless protected by personal protective equipment such as mask (or gown, if rash presents).***~~

~~D.~~ ~~**Tdap (tetanus, diphtheria, and acellular pertussis):**~~

~~1.~~ ~~New employees will be asked to submit documentation of their tetanus/diphtheria/pertussis vaccination status. Those who haven't received a diphtheria/tetanus booster in the past 10 years will be given a tetanus, diphtheria and pertussis booster (Tdap). Exceptions will be to those allergic to any of the components. Pregnant employees will be deferred until after pregnancy if recommended by their OB medical provider.~~

~~2.~~ ~~IMPORTANT NOTE: Serology for diagnostic testing for pertussis is unpredictable in people who have had Tdap vaccine within the previous 3 years "leaving no reliable method for making the diagnosis in vaccinated individuals who present late in the course of their illness". (Clin. Microbiol. Rev. July 2008 vol. 21 no. 3 426-434)~~

~~E.~~ ~~Periodically, the state or federal health programs (i.e., the Iowa Department of Public Health, the Centers for Disease Control, et cetera) may recommend other testing or vaccination as appropriate for outbreaks or epidemics or may recommend variance from the above standards. In all cases, current recommendations will take precedence over established policy.~~

TESTING FOR TUBERCULOSIS

~~Baseline Tb testing (according to Iowa Code Chapter 59) will be required on all new employees, contracted staff, medical providers, volunteers, and clergy will provide documentation of or receive TB testing upon employment or commencement of DCH activity:~~

~~A.~~ ~~Assessing for current symptoms of active TB diseases and,~~

~~B.~~ ~~Testing using the 2step TST procedure or a single IGRA to screen for infection with *M. tuberculosis.*~~

Screening of HCWs who transfer to other health care facilities or hospitals. (Iowa Code 59.7)

HCWs transferring from a low-risk health care facility or hospital to another low-risk health care facility or hospital. HCWs with documentation of baseline TB screening who are transferring from a low-risk health care facility or hospital to another low-risk health care facility or hospital do not need to repeat baseline TB screening if the time frame between employment from one facility or hospital to another does not exceed 90 days. If the time frame between employment from one facility or hospital to another exceeds 90 days, baseline TB screening shall be restarted for a HCW with a previous negative test result and a TB symptom screen shall be performed for a HCW with a previous positive TB test result in accordance with Iowa Code 59.5(5)

If the IGRA (Interferon-Gamma Release Assay) Quantiferon Gold test is positive, documentation of a Chest X-Ray (CXR) is necessary to rule out active disease. If no previous documentation is available, a CXR will be ordered at no charge to the employee. For volunteers, any testing beyond the positive TB (IGRA) test will be referred back to the personal medical provider for counseling and clearance into the volunteer program at the volunteer's expense.

For employees who are determined to be positive for latent TB from a documented DCH exposure, the employee will be referred to the Employee Health Coordinator for determination of appropriate treatment. Those employees determined to be positive for latent TB without DCH exposure will be referred back to his/her personal medical provider for treatment. The employee may continue to work with latent TB regardless of whether he/she chooses to medically treat the dormant disease. Counseling will be given (and documented in the employee health file) of the potential for conversion to active disease.

Previous BCG vaccination is not a contraindication to having an IGRA,~~ a TST~~ or a two-step skin testing administered. Health Care Workers with previous BCG vaccination should receive baseline and serial testing in the same manner as those without ~~BCH~~BCG vaccination. (Iowa Code 59.5(6)

Follow-up TB testing will be indicated if an employee experiences unprotected respiratory exposure to a patient with active tuberculosis.

~~PREGNANT HEALTHCARE WORKERS~~

~~Employees who are pregnant will not care for patients with the following communicable diseases:~~

~~A. Chickenpox [Varicella] / Shingles [Herpes Zoster]:~~
~~Pregnant employees who have negative immune status for varicella~~

~~B. Fifth's Disease / Parvovirus B 19: all pregnant employees~~

~~There are no other communicable diseases that pose any special hazard to pregnant healthcare workers when Standard Precautions are observed.~~

~~COMMUNICABLE DISEASE EXPOSURE~~

~~Employees must comply with Employee Health and Infection Prevention communicable disease policies to minimize the possibility of transmission of infection among staff and patients. Employees who are exposed to a communicable disease while on duty are offered appropriate prophylaxis and/or screening for susceptibility to the disease and must file an employee incident report. Employees who have been exposed to a non-work related communicable disease should contact Employee Health and Human Resources and the department manager to arrange any required time off from work.~~

~~Employees who may have or who have been exposed to any of the following diseases will be provided with information as described below. Department managers are encouraged to watch for signs of illness in their employees and their ability to perform their duties if there are symptoms of illness. If there is any question about an employee being fit for work due to communicable disease, the department manager should contact the Employee Health Coordinator. It will be the duty of the Employee Health Coordinator to evaluate the employee for the suspected communicable disease, in a confidential manner.~~

~~In all cases, the provider release shall take precedence over the recommended length of exclusions specified below. This may be shorter or longer than recommended, but is most appropriate on a case by case basis.~~ **~~(or according to any governors proclamation in effect at the time)~~**

~~Please note: This information may temporarily change in response to the most recent CDC, IDPH, or hospital/employee health guidelines as necessary to handle outbreaks, epidemics, or other health issues without instigating a change in the formal policy. Lost work time for work-related exposure to disease or illness will be handled per DCH's Workers' Compensation policy.~~

~~A. Chickenpox (Varicella)~~

   1. ~~Immune persons have no work restrictions.~~
   2. ~~Non-immune persons will remain off work from day 10 from the start of the exposure through day 21 from end of the exposure.~~
   3. ~~Any lesions must be dry and crusted before return to work.~~
   4. ~~Non-immune employees will be encouraged to be vaccinated and will be counseled regarding post-vaccination concerns.~~

B. ~~**Conjunctivitis**~~
~~The employee with conjunctivitis will be removed from work until the discharge ceases. Diligent handwashing will be encouraged.~~

C. ~~**Gastroenteritis**~~
   1. ~~Employee with abdominal cramping and/or diarrhea will not work until 24 hours after symptoms resolve.~~
   2. ~~The employee with *Salmonella* positive stool culture will not work until 24 hours after diarrhea is resolved.~~
   3. ~~The employee with *Shigella* positive stool culture will not be cleared to return to work until they submit two (2) negative stool cultures taken at least 24 hours apart that are collected at least 48 hours after finishing antibiotic therapy.~~
   4. ~~The employee with *Campylobacter, Giardia*, or other known stool pathogen-based infections shall not work until symptoms have resolved at least 24 hours.~~
   5. ~~The employee with *Clostridium difficile (C. diff)* positive stool culture will not work until 48 hours after diarrhea is resolved.~~

D. ~~**Hand, Foot, &amp; Mouth Disease (Coxsackie)**The employee will not work while symptomatic with a fever, sore throat, malaise, and/or rash or lesions present on hands. Employee may be contagious for weeks, even if symptom free; therefore, diligent hand washing is required (be cognizant of family members with the virus).~~

E. ~~**Hepatitis A**~~
   1. ~~Infected employee: No work starting when symptoms are evident until 7 days after the onset of jaundice. Employee must be cleared by Provider and HR prior to returning to work.~~
   2. ~~Exposed employee: Immune Globulin will be offered to employee who ate food prepared by the source person within the past 2 weeks.~~
   3. ~~No special post-exposure measures are indicated following a blood borne pathogen exposure involving a patient with Hepatitis A.~~

F. ~~**Hepatitis B**~~
   1. ~~Employee HBsAg Positive~~
   2. ~~Will be removed from direct patient care until the acute illness resolves~~
   3. ~~May return to work when cleared through their Provider and HR.~~
   4. ~~Employee with chronic illness will be specially counseled about the importance of Standard Precautions but will not normally have any work restrictions put in effect.~~
   5. ~~Treatment following a bloodborne pathogen exposure depends on patient infectivity and the employee's Hepatitis B immunization record.~~

~~6. *Patient infective / non-vaccinated employee:* For the non-vaccinated employee (0-1 doses of Hepatitis B vaccine received), Hepatitis B Immunoglobulin (HBIG) is administered within 7 days (ideally within 24 hours) of exposure. To prevent further risk, Hepatitis B vaccination should begin at the same time unless the health care worker refuses. If vaccination is refused, a second dose of HBIG must be given in 30 days.~~

~~7. *Patient infective / employee has had at least 2 doses of vaccine:* The HBsAb status of the employee should be determined as soon as possible. If positive, no prophylaxis is indicated. If negative, one dose of HBIG should be given as above, and vaccination should proceed on schedule. If the vaccination series has already been completed, but HBsAb is negative, then one more vaccine dose is administered along with one dose of HBIG.~~

~~8. *Patient not infective:* No prophylaxis is needed. The employee is urged to obtain Hepatitis B vaccination if not already immunized.~~

~~9. *Unable to determine patient infectivity:* The only recommended treatment is to ensure that the employee has received the Hepatitis B vaccination series. In some cases, the employee may be treated as if the source did have positive HBsAg, at the discretion of the Employee Health Coordinator, or designee, or Primary Care Provider.~~

~~G. **Hepatitis C**~~

~~1. Antibody testing shall be performed following blood borne pathogen exposure event as follows:~~

~~a. The source patient is tested as soon as possible, in conjunction with other serological testing performed.~~

~~b. The exposed healthcare worker is tested at baseline and at 6 months (follow-up) if the source patient was HCV positive or the source was unknown, along with other serological testing being performed at those times.~~

~~2. No evidence for use of immune globulin post-exposure~~

~~3. No reliably effective preventive treatment for hepatitis C is known.~~

~~H. **Hepatitis D**~~
~~Follow Hepatitis B protocol.~~

~~I. **Hepatitis E**~~
~~No prophylaxis procedure indicated.~~

~~J. **Herpes Simplex (oral or genital)**~~

~~1. Contact should be avoided with neonates, obstetrical patients, burn patients, and immunosuppressed patients.~~

~~2. No work restrictions but increased diligence with handwashing.~~

~~K. **Herpetic Whitlow**~~

~~1. Defined as single or multiple lesions on the distal parts of fingers caused by Herpes Simplex Virus I/ II.~~

~~2. Personnel will be excluded from any patient care until lesions are dried and crusted.~~

~~L. **Influenza**~~

~~1. Employees with confirmed or probable influenza shall not work until symptoms, including fever, have been resolved at least 24 hours (without the use of fever-reducing medication). Generally, 7 days~~

~~from onset of symptoms will be considered the minimum time period for reduction of infectivity to allow return to work. Relief of symptoms will drive the ability to return to work, regardless of Tamiflu use.~~

2. ~~In the event that a novel strain of influenza is circulating (pandemic, avian, etc.), Employee Health reserves the right to modify work exclusion criteria, based on guidance from the CDC and IDPH.~~

~~M.~~ **~~Lice (Pediculosis)~~**

1. ~~Employees will avoid unprotected contact with infected patient and belongings until 24 hours after application of insecticide (see Infection Prevention Manual for specific Precautions needed).~~
2. ~~Exposed employee: no work restrictions~~
3. ~~Infected employee: will notify Employee Health and Infection Prevention to consider outbreak evaluation.~~
4. ~~Infected employee will be placed on immediate work restrictions until 24 hours post-treatment with an effective insecticide.~~

~~N.~~ **~~Measles (Rubeola)~~**

1. ~~Infected employee: immediate work restrictions until seven (7) days after rash appears~~
2. ~~Exposed employee: determine immune status.~~
   - ~~a. if immune, no further action needed.~~
   - ~~b. if cannot prove immunity, MMR may provide protection if administered within 72 hours after initial exposure if employee not pregnant and not considering becoming pregnant within the next 3 months.~~
   - ~~c. If nonimmune, MMR is contraindicated or given after 72 hours following exposure, work restrictions will begin day 5 through day 21 after exposure.~~
   - ~~d. Immune employee will be asked to monitor temperature day 5 through day 21 after exposure. During this time, the employee will be assigned to care only for persons considered immune.~~
   - ~~e. Work restrictions will be enforced if employee develops coryzal (profuse runny nose) symptoms or temperature elevation.~~

~~O.~~ **~~Meningococcal Disease~~**

1. ~~Employees in "close contact" with patient secretions (nasal or oral) will be offered prophylaxis according to CDC recommendations.~~
2. ~~Medication distribution will not await laboratory confirmation or sensitivity results.~~
3. ~~Staff offered prophylaxis (close contacts) will:~~
   - ~~a. record temperature twice daily for 5 days.~~
   - ~~b. report fever (greater than 100°F), other signs and symptoms.~~
4. ~~Antimicrobial prophylaxis is not indicated for employees who did not have "close contact" with the patient.~~
5. ~~Contacts will be determined by the infection prevention coordinator.~~
6. ~~Employees who meet the close contact criteria must file an employee incident report.~~

~~P.~~ **~~Multiple drug resistant organism infections (e.g., MRSA, VRE)~~**

~~1. Cultures may be obtained if indicated.~~

~~2. If employee infection is identified:~~

~~a. immediately remove employee from patient care activities.~~

~~b. refer to physician for appropriate treatment~~

~~c. allow employee to return to work if infective wound drainage can be contained.~~

~~d. notify infection prevention for surveillance of patients.~~

~~e. culture anterior nares and perineum to detect carrier states, if appropriate, at discretion with the Infection Prevention Nurse.~~

~~Q. **Mumps**~~

~~1. Infected employee will be removed from duty until 9 days after onset of symptoms.~~

~~2. Exposed employee:~~

~~a. no action needed if the employee is known or shown to be immune.~~

~~b. if the employee has no documented immunity:~~

~~i. Order IgG titer~~

~~ii. If titer negative, remove employee from direct patient care day 11 through day 26 after exposure.~~

~~iii. Offer MMR vaccine according to vaccine contraindications~~

~~iv. MMR after exposure may not provide protection against that exposure.~~

~~R. **Norovirus**~~

~~1. Exposed employee to diagnosed Norovirus outbreak:~~

~~a. employee will wear gloves when performing ALL patient care activities until the incubation period has passed (48 hours) and will not bring food products to work that are intended to be shared with others.~~

~~2. The employee with diagnosed Norovirus will not be allowed to return to work until vomiting and/or diarrhea have resolved for 48 hours~~

~~S. **Pertussis**~~

~~1. Post-exposure--asymptomatic employee requires no restrictions~~

~~2. Post-exposure symptomatic employee will not work from beginning of the catarrhal (symptomatic) stage through the 3rd week after onset of paroxysms or until 5 full days after start of appropriate antibiotics.~~

~~T. **Rubella (German Measles)**~~

~~1. Infected employee: will be removed from duty from the onset of symptoms until 7 days after the rash appears~~

~~2. Exposed employee:~~

~~a. no action needed if the employee is known or shown to be immune.~~

~~b. if the employee has no documented immunity:~~

~~i. a rubella titer will be obtained~~

ii. ~~if the titer is negative, MMR will be given if employee is not pregnant or considering becoming pregnant in the next 3 months.~~

iii. ~~remove from duty from day 7 through day 21 after exposure since MMR after exposure does NOT provide protection against that exposure.~~

U. ~~**Scabies**~~

1. ~~Employees will avoid unprotected contact with infected patient and belongings until 24 hours after application of insecticide. (See Infection Prevention Manual for specific Precautions needed).~~
2. ~~Exposed employee: no work restriction~~
3. ~~Infected employee: must notify Employee Health (who will notify Infection Prevention to consider outbreak evaluation)~~
4. ~~Infected employee will be placed on immediate work restriction until 24 hours post-treatment with an effective insecticide.~~
5. ~~Ineffective treatments or re-infestations must be reported to Employee Health. These circumstances may warrant further work restrictions.~~

V. ~~**Shingles (Herpes Zoster)**~~

1. ~~Employee may work if body lesions are covered.~~
2. ~~Contact should be avoided with neonates, obstetrical patients, burn patients, and immunosuppressed patients.~~
3. ~~Employee must increase diligence with handwashing.~~

W. ~~**Streptococcal (Group A) Respiratory Infections**~~

1. ~~The employee will be restricted from work until 24 hours after effective antibiotic treatment has been started.~~

X. ~~**Tuberculosis**~~

~~Follow-up of exposures to a patient with untreated tuberculosis (e.g., who is not in isolation), is based on the infectivity of the patient and the length of employee exposure. Since organisms must be inhaled for initial infection to occur, the person with active disease must be disseminating live tubercle bacilli via the respiratory tract. In the event of a probable exposure, personnel who have cared for the patient directly should be monitored.~~

1. ~~Baseline testing of previously negative but newly exposed employees should be by TST or IGRA within one to two weeks after the exposure (unless previous testing was done within the past 3 months) and again in 8-10 weeks.~~
2. ~~Exposed employees who are prior reactors will be monitored by chest x-rays and examination as needed.~~
3. ~~Specific therapies will be ordered by the designated physician, based on CDC recommendations through the Iowa Department of Public Health.~~

~~SYMPTOMS OF~~ ILLNESS

~~All employees shall be free of the following symptoms (without or precluding diagnosis) for the designated time periods before returning to work:~~

A. ~~Vomiting without diarrhea– at least 24 hours without vomiting or nausea (following return to normal diet).~~

~~B. Diarrhea without vomiting – at least 24 hours of normal stool (following return to normal diet and without anti-diarrheal medication).~~

~~C. Both vomiting and diarrhea – without all symptoms 24 hours following return to normal diet.~~

~~D. If vomiting or diarrhea occurs for non-infectious reasons (i.e., pregnancy, Crohn's disease, etc), physician must document ability to work with these symptoms.~~

~~E. Jaundice (yellow skin or eyes) – at least 7 days from onset of jaundice, with physician documentation of non-infectious condition.~~

~~F. Sore Throat with fever – until employee has been on antibiotics for at least 24 hours or is no longer infectious.~~

~~G. Fever > 100 °F until fever-free (without fever-reducing medication) at least 24 hours.~~

~~H. Lesions with pus unless wound can be covered with impervious bandage.~~

~~I. Symptoms of upper respiratory illness (URI) (cough, head congestion, etc., WITHOUT fever) may NOT provide care to neonates, pediatric patients, COPD, or immunocompromised patients. Those employees with severe URI symptoms should preclude themselves from work until symptoms resolve.~~

~~Any employee who is ill more than three (3) consecutive calendar days must have Return to Work clearance from a medical provider before reporting for duty. For instance, if the employee is absent (ill) on Friday, not scheduled to work Saturday and Sunday, and reports ill on Monday, he/she will need a Return to Work clearance. Note: if the symptoms reported require a post-symptom waiting period before return to work (i.e., fever, vomiting, diarrhea), the post-symptom waiting period will not apply towards the requirement for a Return to Work Clearance or an FMLA. Human Resources should be consulted by the dept for all absences greater than 3 days~~

~~BLOODBORNE PATHOGEN EXPOSURE~~

~~For Employee~~

~~A. After any parenteral (e.g., needlestick, cut, bite) or mucous membrane or non-intact skin exposure (e.g., splash to eye, nare, or mouth) to any blood or OPIM (other potentially infectious materials), the site will be thoroughly washed (eyes copiously flushed at eye wash station) as soon as possible.~~

~~B. Employee will report incident to his/her supervisor.~~

~~C. Report to Employee Health or ER~~

~~D. An employee incident report will be completed.~~

~~Employee Health Coordinator (or designee) will:~~

~~A. Obtain a brief history concerning the circumstances of the exposure~~

~~B. Complete counseling concerning risk of infectivity, with respect to donating blood, sexual activity, and IV drug use~~

~~C. Appropriate consent forms will be signed prior to drawing blood for HIV antibody baseline.~~

~~D. If the known source person is HIV positive or the source is unknown, repeat blood testing for HIV antibody will be ordered at 6 weeks, 3 months, and 6 months.~~

~~E. If the known source person tests negative for bloodborne pathogens, no further follow-up or testing is required of the exposed employee.~~

~~F. Upon completion of the testing, the information will be sealed and placed in the employee's health file.~~

~~G. Refer to "Exposure Control Plan" in the Infection Prevention Manual for further details.~~

~~For Source Patient:~~

~~A. If the known source patient's blood is negative for HIV, HBV, and HCB, no baseline or further testing of the exposed employee is required~~

~~B. Employee Health or Infection Control nurse will arrange for testing of the source patient.~~

~~C. In the event the source is known to be positive for HIV or strongly believed to be HIV infected but unable or unwilling to confirm HIV infection, the employee will be immediately referred for care as described in the Post-Exposure Prophylaxis against HIV policy attached below.~~

~~D. When indicated, anti-retroviral chemoprophylaxis will be started in accord with the Post-Exposure Prophylaxis against HIV policy attached below.~~

~~E. If source patient has a positive antibody test for HCB, a confirmatory RNA test will be performed to determine if active virus is present in the blood.~~

~~According to the CDC MMWR 2001 report, source patients are tested for HIV, Hepatitis B and C in accordance with applicable state and local laws. Iowa Code 141A.8- "Care Provider Notifications", #7- states that the individual (eg. source patient) to whom the care provider (eg. employee) was exposed is deemed to consent to a test (HIV) upon the written request to be treated by the exposed care provider. Therefore, source patients cannot refuse testing.~~

~~Post-Exposure Prophylaxis Against HIV~~

~~See the Bloodborne Pathogens Exposure Control Plan policy for further details.~~

if employee has any signs/symptoms of illness ie; vomiting, diarrhea, sore throat, fever, cough, etc., that is not covered under a current FMLA leave, should not report to work but report to their supervisor for further instruction. The employee must be free of fever (without use of fever reducing medication), diarrhea, and vomiting for 24 hours before returning to work. Any employee who is ill for three or more consecutive scheduled working days, or if the employee has been taken off work by a provider, they must have a release to return to work. Refer to HR Return to Work Policy.

INJURY/ILLNESS ON THE JOB

Please refer to the Worker's Compensation Program policy for the correct procedures to obtain appropriate care and follow-up after a work-related injury or illness.

LATEX SENSITIVITY/ALLERGY MANAGEMENT

A. Any problems with or reactions to latex containing products will be noted on the health file and appropriate precautionary actions taken to assure the worker's safety as described in B, below.

B. Healthcare Worker Management Protocol: The Employee Health Coordinator will:

1. Obtain and document a careful allergy history
2. Conduct an environment survey
3. Refer to an allergist to confirm diagnosis, where needed
4. Provide safe alternatives to latex products, as needed

5. Evaluate the need for temporary or permanent work restrictions in consultation with the employee's department manager & Human Resources.

EMPLOYEE HEALTH AUTHORITY STATMENT

A. The Employee Health Staff, under the direction of the Medical Director of Employee Health, may administer vaccines and TST, order titers and IGRA testing as needed in accord with the Employee Health Policy. Guidelines and standards from the CDC, the Iowa Food Code, and the Iowa Dept. of Public Health are used for all Employee Health Policies.

B. The Employee Health Staff may, under direction of the Medical Director of Employee Health, order serological, microbiological, or other clinical testing as required by Employee Health Policy and as needed to manage staff exposures, outbreaks, etc.

C. The Employee Health Staff, under the direction of the Medical Director of Employee Health, may cause an employee to be furloughed from work for the purposes of prevention of spread of disease or to promote the recovery from any illness or injury as needed.

D. The Employee Health Staff, under the direction of the Medical Director of Employee Health, may cause an employee to be examined to be "fit for duty" by a physician during an illness in which an employee wishes to remain at work or following return to work from an illness of any type.

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
CAH	Kayla Miller: Quality Director	pending
Medical Director	Dr. Ron Graeff: Provider	09/2021
Senior Leader	Nikki Thordarson: Education/Infection Prevention/Wellness	09/2021
	Lynn Fellinger: Public Health Manager	09/2021

Applicability

Davis County Hospital

Current Status: *Pending*	**PolicyStat ID:** *10536840*
Origination:	*05/1991*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Nikki Thordarson: CNO*
Policy Area:	*Infection Prevention*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Antibiotic Guidelines

Policy Number: IC 02.01

POLICY:

The infection prevention coordinator in coordination with pharmacist shall monitor the use of antibiotics as to appropriateness for diagnosis, dosage, and cultures obtained.

PROCEDURE:

1. The staff will treat infections in an appropriate manner, using the laboratory, x-ray and clinical findings.
2. The medical provider should use his/her clinical and physical acumen to ascertain and plan the most effective course of therapy for each individual patient. Cultures should be taken before starting antibiotic if possible and the antibiotic should be changed according to the sensitivity pattern and the clinical picture.
3. Prophylactic therapy is to be the responsibility of the medical provider in charge of the patient. This should be in accordance with the accepted medical and surgical treatment of the patient. Prophylactic antibiotics should be administered prior to the skin incision within one (1) hour prior to surgery.
4. If there is evidence of inappropriate antibiotic usage, as noted by medical provider, nurse or pharmacist, this should be reported to the ~~infection prevention coordinator to investigate and report on to the hospital epidemiologist~~quality director for additional follow-up as needed.

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Senior Team Leader	Nikki Thordarson: CNO	pending
	Nikki Thordarson: CNO	10/2021

Applicability

Davis County Hospital

Draft saved by Thordarson, Nikki: CNO 10/7/2021, 12:35PM EDT

Edited by Thordarson, Nikki: CNO 10/7/2021, 12:35PM EDT

Added pharmacist to policy statement

Last Approved by Thordarson, Nikki: CNO 10/7/2021, 12:35PM EDT

Draft saved by Thordarson, Nikki: CNO 10/7/2021, 6:24PM EDT

Edited by Thordarson, Nikki: CNO 10/7/2021, 6:24PM EDT

fixed typo in policy statement

Last Approved by Thordarson, Nikki: CNO 10/7/2021, 6:24PM EDT

Current Status: *Pending* **PolicyStat ID:** *10512368*

Davis County
HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*03/2018*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Asset Decommission Procedure

Purpose:

To detail a practical decommission process for ~~DCH~~DCHC owned information resources, including but not limited to: desktops/laptops/servers/MFPs. Any item that could contain ePHI is subject to the asset decommission procedure.

Procedure:

1. Open the asset in consolidated asset tracking spreadsheet, and move the entire asset row to the decommissioned asset tab. Indicate the date the asset was retired/decommissioned in this row.
2. Remove the computer from Active Directory
3. Remote the computer from Cisco AMP
4. Remove the computer from ManageEngine Desktop Central/Spiceworks Inventory if needed
5. Remove/retain hard drive for a minimum of two weeks standard user pc and per case as needed for executives, physicians, department managers and place into the holding bin in TR4 to await final disposition/destruction. (Mark physical drive with asset name using painters tape or Sharpie)
6. Place piece of painter's tape on asset to indicate that the drive has been pulled and date/initial on tape
7. Check any removable media bays, e.g., optical drive for physical media.
8. After above retention period has passed, utilize contracted on-site data destruction to permanently destroy media and keep certificate of destruction. Store certificates in ITS drive electronically.
9. If device has internal storage such as MFP, retain drive before leased or other equip is returned or destroyed.
10. Recycle physical asset hardware as appropriate

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Senior Leader	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending*	**PolicyStat ID:** *10512361*

Origination:	*03/2018*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Asset Management Policy

Policy:

The purpose of the Davis County Hospital & Clinics Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by Davis County Hospital & Clinics in order to protect the confidentiality, integrity and availability of information created, collected and maintained, to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Department of Health and Human Services ("DHHS") security and privacy regulations.

Audience

The Davis County Hospital & Clinics Asset Management Policy applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of Davis County Hospital & Clinics Information Resources

Contents

Procedure:

Hardware, Software, Applications and Data

- All hardware, software and applications must be approved and purchased by Davis County Hospital & Clinics IT.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved Davis County Hospital & Clinics procedures and change control processes.
- Software used by Davis County Hospital & Clinics employees, contractors and/or other approved third-parties working on behalf of Davis County Hospital & Clinics, must be properly licensed.
- Software installed on Davis County Hospital & Clinics computing equipment, outside of that noted in the

Davis County Hospital & Clinics Standard Software List, must be approved by IT Management and installed by Davis County Hospital & Clinics IT personnel.

- Only authorized **cloud computing applications** may be used for sharing, storing and transferring **confidential** or **internal information**.
- The use of **cloud computing applications** must be done in compliance with all laws and regulations concerning the information involved, e.g. personally identifiable information (PII), protected health information (PHI), corporate financial data, etc.
- Two-factor authentication is recommended for external **cloud computing applications** with access to any **confidential information** for which Davis County Hospital & Clinics has a custodial responsibility.
- Contracts with **cloud computing applications** providers must address data retention, destruction, data ownership and data custodian rights.
- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- All Davis County Hospital & Clinics assets must be formally classified with ownership assigned.
- All Davis County Hospital & Clinics physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by Davis County Hospital & Clinics.
- Confidential information must be transported either by an Davis County Hospital & Clinics employee or a courier approved by IT Management.
- Upon termination of employment, contract or agreement, all Davis County Hospital & Clinics assets must be returned to Davis County Hospital & Clinics IT Management.

Mobile Devices

- The use of a personally-owned mobile device to connect to the Davis County Hospital & Clinics network is a privilege granted to employees only upon formal approval of IT Management.
- Mobile devices used to connect to the Davis County Hospital & Clinics network are required to use the approved mobile device management (MDM) solution.
- Mobile devices that access Davis County Hospital & Clinics email must have a PIN or other authentication mechanism enabled.
- Confidential data should only be stored on devices that are encrypted in compliance with the Davis County Hospital & Clinics Encryption Standard.
- All mobile devices must maintain up-to-date versions of all software and applications.

Media Destruction & Re-Use

- Media that may contain **confidential** or **internal information** must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- Media reuse and destruction practices must be conducted in compliance with Davis County Hospital & Clinics's **Asset Decommission Procedure**.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information that cannot be encrypted and/or wiped through means of approved methods of data destruction must be physically destroyed when no longer needed.
- Any contractors providing media services shall provide a certificate of destruction for each media destroyed containing **confidential information**.

Backup

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The Davis County Hospital & Clinics backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for Davis County Hospital & Clinics must be formally approved to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest Davis County Hospital & Clinics sensitivity level of information stored.
- A process must be implemented to verify the success of the Davis County Hospital & Clinics electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Backups containing **confidential information** must be encrypted.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
  - System name
  - Creation Date
  - Sensitivity Classification
  - Davis County Hospital & Clinics Contact Information

Removable Media

- The use of **removable media** for storage of Davis County Hospital & Clinics Information must be supported by a reasonable business case.
- All **removable media** use must be approved by Davis County Hospital & Clinics IT prior to use.
- **Personally-owned removable media** use is not permitted for storage of Davis County Hospital & Clinics information.
- Users are not permitted to connect **removable media** from an unknown origin, without prior approval from Davis County Hospital & Clinics IT.
- Confidential and internal Davis County Hospital & Clinics information should not be stored on **removable media** without the use of encryption.
- The loss or theft of a **removable media** device that may have contained Davis County Hospital & Clinics information must be reported to the Davis County Hospital & Clinics IT.
- The transfer of information to removable media will be monitored.

Definitions

- See Appendix A: Definitions

References

- ISO 27002: 6, 8, 11, 12, 16, 18
- NIST CSF: ID.AM, PR.IP, PR.DS, PR.PT, DE.CM
- Davis County Hospital & Clinics Information Classification and Handling Policy

- Davis County Hospital & Clinics Encryption Policy

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Attachments

Appendix_A_Definitions.pdf

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending*	PolicyStat ID: *10512370*
Origination:	03/2018
Effective:	Upon Approval
Last Approved:	N/A
Last Revised:	10/2021
Next Review:	2 years after approval
Owner:	Chris Hickie: Information Technology
Policy Area:	Information Technology
Standards & Regulations:	
References:	
Applicability:	Davis County Hospital

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Authentication Standard Procedure

Purpose:

The purpose of this Authentication Standard Procedure is to provide practical guidance on configuring, deploying, and managing passwords on Davis County Hospital & Clinics systems to ensure all activity on Davis County Hospital & Clinics Information Resources can be tied to unique users and to minimize the risk of unauthorized access to Davis County Hospital & Clinics Information Resources.

Audience

The Davis County Hospital & Clinics Authentication Standard Procedure document applies to all Information Technology staff who set up and manage Davis County Hospital & Clinics Information Resources.

Roles and Responsibilities

Director of IT:

- Approve or Deny changes to password configurations.
- Review the Authentication Standard Procedure annually and update as needed.

IT Support:

- Configure systems and applications to comply with the Authentication Standard Procedure.
- Review all password configurations at least annually.
- Assist users with adherence to the documented requirements, as needed.

Procedure:

General Requirements

- Authentication mechanisms must be assigned to an individual.
- Authentication data should not be stored after authorization (even if encrypted).
- In the event that a user's authentication is compromised or discovered, it must be immediately changed.

- Automatic log off and/or lock system settings should be employed on all devices:
    - Workstations are set to lock after 5 minutes of inactivity.
- Default system accounts must be changed immediately to a unique password.
- Vendor-supplied passwords must be changed before connecting to the network or as soon as practical after initial connection.

Password Configuration

- The password must be communicated separately from the User ID.
- Initial set-up passwords must follow the configuration requirements based on the type of account and must be unique for every new account set-up.
- Initial set-up passwords must force a password change upon initial log-on.
- Passwords should not be displayed when entered.
- Passwords must be saved as one-way hash/encrypted files.
- Passwords must not be transmitted in clear text.
- Access to password files must be restricted to IT support.
- Service account credentials must not be stored in clear text within any application.
- Authentication data must not be stored after authorization.
- Password files must be stored separately from application data.

Standard User Configuration:

Unless system configuration limitations prevent compliance, all systems and application passwords on the Davis County Hospital & Clinics network must be configured using the following parameters:

- Must be changed every 180 days maximum
- Must be a minimum of 8 characters
- Must be a combination of alpha and numeric characters
- Must have a no reuse history of 5 passwords
- Must lockout after 10 invalid attempts and remain locked out

Privileged User Configuration:

Unless system configuration limitations prevent compliance, all systems and application administrative passwords on the Davis County Hospital & Clinics network must be configured using the following parameters:

- Must be changed every 180 days maximum
- Must be a minimum of 10 characters
- Must be a combination of alpha and numeric and special characters
- Must have a no reuse history of 5 passwords
- Must lockout after 10 invalid attempts and remain locked out
- Remote Access Configuration Requirements:
    - The use of two-factor authentication is required for remote access connections to the Davis County Hospital & Clinics network.
    - Exceptions may be made for specific applications (like automated backup) with the approval of the Davis County Hospital & Clinics Security Officer. In order for an exception to be approved there must be a method or procedure to change the passwords.

Administrator/Special Access Accounts

Davis County Hospital & Clinics users with administrator/special access accounts must also have a standard access account and use the account most appropriate for the given activity (i.e. email/internet use should only be conducted using a standard user account).

- Service accounts must be set up to deny interactive logon.
- Temporary special access accounts (i.e. for auditing purposes) requirements:
  - Must be authorized,
  - Must be created with a specific expiration date,
  - Must be removed when the work is complete.

Password Manager/Vault

- The use of a password vault/manager is encouraged for both privileged and standard users.
- Password managers must:
  - enforce the use of individual user IDs and passwords to maintain accountability;
  - allow users to select and change their own passwords;
  - enforce a choice of quality passwords;
  - store and transmit passwords in protected form.

Trouble-Shooting/General Assistance

- IT Support should not ask a user for their password to assist in troubleshooting but should use their own appropriate administrative access to assist, whenever possible.
- If troubleshooting cannot be conducted without the use of the user's password, IT Support must instruct the user to change their password immediately after use of the known password is complete.

Password Support

- If a user requests a password reset via phone, IT Support must ensure that a support ticket is documented and that an email be sent to the requesting user that a password reset event occurred.
- Upon reset of the password, configure the system/application to require the user to change their password once they log-in.

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Senior Leader	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512586*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*02/2005*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Contingency Planning

~~Policy Number: HS - 1004.00~~

POLICY:

~~The~~Davis County Hospital & Clinics will implement appropriate procedures for safeguarding the integrity and confidentiality of electronic PHI in the event an emergency or other event compromises the Hospital's information systems containing electronic PHI or otherwise prevents access to or interrupts these information systems.

PROCEDURES:

- The ~~Hospital~~facility institutes the following data~~-~~ backup procedures to create and maintain an exact copy of its electronic PHI: 'Server~~/Data~~ Backup Policy~~ No: HS - 1005.00~~'
- In the event any emergency or other event compromising ~~the~~Davis County Hospital~~'s~~ & Clinics information systems resulting in lost electronic PHI, the ~~Hospital~~facility will implement the following process to retrieve and restore the lost data: The last known good backup will be obtained and restored from its storage media.
- In the event of an emergency or other event which prevents the ~~Hospital~~facility, its employees and contractors from accessing the information systems containing electronic PHI, the ~~Hospital~~facility has implemented the following: A paper process that is department specific, known to be in effect by all employees.
- ~~The ~~Davis County Hospital ~~and ICE Technologies~~& Clinics have installed the following security measures to safeguard electronic PHI while operating in an emergency mode: Unauthorized physical access will not be allowed into the areas where the server hardware resides. Servers and infrastructure will be placed on auxiliary power, to maintain accessibility and eliminate single points of failure.
- In the event of an emergency or other event which compromises the ~~Hospital's~~facilities information systems containing electronic PHI, the Hospital will allow its security personnel and other contractors who have previously signed business associate agreements to access available facilities and workstations for the purpose of restoring the ~~Hospital's~~facilities information systems and recovering any lost data. The Security Officer, or his/her designee, will supervise the restoration of information systems and lost data.
- In order to ensure contingency measures work in the event of an emergency or other event, ~~the~~Davis County Hospital ~~or designate~~& Clinics or designee shall perform periodic testing, not less than once per

year, and changes to this policy will be based on the aforementioned tests. In addition, as part of its periodic review of contingency measures, the ~~Hospital~~facility will assess the importance of applications and data in support of its contingency plan.

~~Sources; ICE Technologies Hosting Services Level Agreements~~

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512602*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*05/2008*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Disaster Recovery Planning

~~Policy Number: HS - 1016.00~~

POLICY:

~~The~~Davis County Hospital & Clinics will take measures to ensure a disaster plan is in place and includes periodic testing and logging of results.

PROCEDURE:

- Application and Data Criticality Analysis in the form of an AIA [Application Impact Analysis] will be performed on a yearly basis.
- ~~Application and Data Criticality Analysis in the form of an AIA [Application Impact Analysis]~~Departments will be ~~performed on a yearly basis. Departments will be~~ responsible to keep a ~~policy and~~ procedure in place, to allow for contingency plans of care, lost revenues, delay in billings, etc., in the case of failure of computer systems.
    - Purpose is to know how long the paper process will carry the workflow while waiting for hardware and data restoration
- Annual review of contingency measures per policy "Contingency Planning Policy ~~HS - 1004.00~~" will be tested.
- "Server~~/Dat~~ Backup Policy ~~HS - 1005.00~~" will be incorporated to manage restores, whether in test mode, or true disaster

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending*	**PolicyStat ID:** *10512398*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*03/2018*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Identity And Access Management Policy

Policy:

The purpose of the Davis County Hospital & Clinics Identity and Access Management Policy is to establish the requirements necessary to ensure that access to and use of Davis County Hospital & Clinics **Information Resources** is managed in accordance with business requirements, information security requirements, and other Davis County Hospital & Clinics policies and procedures and to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Department of Health and Human Services ("DHHS") security and privacy regulations.

Audience

The Davis County Hospital & Clinics Identity and Access Management Policy applies to individuals who are responsible for managing Davis County Hospital & Clinics Information Resource access, and those granted access privileges, including special access privileges, to any Davis County Hospital & Clinics **Information Resource**.

Contents

Procedure:

Access Control

- Access to Davis County Hospital & Clinics **Information Resources** must be justified by a legitimate business requirement prior to approval.
- Access to **confidential information** is based on a "need to know".
- Confidential data access must be logged.
- Access to the Davis County Hospital & Clinics network must include a secure log-on procedure.

- Workstations and laptops must force an automatic lock-out after a pre-determined period of inactivity.
- Documented user access rights and privileges to **Information Resources** must be included in disaster recovery plans, whenever such data is not included in backups.

Account Management

- All personnel must sign the Davis County Hospital & Clinics **Information Security Policy Acknowledgement** before access is granted to an account or Davis County Hospital & Clinics **Information Resources**.
- All accounts created must have an associated, and documented, request and approval which shall be submitted to IT from manager, director, EHR superuser or compliance officer. User Access Request form is located on the ~~DCH~~DCHC Intranet.
- **Information Resource** owner supervisors, managers and directors are responsible for the approval of all access requests.
- User accounts and access rights for all Davis County Hospital & Clinics **Information Resources** must be reviewed and reconciled at least annually.
- All accounts must be uniquely identifiable using the user name assigned by Davis County Hospital & Clinics IT and include verification that redundant user IDs are not used.
- All accounts, including default accounts, must have a password expiration that complies with the Davis County Hospital & Clinics **Authentication Standard**.
- Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege".
- Level of access change requests to an account must be submitted as a request and documented accordingly.
- Directors, managers, EHR superusers or compliance officer will submit recommended levels of access to the Information Technology Department. The requester will ensure that all prospective data users receive required training based on the minimum necessary standard and data elements identified for routine requests or disclosures in their area and annotate such training on the submission. If access is needed before training can be completed, the requester will annotate such, the reason why, and the date such training will be completed. All required training must be completed in a timely manner after the receipt of access.
- Whenever possible, access to **Information Resources** should be granted to user groups, not granted directly to individual accounts.
- Shared accounts must not be used. Where shared accounts are required, their use must be documented and approved by the Information Resource owner.
- User account set up for third-party **cloud computing applications** used for sharing, storing and/or transferring Davis County Hospital & Clinics **confidential** or **internal information** must be approved by the resource owner and documented.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Any accounts that have not been accessed within a defined period of time will be disabled.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- System Administrators or other designated personnel:
    - Are responsible for modifying and/or removing the accounts of individuals that change roles with Davis County Hospital & Clinics or are separated from their relationship with Davis County Hospital & Clinics.
    - Must have a documented process to modify a user account to accommodate situations such as

  - name changes, accounting changes, and permission changes.
  - Must have a documented process for periodically reviewing existing accounts for validity.
  - Are subject to independent audit review.
  - Must provide a list of accounts for the systems they administer when requested by authorized Davis County Hospital & Clinics IT management personnel.
  - Must cooperate with authorized Davis County Hospital & Clinics Information Security personnel investigating security incidents at the direction of Davis County Hospital & Clinics executive management.

Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves Davis County Hospital & Clinics altogether.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- Special access accounts for internal or external audit, software development, software installation, or other defined need, must be administered according the Davis County Hospital & Clinics **Authentication Standard**.

Authentication

- Personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following Davis County Hospital & Clinics rules:
  - Must meet all the requirements established in the Davis County Hospital & Clinics **Authentication Standard**, including minimum length, complexity and rotation requirements.
  - Must not be easily tied back to the account owner by using things like: user name, social security number, nickname, relative's names, birth date, etc.
  - Should not include common words, such as using dictionary words or acronyms.
  - Should not be the same passwords as used for non-business purposes.
- Password history must be kept to prevent the reuse of passwords.
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (i.e. security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated and unnecessary default accounts

removed or disabled before installing a system on the network.

- User account passwords must not be divulged to anyone. Davis County Hospital & Clinics support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Davis County Hospital & Clinics, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the Davis County Hospital & Clinics **Authentication Standard** for the sake of ease of use.
- Users should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Davis County Hospital & Clinics IT Management.
- If a password management system is employed, it must be used in compliance with the Davis County Hospital & Clinics Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off of the device.
- Davis County Hospital & Clinics IT Support password change procedures must include the following:
    - authenticate the user to the helpdesk before changing password
    - change to a strong password
    - require the user to change password at first login.
- In the event that a user's password is compromised or discovered, the password must be immediately changed and the security incident reported to Davis County Hospital & Clinics IT support.

Remote Access

- All remote access connections to the Davis County Hospital & Clinics networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
- Remote users may connect to the Davis County Hospital & Clinics networks only after formal approval by the requestor's manager or Davis County Hospital & Clinics Management.
- The ability to print or copy **confidential information** remotely must be disabled.
- Users granted remote access privileges must be given remote access instructions and responsibilities.
- Remote access to **Information Resources** must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the Davis County Hospital & Clinics network unless approved in advance by Davis County Hospital & Clinics IT management.
- Non-Davis County Hospital & Clinics computer systems that require network connectivity must conform to all applicable Davis County Hospital & Clinics IT standards, and must not be connected without prior written authorization from IT Management.
- Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.
  To be granted remote access, submit a remote access request form to HR, who will in turn submit to IT for enablement.

Vendor Access

- Vendor access must be uniquely identifiable and comply with all existing Davis County Hospital & Clinics policies.
- External vendor access activity shall be monitored.

- All vendor maintenance equipment on the Davis County Hospital & Clinics network that connects to the outside world via the network, telephone line, or leased line, and all Davis County Hospital & Clinics Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 6, 7, 8, 9, 12, 15
- NIST CSF: PR.AC, PR.IP, PR.MA, PR.PT, DE.CM
- Remote Access Request Form
- Authentication Standard Procedure
- User Access Request Form

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Attachments

Remote_Access_Request_Form.docx
Appendix_A_Definitions.pdf

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512402*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE

Origination:	*03/2018*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Information Classification And Management Policy

Policy:

The purpose of the Davis County Hospital & Clinics Information Classification and Management Policy is to provide a system for classifying and managing **Information Resources** according to the risks associated with its storage, processing, transmission, and destruction.

Audience

The Davis County Hospital & Clinics Information Classification and Management Policy applies to any individual, entity, or process that interacts with any Davis County Hospital & Clinics **Information Resource**.

Contents

Information Classification

Information Handling

Information Retention & Destruction

Responsibilities

Information User

- The person, organization or entity that interacts with Information for the purpose of performing an authorized task.
- Have a responsibility to use Information in a manner that is consistent with the purpose intended and in compliance with policy.

  Information Owner
- The person responsible for, or dependent upon, the business process associated with an information asset.
- Is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

- Determines the appropriate value and classification of information generated by the owner or department.
- Must communicate the information classification when the information is released outside of the department and/or Davis County Hospital & Clinics.
- Controls access to their information and must be consulted when access is extended or modified.
- Must communicate the information classification to the Information Custodian so that the Information Custodian may provide the appropriate levels of protection.

Information Custodian

- Maintains the protection of Information according to the information classification associated to it by the Information Owner.
- Delegated by the Information Owner and is usually Information Technology personnel.

Procedure:

Information Classification

- Information owned, used, created or maintained by Davis County Hospital & Clinics should be classified into one of the following three categories:
  - Public
  - Internal
  - Confidential
- **Public Information:**
  - Is information that may or must be open to the general public.
  - has no existing local, national, or international legal restrictions on access or usage.
  - While subject to Davis County Hospital & Clinics disclosure rules, is available to all Davis County Hospital & Clinics employees and all individuals or entities external to the corporation.
- Examples of **Public Information** include:
  - Publicly posted press releases,
  - Publicly available marketing materials,
  - Publicly posted job announcements.
- **Internal Information:**
  - Is information that must be guarded due to proprietary, ethical, or privacy considerations.
  - Must be protected from unauthorized access, modification, transmission, storage or other use and applies even though there may not be a civil statute requiring this protection.
  - Is restricted to personnel designated by Davis County Hospital & Clinics, who have a legitimate business purpose for accessing such Information.
- Examples of **Internal Information** include:
  - Employment Information,
  - Business partner information where no more restrictive confidentiality agreement exists,
  - Internal directories and organization charts,
  - Planning documents,
  - Contracts.
- **Confidential Information:**
  - Is information protected by statutes, regulations, Davis County Hospital & Clinics policies or contractual language. Information Owners may also designate Information as Confidential.
  - Is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis only.

    - Disclosure to parties outside of Davis County Hospital & Clinics must be authorized by executive management, approved by the Director of Information Technology and/or General Counsel, or covered by a binding confidentiality agreement.
- Examples of **Confidential Information** include:
    - Customer data shared and/or collected during the course of a consulting engagement,
    - Financial information, including credit card and account numbers,
    - Social Security Numbers,
    - Personnel and/or payroll records,
    - Any Information identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction,
    - Any Information belonging to an Davis County Hospital & Clinics customer that may contain personally identifiable information,
    - Patent information.

Information Handling

- All Information should be labeled according to the Davis County Hospital & Clinics **Labeling Standard**.
- **Public:**
    - Disclosure of **Public Information** must not violate any pre-existing, signed non-disclosure agreements.
- **Internal:**
    - Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
    - Must be protected by a confidentiality agreement before access is allowed.
    - Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
    - Is the "default" classification level if one has not been explicitly defined.
- **Confidential:**
    - When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords as defined in the **Authentication Standard**.
    - When stored on mobile devices and media, must be encrypted.
    - Must be encrypted at rest.
    - Must be stored in a locked drawer, room, or area where access is controlled by a cipher lock and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
    - Must not be transferred via unsecure communication channels, including, but not limited to:
        - Unencrypted email
        - Text messaging
        - Instant Messaging
        - Unencrypted FTP
        - Mobile devices without encryption
    - When sent via fax, must be sent only to a previously established and used address or one that has been verified as using a secured location.
    - When transmitted via USPS or other mail service, must be enclosed in a sealed security envelope.
    - Must not be posted on any public website.
    - Davis County Hospital & Clinics Management must be notified in a timely manner if Information classified as **Confidential** has been or is suspected of being lost or disclosed to unauthorized parties.

Information Retention & Destruction

- All information maintained by Davis County Hospital & Clinics must include a documented timestamp, or include a timestamp as part of metadata.
- Information that is no longer required to be maintained by Davis County Hospital & Clinics is classified as "Expired" and must be destroyed in accordance with Davis County Hospital & Clinics **asset decommission procedure**
- Information owners should be consulted prior to information destruction and may have the opportunity to extend Information expiration, given business needs and/or requirements for the extended retention.
- Davis County Hospital & Clinics customers may have their own information retention requirements that supersede Davis County Hospital & Clinics's requirements. Such customer requirements should be documented in contractual language.

Definitions

- See Appendix A: Definitions

References

- ISO 27002: 8, 14, 18
- NIST CSF: ID.AM, PR.DS, PR.IP

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Attachments

Appendix_A_Definitions.pdf

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512412*

Davis County
HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*03/2018*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Information Security Policy

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Davis County Hospital & Clinics Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

Confidentiality – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic "need-to-know" principle.

Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.

Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Davis County Hospital & Clinics has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to Davis County Hospital & Clinics by its stakeholders, partners, customers and other third-parties.

The Davis County Hospital & Clinics Information Security Program is built around the information contained within this policy and its supporting policies.

Policy:

The purpose of the Davis County Hospital & Clinics Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Davis County Hospital & Clinics, its business partners, and its stakeholders. Additionally, that the use of Davis County Hospital &

Clinics **Information Resources** are managed in accordance with business requirements, information security requirements, and other Davis County Hospital & Clinics policies and procedures and to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Department of Health and Human Services ("DHHS") security and privacy regulations.

Audience

The Davis County Hospital & Clinics Information Security Policy applies equally to any individual, entity, or process that interacts with any Davis County Hospital & Clinics Information Resource.

Responsibilities

Executive Management

Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all **Information Resources** collected or maintained by or on behalf of Davis County Hospital & Clinics.

Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.

Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.

Ensure that the IT Security officer is given the necessary authority to secure the **Information Resources** under their control within the scope of the Davis County Hospital & Clinics Information Security Program.

Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.

Ensure that the Information Security Officer, in coordination with IT support, reports annually to Executive Management on the effectiveness of the Davis County Hospital & Clinics Information Security Program.

Information Security Officer

Provides updates on the status of the Information Security Program to Executive Management.

Manage compliance with all relevant statutory, regulatory, and contractual requirements.

Participate in security related forums, associations and special interest groups.

Assess risks to the confidentiality, integrity, and availability of all **Information Resources** collected or maintained by or on behalf of Davis County Hospital & Clinics.

Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.

Ensure that Davis County Hospital & Clinics has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.

Ensure that appropriate information security awareness training is provided to company personnel, including contractors.

Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of Davis County Hospital & Clinics.

Develop and implement procedures for testing and evaluating the effectiveness of the Davis County Hospital & Clinics Information Security Program in accordance with stated objectives.

Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.

Report annually, to Executive Management on the effectiveness of the Davis County Hospital & Clinics Information Security Program, including progress of remedial actions.

All Employees, Contractors, and Other Third-Party Personnel

Understand their responsibilities for complying with the Davis County Hospital & Clinics Information Security Program.

Use Davis County Hospital & Clinics **Information Resources** in compliance with all Davis County Hospital & Clinics Information Security Policies.

Seek guidance from the Information Security Team for questions or issues related to information security.

Procedure:

- Davis County Hospital & Clinics maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that:
    - Serve to protect the Confidentiality, Integrity, and Availability of the **Information Resources** maintained within the organization using administrative, physical and technical controls.
    - Provide value to the way we conduct business and support institutional objectives.
    - Comply with all regulatory and legal requirements, including:
        - HIPAA Security Rule,
        - State breach notification laws,
        - Information Security best practices, including ISO 27002 and NIST CSF,
        - Contractual agreements,
        - All other applicable federal and state laws or regulations.
- The information security program is reviewed no less than ~~annually~~once every two years, or upon significant changes to the information security environment.
- Information security program shall be reviewed by an independent third party no less than annually.

Waivers:

Waivers, or exceptions, from certain IT policy provisions may be sought following the DCHC Waiver Process, which is as follows:

- End user seeking waiver contacts manager about the exception to an information policy he or she is seeking.
- If manager is willing to justify request he or she will enter a help desk ticket requesting the waiver.
- The information technology security officer will make a determination whether to accept or reject the waiver.
- If the information security officer accepts the waiver he or she should require a reasonable and appropriate compensating control whenever possible.

- The helpdesk ticket will be kept as a historical record of the acceptance or rejection of the waiver request.
- If the waiver was approved the ticket will also contain the activity performed by the information technology to accommodate the waiver request as a historical record of change.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 5, 6, 7, 18
- NIST CSF: ID.AM, ID.BE, ID.GV, PR.AT, PR.IP

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Attachments

Appendix_A_Definitions.pdf

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512477*

Davis County
HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*12/2016*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Physical and Environmental Security

~~Policy~~

~~DCH will ensure proper measures are in place to prevent unauthorized physical access or damage to the organization's information and facilities.~~

~~Scope: This Physical and Environmental Security Policy applies to all business processes and data, information systems and components, personnel, and physical areas of Davis County Hospital.~~

~~Procedure~~

~~Physical Access and Security:~~

- ~~Physical security perimeters will be identified and will protect mission critical information or facilities.~~
- ~~Appropriate entry controls will be implemented at secure access points to ensure only individuals with appropriate access levels are allowed access. These access points will be monitored.~~
  - ~~Davis County Hospital should develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.~~
  - ~~Davis County Hospital should establish a process to review, approve, and issue credentials for facility access.~~
  - ~~Information Security shall remove individuals from the facility access list when access is no longer required.~~
  - ~~Davis County Hospital should maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points. (See Facilities Security Policy)~~
  - ~~Security measures will be implemented for working in various identified safe spaces and delivery and loading spaces.~~

~~Environmental Security:~~

- ~~Protection against natural disasters or other malicious attacks, as well as accidental incidents, will be determined and implemented.~~
- ~~Davis County Hospital should place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.~~
- ~~Applicable security measures will be implemented for offices, boardrooms, etc., including considerations~~

~~for temperature, protection against water damage, and emergency lighting.~~

~~**Equipment Security:**~~

- ~~Equipment will be handled and protected to ensure risks are reduced, preventing potential environmental threats and hazards.~~
- ~~Redundancies and other supporting procedures will be put in place to protect from power failures and other disruptions, including ensuring power and telecommunications cabling carrying data will be properly protected.~~
- ~~Equipment will be regularly maintained.~~
- ~~Any removal of assets must be done with prior authorization from the right party.~~
- ~~Any offsite assets will be treated with the same security measures, with special consideration to risks of being off-premise.~~
- ~~Disposal or re-use of equipment must be done after the removal of sensitive or critical data has been completed.~~
- ~~Any unattended equipment must have applicable protection.~~
- ~~Personnel are responsible for maintaining their personal workspaces and ensuring media or literature containing sensitive or critical information is properly stored and not in the open.~~

POLICY:

Physical and environmental security controls must be implemented to protect the facilities that house information technology (IT) resources, including but not limited to network communication closets. Access to IT assets and/or **information resources** must be controlled through key locks, biometric authentication, or computer controlled badge access systems.

Scope: Facilities that house Davis County Hospital & Clinics **information resources** must be protected by physical entry controls, other protection measures, and maintenance records/change control procedures. These measures, controls and procedures must ensure that appropriate physical and environmental security precautions are stipulated across the facility to protect IT assets. Other protection measures should be in place to protect **information resources** from physical damage, theft, power surges, water, overheating, electrostatic discharge and other forms of physical and environmental threat. Maintenance records/change control shall be in place to ensure that repairs and modifications to the physical components that house information resources, such as hardware, walls, doors and locks, are documented.

PROCEDURE:

Physical Entry Controls

A. Facilities that house information resources must be protected by entry controls to ensure that only authorized Users have access;

B. Within facilities that house information resources, all employees must wear visible identification and are required to challenge unescorted or unauthorized visitors (if the employee feels threatened by the visitor, they should notify appropriate personnel);

C. Additional entry controls should also be used in each area that contain or support information resources, such as network communication closets and sources of electrical power for information resources. Telephone closets, network router and hub rooms, network switching rooms and similar areas containing communications equipment must be kept locked at all times;

D. Additional requirements for access to information resources, which apply to employees and all other visitors to computer data centers, are detailed below.

Access To Data Center or Secondary Network Closets

A. The IT Director will serve as an access custodian responsible for determining who should be authorized to physically access information resources. The access custodian will:

B. Maintain a current list of persons authorized to access these facilities;

C. Review and approve access requests based on valid business requirements;

D. Review the camera surveillance of non-routine accesses on a periodic basis;

E. Review the access list on a regular basis (at least once a year) to delete persons who no longer need access. This does not preclude the requirement to immediately delete persons whose need has expired (e.g., due to termination or transfer)

Maintenance Records/Change Control Procedures

All repairs and modifications to the physical components that house information resources, such as hardware, walls, doors and locks, must be documented and change management procedures followed.

Hardware and Software Modifications/Installation

No one shall install, modify or reconfigure the hardware or software of any **information resource** or IT Asset without authorization from a DCHC IT staff member. Installation or modification of any DCHC **information resource** must adhere to all applicable IT policies. IT Administrators and the IT Directory will conduct spot audits of **information resources** perodically and will remove applications, information or other system changes that have been placed there inappropriately.

Moving Computer Equipment

Computer equipment (e.g. workstations, servers, printers, network infrastructure, etc.) must not be moved or relocated without the prior approval of IT personnel and must be moved only by IT personnel or their designee.

Other Physical and Environmental Protection Measures

A. **Base Physical Standards**

1. Data centers and secondary closets shall have camera surveillance installed to monitor ingress/egress.
2. Fire detection and suppression systems must be used in compliance with NFPA Standard for the Protection of Electronic Computer/Information Processing Equipment
3. Smoke and heat detectors shall be installed wherever information resources are located. Floor and ceiling tiles that conceal detectors must be marked.
4. Sprinkler systems must have separate shut-off valves and delayed deployment capabilities. When possible, a switch should automatically cut power to discharge sprinklers.
5. Locating IT equipment in lower floors, under pipes or ductwork subject to becoming a conduit for drainage from internal flooding should be avoided.
6. Facilities located in areas subject to external flooding should be equipped with sump pumps.

   7. Basement facilities that house information resources, including telecommunications equipment, shall include reasonable protection from flooding, such as elevation of the equipment off the floor or availability of waterproof covers.
   8. IT data centers, including telecommunication facilities must be locked at all times. Conspicuous identification of these locations should be avoided. Information about security controls should be safeguarded from unauthorized disclosure.
   9. All non-electrical piping should be identified and labeled to allow for rapid shut-off in the event of an emergency.
   10. Cables used in raised floor, drop-ceiling environments must be made of fire-rated quality.
   11. Conduit and building wiring systems should be in good repair. Telephone and electrical cables should not occupy the same conduit.

B. **Housekeeping**

   1. Combustible supplies, such as paper and flammable cleaning fluids, must be stored in the IT data centers in small quantities and must be kept in metal cabinets whenever possible. Large quantities of these materials must be stored elsewhere. Solvents must be stored in closed, fire retardant containers away from paper and other combustibles.
   2. Smoking is prohibited in all areas that house information resources.
   3. IT data centers and communication closets should, if possible, not be used as storage areas for miscellaneous supplies and janitorial cleaning tools/supplies.
   4. Co-location of printing and other dust producing operations in the same room with computers and communication equipment should be avoided if possible.

C. **Electrical Power and Environmental Conditioning**

   1. The need for power conditioning must be evaluated as part of the installation of all IT equipment and must at a minimum include surge protection.
   2. Computer equipment requiring a planned shutdown process must have Uninterruptible Power Supplies (UPS).
   3. When justified by the critical nature of ongoing operations, backup power must be available. When implemented, backup power must be tested periodically.
   4. When economically feasible, IT data centers should be supplied by more than one electrical power grid.
   5. All critical electrical switching devices used to support emergency power or alternate power grids must be tested regularly.
   6. Air conditioning systems, including temperature and humidity control systems, must be implemented consistent with the environmental requirements of the hardware manufacturers.
   7. Emergency lighting should be available in areas that house IT computer equipment.
   8. Manufactures electrical specifications and applicable building codes must be followed.

Guidance

Guidance	Section
ISO27001:2013	A.11 (A.11.1, A.11.2)

NIST SP 800-53 v4	PE-2~PE-6, MA-5, PE-8, CP-2, CP-6, CP-7, PE-1, CP-8, PE-19~PE-16, MA-2~MA-6, AC-19, AC-20, MP-5, PE-17, MP-6, MA-2, MP-5

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512437*

Davis County
HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*02/2005*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Risk Assessment Procedures

~~Policy Number: HS-1002.00~~

~~POLICY:~~

~~The Hospital will implement a process to assess and address security risks and to periodically review its security measures in order to prevent, detect, contain and correct security violations, and to ensure compliance with the Security Regulations.~~

~~PROCEDURES:~~

- ~~The Hospital has conducted an initial risk assessment of the potential risks and vulnerabilities of the confidentiality, integrity and availability of its electronic PHI. This initial risk assessment is an inventory and assessment of the potential risks and vulnerabilities to electronic PHI maintained by the Hospital.~~
- ~~Based on this initial risk assessment, the Hospital has identified security measures it deems reasonable and appropriate to reduce the risks and vulnerabilities identified in the risk assessment. In addition, it has identified those additional security measures contained in these policies and procedures as being reasonable and appropriate to protect and safeguard the electronic PHI it maintains.~~
- ~~The Hospital will conduct periodic follow-up risk assessments as it deems appropriate. Risk assessments may be conducted internally by Hospital personnel or through outside contractors. The Security Officer, or his or her designee, shall keep documentation of each risk assessment and the identifiable security measures the Hospital deems reasonable and appropriate to reduce the risks and vulnerabilities identified by a particular risk assessment.~~
- ~~The Hospital will periodically review, but not less than annually, its records of system activity for systems containing electronic PHI in order to monitor its security controls.~~
- ~~The Hospital will periodically evaluate, but not less than annually, the security measures it implements under these policies and procedures to demonstrate and document its compliance with the Security Regulations. In addition, evaluations will be performed in response to environmental or operational changes impacting the security of electronic PHI. Evaluations will include a review of both technical and non-technical components of the Hospital's security system. Any evaluation conducted hereunder may be conducted internally by the Hospital personnel or through outside contractors. .~~
- ~~Risk Assessment and Analysis outcomes will be documented and introduced to monthly Compliance and HIPAA meetings. Remediation will be recorded and stored in locked office of IT Director.~~

- ~~Monitoring reports will be diligently completed and documented.~~

POLICY:

Davis County Hospital & Clinics will continually identify and assess the Information Technology systems vulnerabilities and potential threats to the confidentiality, integrity and availability of internal networks, systems and confidential information. Davis County Hospital & Clinics will select and implement reasonable and appropriate, cost effective controls and safeguards and will institute corrective action as necessary to protect the systems. Sufficient security measures will be implemented that will mitigate risks, threats and vulnerabilities identified in the assessment.

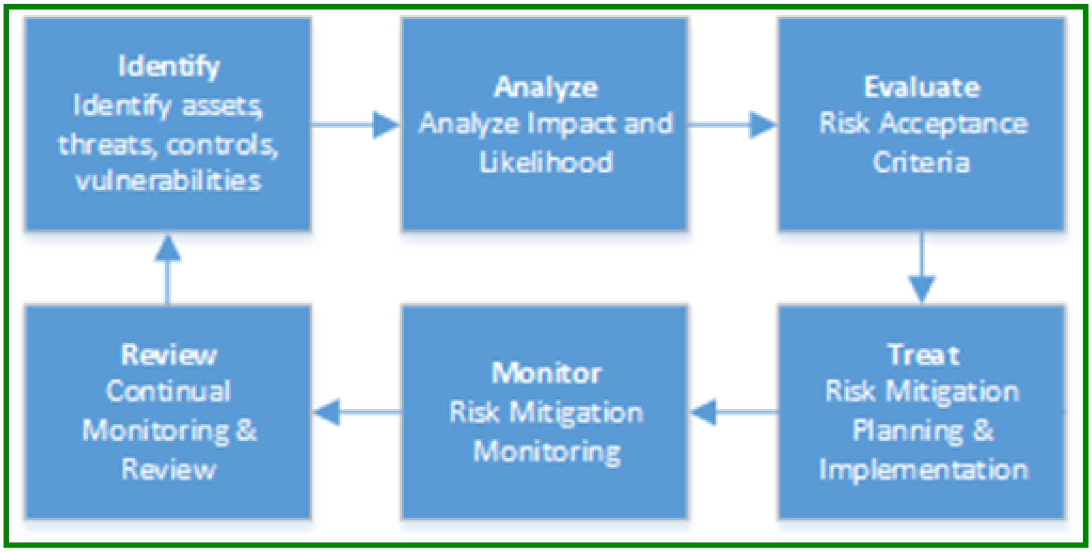
PROCEDURE:

A. ***Risk Assessment Procedure***:

1. The IT Security Officer will:
    a. Coordinate the development and maintenance of risk management policy and strategy.
    b. Report annually to Senior Leadership and the Board of Trustees on the effectiveness of the information security program.
    c. Ensure that personnel who are tasked with significant risk management and information security responsibilities are adequately skilled to carry out their responsibilities.
    d. Develop and maintain procedures, standards and forms that are in compliance with this and all other applicable information security policies.
    e. Assess the risk and impact from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of Davis County Hospitals & Clinics.

B. ***Risk Assessment Process***:

1. In order for Davis County Hospital & Clinics to adequately protect the information that is entrusted to it, the organization must gain an understanding of and manage the risks to the information security environment. The risk assessment should be repeatable and based on industry best practices. In order to meet the requirements of an ongoing risk management program, Davis County Hospital & Clinics uses ISO/IEC 27005 (Information technology – Security techniques – Information security risk management) as a reference for the risk management practices.


Identify
Identify assets, threats, controls, vulnerabilities
Analyze
Analyze Impact and Likelihood
Evaluate
Risk Acceptance Criteria
Treat
Risk Mitigation Planning & Implementation
Monitor
Risk Mitigation Monitoring
Review
Continual Monitoring & Review

2. The risk assessment is implemented using the Risk Assessment Template. The risk assessment process is coordinated by the Information Security Officer, identification of threats and vulnerabilities is performed by asset owners, and assessment of existing controls, impact and likelihood is performed by Information Security Officer.
   Information security risk management procedures include the following (at a minimum):
   a. Identification of Assets
   b. Identification of Threats
   c. Identification of Vulnerabilities
   d. Identification of Existing Controls
   e. Risk Analysis
   f. Risk Treatment
   g. Risk Communication
   h. Risk Monitoring and Review
3. Formal facility wide IT risk assessments will be conducted by a competent, independent third party IT Security vendor no less than annually or upon signification changes to the information security environment. Risk assessments should account for natural, environmental, and human threats. Risk assessments must include administrative, physical, and technical controls. Risk evaluation criteria should be developed for evaluating the company's information security risks considering the following:
   a. The strategic value of the business information process
   b. The criticality of the information assets involved
   c. Legal and regulatory requirements, and contractual obligations
   d. Operational and business importance of availability, confidentiality and integrity
   e. Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation
4. The first step in risk assessment is the identification of all assets in scope – i.e. all assets which may affect confidentiality, integrity and availability (CIA) of information in the organization. Assets may

include documents in paper or electronic form, applications and databases, people, hardware, software, IT equipment, infrastructure, and external services/outsourced processes (see Risk Assessment Template).

5. The next step is to identify all threats and vulnerabilities associated with each asset. Threats are what we are trying to protect assets from, like data leakage, accidental deletion, or a breach of the network. Vulnerabilities are weaknesses in our protection efforts, like lack of encryption, inadequate backups, or unpatched systems. Common threats and vulnerabilities are incorporated into the risk assessment table. Additional threats and vulnerabilities should be identified using the threats and vulnerabilities catalogs as guides (see **Risk Assessment Template**). Each asset may have several threats that have a potential impact on the asset and every threat may be associated with several vulnerabilities.

6. While there are many ways to gather evidence to complete the risk assessment, the primary methods utilized as part of this methodology include:

   a. Asset Review: perform reviews of all hardware, software and data assets and functionality to determine where potential risks exist

   b. Interviews: perform interviews with responsible person(s) from each department and review list of people, processes and other assets utilized and discuss where potential risks to CIA of information exist

   c. Observation: review existing documentation (policies, procedures, organizational charts, network configuration, data mapping, etc.) and determine where potential risks to CIA of information exist

   d. Education: review updates or additions to existing laws, regulations, frameworks and industry guidance (i.e. Critical Security Controls) against current processes to look for potential gaps that may increase risk to CIA of information

   e. External or Internal Audit Findings: these reports can provide insight into noted gaps or weaknesses that may increase risks to CIA of information

7. Once threats and vulnerabilities have been assigned to each asset, identification of existing controls should be conducted. Existing controls include all applicable policies and procedures that reduce the impact of potential threats.
   For the identification of controls, the following activities can be helpful:

   a. Reviewing documents containing information about the controls (i.e. previous risk treatment implementation plans)

   b. Checking with the employees and those tasked with information security responsibilities as to which controls are implemented and their effectiveness

   c. Conducting an on-site review of the physical controls, comparing those implemented with the list of what controls should be there and verifying their effectiveness

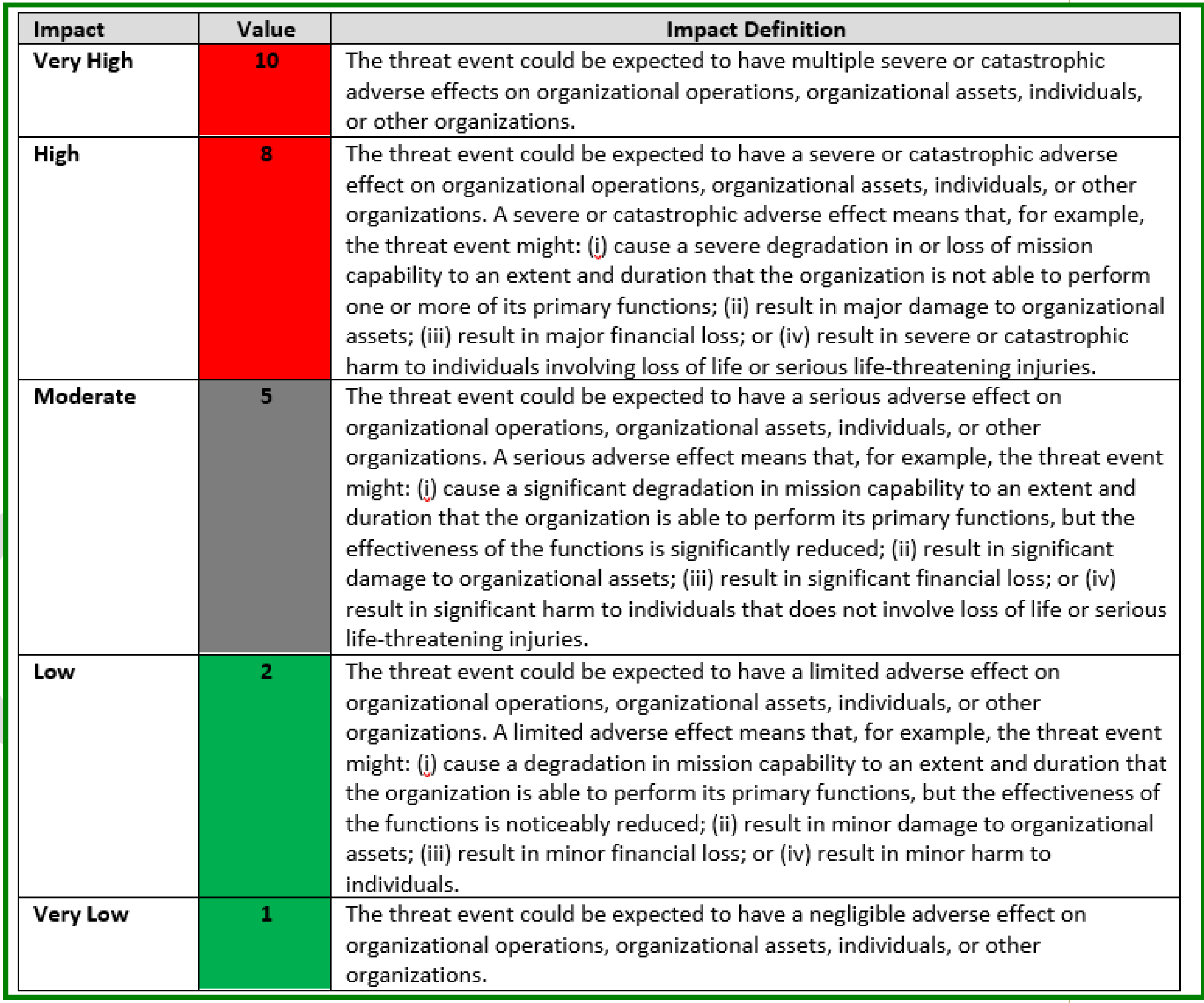
   d. Reviewing results from internal and external audits

8. Once threats, vulnerabilities and controls have been adequately defined for each asset, it is necessary to assess the consequences (impact) to the assets if the risks were to materialize and the probability (likelihood) that the threat will occur.

9. For the Davis County Hospital & Clinics risk assessment, a qualitative scale of Very High, High, Moderate, Low and Very Low is used for calculating both the Impact and Likelihood. When

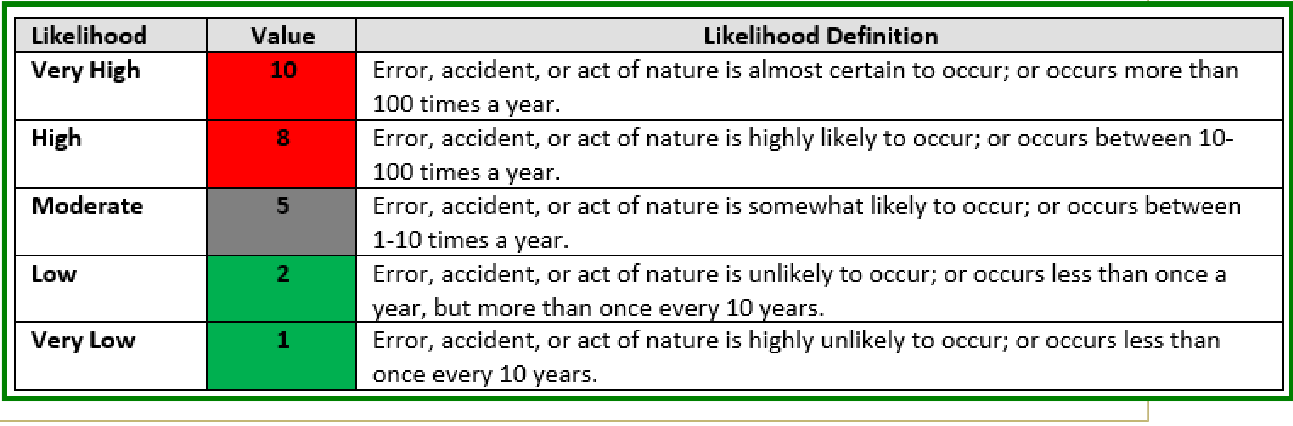
calculating the Impact and Likelihood, the effectiveness of existing controls should be considered. Additionally, the criticality of the asset, as defined by Information Security Values of Confidentiality, Integrity and Availability, should be considered when determining impact.

a. First, consider the impact to the asset if the threat were to materialize because of the vulnerability stated.



Impact	Value	Impact Definition
Very High	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, or other organizations.
High	8	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, or other organizations. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	5	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, or other organizations. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	2	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, or other organizations. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	1	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, or other organizations.

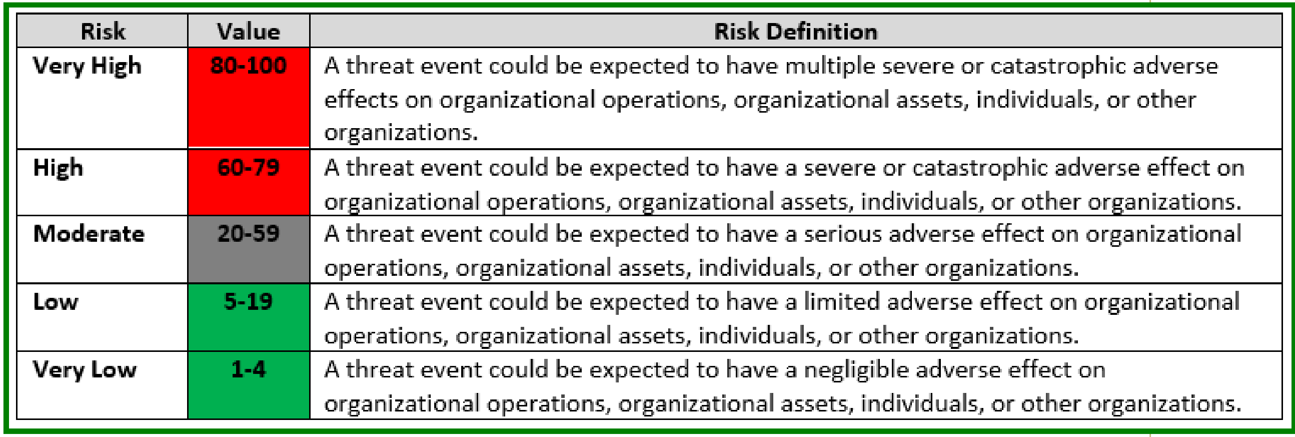
b. After the impact assessment it is necessary to assess the likelihood that the threat will exploit the vulnerability of each asset.



Likelihood	Value	Likelihood Definition
Very High	10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	8	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	5	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	1	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

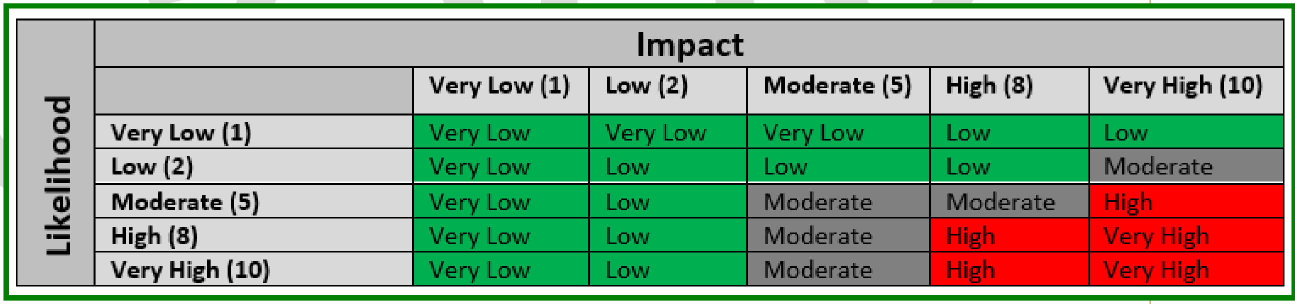
c. To determine the risk, multiply the Impact value by the Likelihood value.

d. Risk ratings are determined using the following table. During risk evaluation, contractual, legal and regulatory requirements are factors that should be taken into account in addition to the estimated risks.



Risk	Value	Risk Definition
Very High	80-100	A threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, or other organizations.
High	60-79	A threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, or other organizations.
Moderate	20-59	A threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, or other organizations.
Low	5-19	A threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, or other organizations.
Very Low	1-4	A threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, or other organizations.

e. Davis County Hospital & Clinics evaluates risk based on a scale of High, Moderate and Low. Risks rated as Very High, High or Moderate should have a corrective action put in place as soon as reasonable and appropriate. Risks rated as Low must be reviewed by the information security committee to determine whether corrective action is needed. Risks rated as very low can be accepted unless otherwise recommended by Senior Leadership or other internal stakeholder.



		Impact				
		Very Low (1)	Low (2)	Moderate (5)	High (8)	Very High (10)
Likelihood	Very Low (1)	Very Low	Very Low	Very Low	Low	Low
	Low (2)	Very Low	Low	Low	Low	Moderate
	Moderate (5)	Very Low	Low	Moderate	Moderate	High
	High (8)	Very Low	Low	Moderate	High	Very High
	Very High (10)	Very Low	Low	Moderate	High	Very High

10. Risk treatment options are determined based on the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options. There are four options available for risk treatment:

    a. risk reduction: reducing the risk level through application of controls

    b. risk retention: accepting the risk "as is"

    c. risk avoidance: avoiding the activity that can lead to the risk

    d. risk transfer: transferring the risk to an external party who can more effectively manage it

11. The four options for risk treatment are not mutually exclusive. Sometimes there is greater benefit in combining multiple options such as reducing the likelihood of risks, reducing their consequences, and transferring or retaining any residual risks.

12. Risk treatment should result in reducing the residual risk to an acceptable level. Davis County Hospital defines an acceptable level to be low or very low. The Risk Treatment plan should describe how the risks will be treated to meet the risk acceptance criteria.

13. Upon completion of the risk treatment(s), the Information Security Officer shall document the

findings in the the residual risk assessment (see Risk Assessment Template) and/or Action Plan as provided by third party vendor conducting an annual risk assessment.

14. Ongoing monitoring and review of the risk assessment and risk treatment actions is necessary in order to ensure they are relevant and appropriate for current circumstances. Improvements should be communicated to those with roles in the risk management process to ensure all necessary elements of the risk assessment are included and the changes will not have adverse impact to the process. Additionally, Davis County Hospital & Clinics should verify that the criteria used to measure risks are still valid and are consistent with business objectives.

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512456*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE

Origination:	*02/2005*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Sanctions

~~Policy Number: HS1012.00~~

POLICY:

The Hospital employee who violates these IT policies and procedures will be subject to disciplinary action up to and including termination.

PROCEDURES:

If an investigation of security incident results in a finding that an employee has violated these Security Policies and Procedures, the employee will be subject to disciplinary action.

- The (1st) first offense will be a written warning. *If the severity of the offense warrants, termination could result.*
- The (2nd) second offense will result in termination.
- Each episode of employee discipline regarding confidential healthcare information is to be documented and reported to the Privacy Officer and HR.

Documentation is to include:

1. Name of Employee
2. Degree of Violation
3. Location of Violation
4. Date and Time of Violation
5. Disciplinary action provided

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending*	**PolicyStat ID:** *10512463*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*03/2018*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Security Training And Awareness Policy

Policy:

The purpose of the Davis County Hospital & Clinics Security Training and Awareness Policy is to describe the requirements to ensure that each user of Davis County Hospital & Clinics **Information Resources** receives adequate training on information security issues.

Audience

The Davis County Hospital & Clinics Security Training and Awareness Policy applies equally to all individuals that use any Davis County Hospital & Clinics **Information Resource**.

Procedure:

- All new personnel must complete an approved Security Awareness training prior to, or within 30 days of, being granted access to any Davis County Hospital & Clinics **Information Resources**.
- All personnel must be provided with relevant information security policies to allow them to properly protect Davis County Hospital & Clinics **Information Resources**.
- All personnel must acknowledge they have received and agree to adhere to the Davis County Hospital & Clinics Information Security Policies before they are granted to access to Davis County Hospital & Clinics **Information Resources**.
- All personnel must complete the annual security awareness training as a core learning competency.
- Davis County Hospital ~~Security~~& Clinics IT Team must develop and maintain a process to be able to communicate new security program information, security bulletin information, and security items of interest.

Definitions

See Appendix A: Definitions

References

- ISO 27002: 7
- NIST CSF: PR.AT

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Attachments

Appendix_A_Definitions.pdf

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending* **PolicyStat ID:** *10512468*

Origination:	*05/2016*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Server Backup

POLICY

Data is one of Davis County Hospital & Clinic's most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on company servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

PROCEDURE

~~1. This policy refers to the backing up of data that resides on Davis County Hospital's servers. Servers and the files and/or data types on these servers that are covered by this policy include:~~

This policy refers to the backing up of data that resides on Davis County Hospital & Clinic's on premise servers and the files and/or data types on these servers that are covered by this policy include:

- Active Directory/User accounts/Groups/Computers
- Application Servers
- ~~Kronos,~~ Quick-Charge, Spiceworks
- Backup Servers/Unitrends
- Interface Servers -Corepoint
- Nessus
- Reporting Servers - Telergy Unite
- Milestone
- Lenel Access Management
- SFTP Server
- Patch Management Server
- File Servers
- Print Server
- Omnicell Server
- ~~VMware~~Nutanix Servers
- SQL Servers- MS SQL 2012/MS SQL 2016

~~2.~~ This policy does not refer to backing up of data that resides on individual PC or notebook hard drives. Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data to their "HOME" drives in order that their data is backed up regularly in accordance with this policy.

~~3.~~In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users are reminded to save and close all files, as well as all related applications, prior to the ~~backup procedure window~~leaving their workstation unattended for long periods of time.

~~4.~~It is the responsibility of server administrators to ensure that all new servers be added to this policy, and that this policy be applied to each new server's maintenance routine. ~~Prior to deploying a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed. Prior to retiring a server, a full backup must be performed and placed in permanent storage.~~

~~5.Backup Schedule~~
~~Backups are conducted automatically using an approved Backup system. [Insert a description of any technologies or tools used to conduct backups that are specific to your organization.]~~
~~The servers listed above must be backed up according to the following procedure. This method ensures that no more than one day's working data will be missing in the event of a data loss incident:~~
~~All backups, stored off site, are to be stored at an approved, secure site.~~
~~All backups will take place between the hours of 8:00pm and 5:00am. This time-frame has been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the IT Department so that exceptions or alternative arrangements can be made.~~
~~Incremental backups (only files changed since the last backup) will be performed daily, Monday through Friday.~~
~~A full backup will be performed each Friday, beginning at 8:00pm and continuing through Sunday at midnight, or until all servers have been fully backed up. These backups will be stored on site, on disk, and moved to off-site weekly.~~
~~A full backup will be performed at the end of each month. This backup will be backed up to a predetermined off-site location for permanent storage.~~
~~All server backups performed logged in the backup server logs immediately upon completion. All logs will be reviewed and monitored for successes and/or failure.~~
~~If, for some reason, the backup cannot be completed, is missed, or crashes, then it must be completed manually the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails more than one day in a row, a support ticket must be opened with the system vendor and resolution documented.~~

~~6. Managing Restores~~

Backup Schedule/Strategies

- Backups are conducted automatically using an approved Backup system.
- Depending on the criticality of the server/system, incremental backup snapshots are taken every 2 hours, every 4 hours, every 8 hours, daily, or weekly. This interval is defined and documented in the backup system at the time the server is built.
- The backup strategy is defined using the best practice of a 3-2-1 strategy: where the organization shall maintain three copies of the data, in two different locations, with one copy of the data off-site and air-

gapped.

- Incremental data backup snapshots shall be taken first to the backup data appliance and retained for a minimum of 30 days.
- Twice weekly, the backups shall be copied to a hardened NAS appliance stored in TR8. These are defined as cold data copies.
- Once weekly, the backups shall be copied to an Archive Disk and stored in TR4, air-gapped.
    - At least every other month, the Archive Disks shall be rotated to the defined off-site secure storage location. At this time, the off-site storage location is maintained in a Safety Deposit Box at South Ottumwa Savings Bank in the Church St location in Ottumwa, Iowa.
    - One of the Archive Disks in the off-site storage location shall be kept for a minimum of 12 months as a long term retention backup copy.
- Backup data shall be encrypted while at rest according to the current **Encryption Standard**.
- Information Technology staff will verify that system backups are successful on a daily basis using daily reporting and log analysis.
    - Anomalies and/or backup failures will be corrected promptly

Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential to regularly test one's ability to restore data from its storage media.

~~A. All daily/weekly backups must be tested at least once every 6 months to ensure that the data they contain can be completely restored.~~

~~B. All monthly tapes must be tested at least once every 12 months to ensure that the data they contain can be completely restored.~~
~~Data will be restored from a backup if:~~
~~There is an intrusion or attack.~~
~~Files have been corrupted, deleted, or modified.~~
~~Information must be accessed that is located on an archived backup.~~
~~In the event a data restore is desired or required, the following policy will be adhered to:~~

~~C. The individual responsible for overseeing backup and restore procedures is approved personal with the IT department. If a user has a restore request, they can contact IT department by calling x4299, or sending an e-mail to it@daviscountyhospital.org.~~

~~D. In the event of unplanned downtime, attack, or disaster, consult Davis County Hospital's Disaster Recovery Plan for full restoration procedures.~~

~~E. In the event of a local data loss due to human error, the end user affected must contact the IT Department and request a data restore. The end user must provide the following information:~~
~~Name.~~
~~Contact information.~~
~~Name of file(s) and/or folder(s) affected.~~
~~Last known location of files(s) and/or folder(s) affected.~~
~~Extent and nature of data loss.~~
~~Events leading to data loss, including last modified date and time (if known).~~
~~Urgency of restore.~~

~~F. Depending on the extent of data loss, will determine the amount of time required to recover. Backups must be retrieved by the server administrator or designee. If backups are offsite and the restore is not~~

~~urgent, then the end user affected may be required to wait up to 24 hours for a time- and cost-effective opportunity for the backups to be retrieved.~~

~~G. If the data loss was due to user error or a lack of adherence to procedure, then the end user responsible may be required to participate in a tutorial on effective data backup practices.~~

- ~~**Backup Schedule and Media Management**~~
  - ~~Backup Strategies~~
    - ~~All backup data will be encrypted at rest~~
    - ~~A backup procedure will be performed periodically which facilities a snap shot of each server profile for "quick" recovery purposes.~~
    - ~~A full system backup will be performed as required~~
    - ~~A differential (daily changes) backup will be performed on a daily basis to both the backup unit and replicated to a secondary archive media.~~
- ~~**Verification**~~
  - ~~Information Technology personal will ensure that the system backups are successful on a daily basis using logs~~
  - ~~File recovery tests will be performed annually in the event no requests for data restores have been received~~
  - ~~"Bare Metal" server restoration test(s) shall be performed annually in a calendar year, in the event no server restorations were needed during a 12 month period.~~

- All backups shall be tested at least annually to verify the data is restorable. Ideally, this is determined by randomized selection of asset to recover. If, during the course of normal operations is becomes necessary to restore data, this shall constitute a successful test.
- "Bare Metal" server restoration test(s) shall be performed annually in a calendar year, in the event no server restorations were needed during a 12 month period.
- Data will be restored from a backup if: There is an intrusion or attack, Files have been corrupted, deleted, or modified, or information must be accessed that is located on an archived backup.
- The individual responsible for overseeing backup and restore procedures is approved personal in the IT department. If a user has a restore request, they can contact the IT department by calling x4299, or sending an e-mail to it@dchc.org with the details of the restore request. Data will we restored using current support SLA's.
- In the event of unplanned downtime, attack, or disaster, consult Davis County Hospital & Clinic's Disaster Recovery Plan for full restoration procedures.

Cloud Hosted Applications

For defined cloud hosted applications including the core EHR systems, data backups and strategies shall be ~~maintaned~~maintained by hosting vendors per contract/agreement.

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
CEO	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Current Status: *Pending*	**PolicyStat ID:** *10512473*

Davis County HOSPITAL & CLINICS

An Affiliate of MERCYONE℠

Origination:	*06/2010*
Effective:	*Upon Approval*
Last Approved:	*N/A*
Last Revised:	*10/2021*
Next Review:	*2 years after approval*
Owner:	*Chris Hickie: Information Technology*
Policy Area:	*Information Technology*
Standards & Regulations:	
References:	
Applicability:	*Davis County Hospital*

Social Networking Procedure

PURPOSE:

Davis County Hospital & Clinics employees that contribute to or through any form of social media ~~(~~including but not limited to, text messaging, instant messaging (IM), chat rooms, Internet forums, etc.~~)~~ are impacting their personal image and potentially impacting Davis County Hospital & Clinics. This procedure applies to all employees when using social media while at work or anywhere else, when the employee's affiliation with Davis County Hospital & Clinics is identified, known or presumed.

~~Davis County Hospital is committed to ensuring the privacy and security of information regarding patients, residents, medical staff members and employees, as well as information about Davis County Hospital. This Policy is not intended to interfere with rights under federal or state law nor restrict employees' rights under the National Labor Relations Act ("NLRA"). Nothing in this policy or any other applicable policy shall discourage or interfere with employee whistle-blower protection rights under the NLRA. Specifically, employees are permitted to use social media and will not be disciplined or discharged for using social media for protected concerted activity.~~

Davis County Hospital & Clinics is committed to ensuring the privacy and security of information regarding patients, residents, medical staff members and employees, as well as information about Davis County Hospital & Clinics. This Policy is not intended to interfere with rights under federal or state law nor restrict employees' rights under the National Labor Relations Act ("NLRA"). Nothing in this policy or any other applicable policy shall discourage or interfere with employee whistle-blower protection rights under the NLRA. Specifically, employees are permitted to use social media and will not be disciplined or discharged for using social media for protected concerted activity.

PROCEDURE:

SOCIAL NETWORKING

Social Media is primarily Internet-based methods of networking using web-based tools to communicate widely, quickly and easily for the purpose of sharing information (public or private), searching for information, and communicating with others. Examples of social media include, but are not limited to Facebook, ~~MySpace,~~ Twitter, YouTube, LinkedIn, podcasts, blogs, message boards, wikis, text messaging, virtual worlds, chat rooms, and other online group discussion forums or social networks. This includes anything published on the

Internet or ~~DCH~~DCHC Intranet.

Employee using their home/personal computer and communication devices should be aware of guidelines and expectations regarding social networking when employed with Davis County Hospital & Clinics. The following apply to all social networking activity regardless of if the employee is at work or at home.

1. When employees create their own blogs, comment on a blog, use Facebook/~~My Space~~Twitter and/or contribute to or through any other form of social media (text messaging, instant messaging, chat rooms, Internet forums, electronic mailings, etc) they are impacting their personal image and potentially impacting Davis County Hospital & Clinics. Davis County Hospital & Clinics cannot prevent employees from participating in social networking outside of the workplace. However, Davis County Hospital & Clinics is committed to ensuring the privacy and security of information regarding patients, residents, medical staff members and employees, as well as information about Davis County Hospital & Clinics.
2. **Employees shall not use Social Media for the purpose of:**
   - Disclosing ~~DCH~~DCHC's clients', patients', or vendors' confidential information, PHI, or ePHI.
   - Using the Hospital's electronic communication system to create send, receive, access, download, display, or print material that is harassing, illegal, sexual, false, threatening, explicit, obscene, offensive, defamatory, discriminatory , or disparaging of others (patients, clients, vendors, competitors, fellow employees or care provided by an employee, physician, health care practitioner) based upon their race, national origin, gender, age, disability, religion, pregnancy, military status, or job position.
   - When using social media, employee must not expressly or implicitly represent that his/her views are the views of ~~DCH~~DCHC unless he/she is expressly authorized to make such representation by Senior Team. When employee's use of social media is not aligned with the position of ~~DCH~~DCHC, the employee may be asked to remove any reference to his/her employment or affiliation with ~~DCH~~DCHC.
   - ~~Employees photographing any individuals (including, but not limited to, patients or unidentified individuals in the background) or physical structures, must obtain written authorizations from the individuals and from the Marketing Leader for physical structures photographed (hallways, artwork, offices, etc) in DCH, if such is going to be posted on any social media site. It is possible that PHI and ePHI as well as confidential information may be disclosed in photographs, thereby violating HIPAA. "Photograph" may include, but not be limited to, videotape, videodisc, podcast, webcast, blog, digital image and any other mechanical or electronic means of recording or producing visual or audio recordings or images.~~Employees photographing any individuals shall comply fully with Administration policy 'Photographic Guidelines'.
   - ~~DCH~~DCHC issued email accounts shall not be used for non-work related social media activities or notification.
3. Social networking activities cannot interfere with work commitments. Employees are prohibited from participating in personal social networking activities while on work time.
4. If an employee's on-line profile indicates he/she works for Davis County Hospital & Clinics, then the activity on that site is associated with Davis County Hospital & Clinics.
5. If an employee's friends or other individual knows the employee works for Davis County Hospital & Clinics, the employee's online presence reflects the organization. The employee should be aware of their actions captured via images, postings, or comments.

6. Social networking may inadvertently or un-intentionally reveal confidential or proprietary information. All employees must abide by Davis County Hospital & Clinics's Confidentiality Agreement that is signed upon employment.
7. There should be no reference to a patient/client at any time. Patient information is confidential. Even if a patient's name is not used, a reader of the site may be able to determine who is being referenced through the exchange of dialogue.
8. Employees must remember that any time they write a comment on a social network account, the employee is recording their thoughts into a potential permanent record. Although the employee may feel they are just "chatting", others can view the employee's comment(s), print the comment(s) or forward the comment(s) to other individuals. These comments could be disparaging to ~~DCH~~DCHC, the employee and others, which is unacceptable.
9. Davis County Hospital & Clinics logos cannot be visible in pictures or documents viewed on social network accounts.
10. Pictures of the work environment, co-workers in the work environment, patients/clients and/or patient family members are not permitted on social network accounts, even if the patient and/or patient family gives permission.
11. Employees must not use social networking accounts to harass, threaten, libel, malign, defame, disparage, retaliate or discriminate against co-workers, managers, or patients/clients.
12. Employees cannot make disparaging remarks regarding Davis County Hospital & Clinics, competitors, other organization in which ~~DCH~~DCHC has affiliations, competing facilities, or other such organizations on social network accounts.
13. Employees are discouraged from allowing patients and family members to post their (employees) phone on the patient/family member's web site. Once the employee provides permission, they no longer can control what is stated on the web site about the employee.

    In addition to the procedures outlined above,

    - Hiring Leaders shall not access social media sites during the recruitment process or after employment nor use inappropriate information inadvertently obtained about a specific individual applicant in the hiring decision process or for disciplining a current employee. Only Human Resources may lawfully and appropriately access and evaluate such information as part of the recruitment or disciplinary process.

14. **Employees shall use Social Media for the purpose of**:
    - social media is to foster lawful, positive, and accurate representations of ~~DCH~~DCHC in all social media,
    - to build and maintain positive relationships with key stakeholders, which may include: employees, patients, customers, physicians, family members, community leaders, religious leaders, potential employees, the general public, vendors/partners, etc., and
    - to represent positive employee participation in social media, including ~~DCH~~DCHC-hosted social media and in non-~~DCH~~DCHC social media when an employee's affiliation with ~~DCH~~DCHC is identified, known, or presumed.
    - to instill responsibility for using ~~DCH~~DCHC Information and IT Assets in a professional and ethical manner,

- to safeguard and protect ~~DCH~~DCHC Information and IT Assets, and to comply with applicable laws and regulations.
- Limited, occasional, or incidental personal use of IT Assets for electronic mailing as permitted, provided that it is conducted in a manner that does not negatively affect work performance, and is in compliance with this policy.

MONITORING

To ensure that the use of the electronic communication systems are consistent with Davis County Hospital & Clinics's legitimate business interests, authorized personnel of the Davis County Hospital & Clinics may monitor the use of any and all electronic equipment from time to time.

~~DCH~~DCHC regularly monitors the User's access and use of ~~DCH~~DCHC IT Assets and inspects the information that a User receives, transmits, downloads, or maintains on the IT Assets. ~~DCH~~DCHC may review any and all User files, information or messages (including those that may appear to be deleted), electronically scan the User's email and items viewed on Internet sites, and personal email when accessed and/or stored on ~~DCH~~DCHC IT Assets. ~~DCH~~DCHC may use various technologies or software to block User's access to certain information which ~~DCH~~DCHC deems inappropriate.

The User does not have privacy rights in connection with his/her use of ~~DCH~~DCHC Information and IT Assets. ~~DCH~~DCHC reserves the right, in its sole discretion, to review, audit, intercept, or take any action necessary regarding the User's Internet and email use, and/or the transmission, receipt, or storage of information on or from ~~DCH~~DCHC IT Assets to ensure that ~~DCH~~DCHC information and IT Assets are used in compliance with the User's job functions, this policy, and applicable laws and regulations.

Complaints may be received regarding your on-line conduct including complaints such as harassment, release of confidential information or other inappropriate behavior. ~~DCH~~DCHC will review any complaint of this nature and investigate the complaint, including review of the on-line postings or other information contained on any public or openly available site or which are provided to ~~DCH~~DCHC by others.

Any violation of this social networking procedure, even off-duty, will result in corrective action up to and including termination.

Employees shall receive notice of policy and may receive periodic education and training on its application and use.

Related Policies:

- Acceptable Use
- Photographic Guidelines

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Senior Leader	Veronica Fuhs: CEO - DCHC	pending
	Chris Hickie: Information Technology	10/2021

Applicability

Davis County Hospital

Accounting Biennal Policy Review
2021

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Accounts Payable - Entering Invoices		X				
Check Request		X				
Issuing Memorial Checks to Employees for Bereavement Recognition		X				
Purchase Orders		X				
Receiving Payments by Mail & Stamping Checks		X				

Infection Prevention Biennial Review
2021

Title	New	No changes	Revised Statement	Revised Procedure	Retired	Comments
Air-Mate – High Efficiency Particulate Filtration System				x	x	Changed from Policy to SOP. Have more than one brand of PAPR so changed from brand specific to Positive Airway Pressure Respirator System and updated procedure to reflect manufacturer guidelines for use
Antibiotic Guidelines			x			Added "in coordination with pharmacist"
Antibiotic Resistant Bacteria		x				
Bed Bugs					x	Not an IP policy-EVS policy
Bioterrorism Readiness for Infection Prevention				x		Removed Caitlin Pedati and just listed IDPH
Cleaning and Decontamination of Blood and Body Fluid Spills Procedure		x				
Cleaning of the Ice Machine		x				
Communicable Disease Control				x		Updated link to epi manual
Computer Keyboard Cleaning		x				
Detection, Treatment and Prevention of Transmission of Lice - Head, Pubic and Body		x				
Disposal of Infectious Waste		x				
Employee Health Program				x		Not an infection prevention policy-Employee health
Employee Laboratory Testing					x	All aspects that are still utilized are in other policies
Employee Reaction to Latex		x				
Environmental Services and Cleaning		x				
Epidemic Contagious Airborne Diseases (ECAD) Plan		x				
Exposure Control Plan - Abbreviations					x	not found in policystat
Exposure Prone Invasive Procedures and Preventing Transmission of HIV and Hepatitis B and C to Patients		x				
Guidelines for Determining the Presence of Healthcare Associated Infections (HAIs)		x				
Guidelines for Infection Prevention in Supplying of Hospital Linen		x				
Hand Hygiene		x				
Hepatitis B Vaccination Program		x				
HIV testing					x	Part of bloodborne pathogen plan
Hospital Approved Disinfectants		x				
Ice Distributing Procedure		x				
Infection Control Risk Assessment for Construction		x				
Infection Control Risk Assessment for Construction- form		x				
Infection Prevention for Medical Imaging Services		x				
Infection Prevention Policies for Laundry Department		x				
Infection Prevention Policies for the Emergency Room		x				
Infection Prevention Policies in Laboratory		x				
Infection Prevention Policies Relating to Blood Bank		x				
Infection Prevention Procedures for Physical Therapy Department					x	Not an IP policy-PT/OT policy
Infection Prevention Reporting		x				
Infectious Disease Surveillance, IC 02.03					x	Covered in other policies-duplicate
Initiation of Isolation and Precautions				x		Added covid-19
Laryngoscope Blade Disinfection/Sterilization					x	Changed to an SOP
Linen Handling					x	Changed to an SOP
Materials Management Infection Prevention		x				
Mopping of Resilient Floors					x	not found in policystat
Notification of Persons Handling a Deceased Patient		x				
Notifying Emergency Services Personnel of Infectious Disease Potential or Exposure		x				
Open Medication Vials, Ampules, Irrigating Solutions, and Oral Liquid Medications		x				
Personal Protective Equipment		x				
Pharmaceutical Cache Dispensing System		x				
Pharmacy Infection Prevention		x				
Positive Results of Blood Borne Pathogen Testing		x				
Preoperative Skin Antisepsis		x				
Principles of Sterile Technique		x				

Infection Prevention Biennial Review (con't)

Title	New	No changes	Revised Statement	Revised Procedure	Retired	Comments
Protocol for Managers of Employees with Latex Allergy		x				
Quality Assurance Program Infection Prevention Surveillance Plan		x				
Release of Employee Health Files		x				
Respiratory Therapy Department Equipment Care					x	Changed to SOP
Reuse of Single Use Packaged Medical Devices		x				
Routine Cleaning of Carpet					x	Not found in policystat
Scabies Diagnosis and Treatment		x				
Shampooing Carpet					x	Not found in policystat
Sharps and Needle Use and Disposal		x				
Specimen Collection		x				
Standard Precautions		x				
Surgery Classifications		x				
Surveillance		x				
Surveillance Program Cultures		x				
Suspected IV Associated Infection		x				
Transporting Isolation Patients		x				
Use of the Isolation Room		x				

Plans	New	No changes	Revised Statement	Revised Procedure	Retired	Comments
Bloodborne Pathogens Exposure Control Plan		x				
Respirator Protection Plan				x		Removed medical evaluation form
Tuberculosis Exposure Control Plan		x				

Information Technology
2021

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Acceptable Use Policy				x		Changed to DCHC. Removed redundant comments regarding using mobile devices in auto. Fixed formatting for Incidental Use section
Asset Decommission Procedure			x			Changed to DCHC.
Asset Management Policy			x			Changed to DCHC.
Authentication Standard Procedure			x			Changed to DCHC.
Contingency Planning			x	x		Changed to DCHC and other minor nomenclature references. Removed all references to ICE Technologies. Removed outdated policy number from heading. -Planning to re-work this within next 12 months and merge with DR policy
Disaster Recovery Planning			x	x		Changed to DCHC and other minor nomenclature references. Removed outdated policy numbers and references to older policy names from heading and procedure.-Planning to re-work still within next 12 months and merge with Contingency policy
Electronic and Digital Signatures					x	Retiring this outdated policy in consultation with HIM Mgr. Acceptable Use and Identity and Access Management Policy are much more robust and cover the authentication portions of this applicability using electronic signatures.
Encryption Management Policy			x			Changed to DCHC.
ER Provider Training			x			Changed to DCHC.
HIPAA Facility Security Plan					x	This policy is being retired as all of these items have been addressed in much more robust policies over the past four (4) years. See 'Information Security Policy' for similar reference.
Identity And Access Management Policy			x			Changed to DCHC.
Information Classification And Management Policy			x			Changed to DCHC.
Information Security Policy			x	x		Changed to DCHC. Added statement and procedure regarding the *Waivers* process.
IT Security Incident Response Plan/Procedure				x		Changed to DCHC. Updated some procedural information and added supply chain attack, added new logging sources, updated network isolation picture, updated call tree for response team. Added six (6) new supplemental security incident specific playbooks for potential use.
IT Systems Account Termination Procedure				x		Changed to DCHC. minor procedural/systems changes.
Patch Management					x	Policy being retired in favor of more robust Vulnerability Management Policy (New)
Physical and Environmental Security			x	x		Heavy re-working of this policy to modernize the physical security requirements consistent with current practices. Several edits made to controls including entry controls, access, hardware/software modifications, moving equipment, and all base physical standards.
Risk Analysis Plan					x	Retired - merging this with re-worked Risk Assessment Procedures policy
Sanctions			x			minor clarification in statement and remove outdated policy number in heading
Security Cameras				x		Added exception statement to #17 regarding official use of video.
Risk Assessment Procedures (Formerly, Security Management and Assessment)			x	x		Changed Title to Risk Assessment Procedures, adopted moderinized procedures for managing risk assessments at the organization.
Security Training And Awareness Policy			x	x		Changed to DCHC. Minor nomenclature change.
Server Backup			x	x		Changed to DCHC. Several procedural changes to align with new backup, retention, and testing strategies and technology enhancements over the past year.
Social Networking Procedure			x	x		Changed to DCHC. Nomenclature changes. Edited references to photos to now point to Photographic Guidelines admin policy.
Vulnerability Management Policy	x					New, more robust policy which supercedes the retired Patch Management Policy.

Medical Associates Biennial Review
2021

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Administrative Structure		X				HS
Bladder Scanner		X				
Bomb Threat		X				
Chaperone Policy				X		added "and clinics" to second paragraph
Cleaning and Sterilization of Instruments		X				
Cleaning of the Clinic		X				
Clinic Charges and Billing				X		added "and clinics" to #2 under financial arrangements and all other references to Davis County Hospital, charge entry made by the clinic HIM clerk removed under recording charges and payments
Clinic Management				X		changed scheduling hours to 8 - 5 M- F
Clinic Office Schedule				X		corrected hours for Dr. Settles, Beverly Oliver, ARNP, Dr M Graeff, Haleigh Skaggs, ARNP, Dianne Knapp, ARNP, and added Megan Whisler Peds ARNP and removed Dr. Sanchez
Clinic Operating Hours				X		updated schedule to remove late night hours and added "and Clinic" where needed
Clinic Staffing				X		added CMA to clinic nurse
Compliance with Federal, State and Local Laws		X				
Concurrent Review of Patient Care		X				
Confidentiality of the Clinical Record		X				
Consent to Treatment/Informed Consent		X				
Disclosure of Ownership		X				
Documentation		X				
Drugs and Biologicals		X				
Emergency Care During Clinic Hours		X				
Emergency Drugs				X		It was also evaluated that antiemetics and antiseizure medications are not needed are not kept in the clinic. added to #4
Fire Safety				X		changed cafeteria to in the grassy area south of the building in #12
Governing Body		X				HS
Guidelines for Medical Management		X				
Hand Hygiene		X				
Human Resources		X				
In-service Training/Continuing Education		X				
Infection Prevention				X		added and clinic's
Injection Administration		X				
Laboratory Services		X				
Location of Clinic		X				
Management of Infectious Waste		X				
Management of Pain Prescriptions		X				
Medical Director				X		removed: Annually reviews clinic written policies and makes recommendations for revision.

Medical Associates Biennial Review (con't)

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Medical Record Audit		X				
Medical Record Content		X				
New Vs. Established Patient Visits		X				
No Show Appointments		X				
Non-Medical Emergencies		X				
Normal Daily Routine of the Clinic				X		changed to match Cerner workflows
Organizational Chart				X		updated org chart
Orientation of Staff		X				
Oxygen Therapy		X				
Parental Consent		X				
Patient Assistance Plan		X				
Patient Dismissal		X				
Patient Health Records				X		added and clinics
Patient Medical History		X				
Patient Right and Responsibilities		X				
Performance Improvement		X				
Performing an Electrocardiogram				X		correct spelling in outpatient process and made copy plural in 1st bullet point after
Pharmacy Review		X				
Physical Plant Safety		X				
Physician Responsibilities		X				
Policies and Procedures		X				
Preventive Maintenance		X				
PRN Clinic Staff				X		removed the prn staff will sign off on department meeting notes
Program Evaluation		X				
Protection of Health Information		X				
Provider Treating Self and Family Members		X				
Provision of Rural Health Clinic Services		X				
Refrigerators at the Clinic		X				
Release of Information		X				
Retention and Storage of Medical Records		X				
Review of Clinic Operations				X		annual was changed to every two years
Review of Health Care Policies		X				
Scope of Care by Midlevel Practitioner		X				
Security and Confidentiality of the Health Record		X				
Storage of Medications				X		changed multi dose vials to expire in 28 days in place of 30 to match pharmacies policy
Tornado Alert Plan/Severe Thunderstorm		X				
Vaccine and Medication Storage and Handling		X				
Vaccines for Children		X				
RHC EOP				X		added "and clinics" where needed and "vetted" to volunteers

Senior Life Solutions Biennial Review
2021

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Access to Services		X				
Admission Criteria		X				
Admission Procedure		X				
Advance Directives		X				
Assessments				X		The eval of the provider must be in the pt. record in 5 business days. Not 3
Certification of Medical Necessity		X				
Competency of Care Providers		X				
Conduct to Minimize Violence		X				
Confidentiality		X				
Confidentiality of Information - General Issues		X				
Confidentiality Policy		X				
Conflict of Interest		X				
Copyright OHPS		X				
Corporate Compliance Plan		X				
Discharge Planning		X				
Disclaimer OHPS		X				
Documentation		X				
Documentation and the Use of Abbreviations, Acronyms and Symbols		X				
Emergencies - Medical		X				
Employee Dress Code		X				
Employee Health Exam		X				
Employee Personnel Records		X				
Exclusion Criteria		X				
Fair Hearing Policy				X		Fixed grammar error
Falls Precautions		X				
Family Participation and Education		X				
Fire Procedures for SE Clinic		X				
Follow-Up		X				
Food Service		X				
Forms		X				
Infection Control		X				
Inservices		X				
Legibility of Medical Record Documentation		X				
Liaison with Referral Source		X				
Management of Assaultive Behavior		X				
Master Treatment Planning and Patient Care		X				
Medical Records and Reports				X		

Senior Life Solutions Biennial Review (con't)

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Medical Records Content				X		
Medical Records Storage				X		removed fireproof storage facility
Med Staff Reappoint. And renewal of Clinical privileges		X				
Medication Self-Administration		X				
Mission Statement		X				
Organizational Structure		X				
Patient Complaints		X				
Patient Orientation		X				
Patient Review of Medical Records		X				
Patient Rights		X				
Patient Satisfaction Survey		X				
Performance Evaluations		X				
Performance Improvement Program/Performance Improvement Plan		X				
Philosophy		X				
Photographing/Videotaping Patients		X				
Program Content		X				
Program Overview		X				
Program Violations - Patient Use of Drugs or Alcohol		X				
Protection and Availability of Medical Records		X				
Recognizing and Reporting Dependent Adult/Elder Abuse/Neglect				X		Added caretaker and it's definition
Referral Process and Screening		X				
Requirements for the Telepsychiatry Process		X				
Resolution of Potential Conflict with Staff Member's Cultural/Ethical/Religious Belief System		X				
Review of Medical Record		X				
Risk Management		X				
Scope of Service				X		Updated hours of operation from 8:30 to 8:00 to 4:30
Staff Meetings		X				
Staff Rights and Ethical Dilemmas in Patient Care		X				
Staffing		X				
Standards of Excellence		X				
Suicide Assessment		X				

Senior Life Solutions Biennial Review (con't)

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Suspected Patient Abuse/Neglect		X				
Tarasoff Warning		X				
Temporary Privileges		X				
The Privileging process		X				
Therapeutic Milieu		X				
Tornado Procedures for SE Clinic		X				
Transfer for Admission to Inpatient Psychiatric Setting		X				
Valuables - Patients' Personal Belongings/Contraband		X				
Verbal and Written Orders - General		X				
Volunteers		X				

Trauma
2021

Title	New	No Changes	Revised Statement	Revised Procedure	Retired	Comments
Medical Provider Competency for Trauma Care		X				Changed all trauma reviews to annual
Organ and Tissue Donation Protocol		X				
Rib Fractures				X		added reason for not transferring patients with multiple rib fractures of "Called Level I or II trauma center and admission was declined"
Spinal Precautions		X				
Suspected Brain Death		X				
Trauma Organizational Structure		X				
Trauma Performance Improvement and Patient Safety (PIPS) Plan		X				
Trauma Service		X				
Trauma Team Activation		X				
Trauma Transfer Protocol		X				