STATE OF COLORADO)
) ss
COUNTY OF ROUTT)

RESOLUTION #2022-_____

A RESOLUTION READOPTING A ROUTT COUNTY SECURITY POLICY UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 AND THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

Recitals

1. On May 12, 2015, the Board of County Commissioners of Routt County (the "Board") adopted a Statement of Policy of Routt County, Colorado, Concerning Security Under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act (the "Security Policy"); and

2. The Board desires to readopt the HIPAA Security Policy; and

3. On May 24, 2022, the Board conducted a public hearing following notice as required by law, to consider the adoption of this resolution and the attached HIPAA Security Policy; and

4. The Board finds that it is in the best interests of the citizens of Routt County that this resolution and the attached HIPAA Security Policy be readopted.

NOW, THEREFORE, BE IT RESOLVED by the Board of County Commissioners of Routt County, Colorado that:

A. The attached Routt County Security Policy Under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act is hereby adopted to be effective May 24, 2022.

B. The Policy may be revised to reflect its policy number once assigned without further need for adoption by resolution.

ADOPTED this 24th day of May, 2022.

BY THE BOARD OF COUNTY COMMISSIONERS OF ROUTT COUNTY, COLORADO.

M. Elizabeth Melton, Chair

Vote:	M. Elizabeth Melton	Aye	Nay	Absent
	Timothy V. Corrigan	Aye	Nay	Absent
	Tim Redmond	Aye	Nay	Absent

ATTEST:

Jenny L. Thomas
Routt County Clerk

STATEMENT OF ROUTT COUNTY SECURITY POLICY

Under the

Health Insurance Portability and Accountability Act of 1996

July 2013

TABLE OF CONTENTS

Statement of Routt County Security Policy Under the
Health Insurance Portability and Accountability Act of 1996

This statement of security policy is adopted by the Board of County Commissioners of Routt County ("the Board") in order to comply with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Security Rule (45 CFR Part 160 and Part 164, Subparts A & C). The Security Rule requires adherence to certain standards for the safeguarding of electronic protected health information ("EPHI"), as well as four other standards defined in 45 CFR §§ 164.314 and 164.316. This policy addresses §§ 164.306, 164.308, 164.310, 164.312, 164.314, and 164.316 of HIPAA as it applies to Routt County ("the County").

INTRODUCTION AND INFORMATION FOR ALL EMPLOYEES

What is HIPAA?
In 1996, Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA") in order to simplify and standardize health care administrative processes. As part of this Act, Congress established standards and requirements to protect the integrity, confidentiality, and availability of health information.

How Does HIPAA Impact the County?
While much of HIPAA addresses the health care industry, sections of the Act provide standards and requirements for organizations that process health information as part of their business functions. All entities that create, store, or process protected health information ("PHI") must comply with these standards and requirements. Because parts of the County process PHI, the County must comply with those provisions of HIPAA.

On March 30, 2004, the Board adopted a policy regarding the County's compliance with a section of HIPAA called the Privacy Rule. This privacy policy dealt with the County's overall compliance with the PHI requirements of HIPAA. In the policy, the Board designated the County as a "hybrid entity" for HIPAA purposes. A hybrid entity is an entity whose main function does not involve providing health care services but does involve processing PHI as part of its business functions. Hybrid entities must identify all "covered entities" that process PHI and ensure that these covered entities comply with HIPAA requirements and standards. In the County's policy regarding the HIPAA Privacy Rule, the Board identified the Human Resources Department (HR) as the only covered entity and designated the HR Director as the "Privacy Official." In 2009, the Board identified the Department of Human Services (DHS) as an additional covered entity and designated the Director of DHS as the Privacy Official for DHS.

In addition to the Privacy Rule, there is a section of HIPAA called the Security Rule which specifically focuses on the safeguarding of EPHI. Because DHS and HR process EPHI, the County is required to comply with HIPAA Security Rule requirements and standards specific to the safeguarding of EPHI. The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 was introduced as an effort to speed the use of electronic health records while providing means of protecting PHI. On January 17, 2013, the U.S. Department of Health and Human Services issued an omnibus rule to enhance a person's privacy rights, provide

individuals new rights to obtain their health information, and to strengthen the government's ability to enforce HITECH privacy and security protections. This document amends the County's policies and procedures adopted to comply with the HIPAA Security Rule.

What Type of Health Information is Considered PHI?
Though the definition of PHI in HIPAA is quite convoluted, PHI is basically defined as any information about your past, present or future medical or mental health condition that is associated with information that can uniquely identify you (*e.g.*, name, address, age, sex, phone number, email address, employee ID, social security number, medical record number).

What is EPHI?
EPHI is just PHI that is created, received, stored, or maintained, processed and/or transmitted electronically via electronic computing devices:

- Electronic media includes, but is not limited to, computer diskettes, hard drives, backup tapes, memory sticks, thumb drives, CDs, and DVDs
- Electronic computing devices include, but are not limited to, workstations, servers, PDAs, smartphones, mobile computational devices, network equipment, networks, dial-modems, Email systems, and websites

What Are Examples of EPHI?
Because EPHI is just electronic PHI, examples of EPHI include (but are not limited to) electronic information that uniquely associates an individual with the following information:

- Patient identifiers, such as address, date of birth, date of death, Social Security number
- Dates of service, such as date of admission, treatment, or discharge
- Medical records, reports, test results, billing records, appointment dates
- Past or present medical or mental health conditions
- Past or present leave requests (FMLA, sick leave donation requests, other requests for leave containing health or medical information)
- Past or present release forms from doctors

How Do the HIPAA Security Rule Policies and Procedures Affect Me?
Though much of the County's Security Rule policies and procedures are directed to employees in HR, DHS, and the Information Systems Department (IS), all County employees are required to comply with reasonable safeguards to protect EPHI everywhere at the County.

Because HR and DHS are the only covered entities under HIPAA, only DHS and HR employees shall use the County computer-based systems for creating, receiving, storing, or maintaining, processing and/or transmitting EPHI. ***Therefore, no other employees will be allowed to use County computer-based systems for creating, receiving, storing, or maintaining, processing and/or transmitting EPHI.***

Thus, the following specific restrictions apply to all non-DHS and HR employees:

1) You cannot use County computers (or any other computer-based resource) to create, manage, or save electronic documents (such as Microsoft Word, Excel or PowerPoint

files, "text files," PDF files, or emails) that contain PHI about yourself or any other person.

2) You cannot use any County electronic media (including but not limited to CDs, DVDs, diskettes, computer disk drives, thumb drives, digital camera memory, or media players) to store PHI about yourself or any other person.

3) You cannot send emails containing PHI about yourself or any other person to anyone inside or outside the County using the County's email system.

4) You cannot use your personal email account (including but not limited to Hotmail, Yahoo, Gmail, or any other external email provider) to send emails containing PHI about yourself or any other person to County employee email accounts.

5) You cannot use any County computer-based transmission system (such as FTP, Instant Messaging, HTTP, or RSS) to transmit PHI about yourself or any other person to anyone inside or outside the County.

One HIPAA Security Rule requirement states that each employee who accesses the County's computer-based resources must have a unique name and/or number (userid) for identifying and tracking user activity. The Security Rule also requires each employee at the County to comply with the County's HIPAA Security Rule policies and procedures. Therefore, the County will hold all employees accountable for all actions and activities conducted under their userids.

In order to uniquely identify all employees who access the County computer systems, networks and applications, the County must guarantee that only one employee is using each unique userid. ***Therefore, County policy prohibits employees from sharing their userids and passwords with ANY other person except for IS employees as part of daily support functions.*** In addition, County employees will be accountable for protecting their userids and passwords from accidental or intentional disclosure to anyone inside and outside the County.

Thus, the following apply to <u>all</u> employees:

1) You cannot reveal the userid and associated password you use to log into your computer to any other person inside or outside the County except IS staff members providing daily support activities.

2) You cannot reveal the userid and associated password you use to log into any County application to any other person inside or outside the County except IS staff members providing daily support activities.

3) If you must write down your userid and password to remember it, you must record and store this information where it cannot be easily obtained or accessed by others.

4) You will be held responsible for all actions and activities conducted under your userid on any County system or application if you fail to comply with these policies.

How Can I Communicate PHI To the HR Office?

You may communicate PHI information to HR employees through any non-computer-based means such as standard mail, fax, phone call, or physically taking the information to the HR office. You can use your own personal computer-based resources to create and store PHI as long as you transfer the information to HR employees only through non-computer-based means.

HIPAA Security Standards & Implementation Matrix
(Appendix A of the Security Rule)

Standards	Sections	Implementation Specifications (R) = Required (A) = Addressable	
Administrative Safeguards			
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R)	Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure (A) Termination Procedures (A)	
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)	
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)	
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)	
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)	
Evaluation	164.308(a)(8)	(R)	
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement (R)	
Physical Safeguards			
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)	
Workstation Use	164.310(b)	(R)	
Workstation Security	164.310(c)	(R)	
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R)	Accountability (A) Data Backup and Storage (A)
Technical Standards			
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R)	Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)	
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)	
Person or Entity Authentication	164.312(d)	(R)	
Transmission Security	164.312(e)(1)	Integrity Controls (A)	Encryption (A)

Other HIPAA Requirements

Organizational Requirements			
Business Associate Contracts or Other Arragements	164.314(a)(1)	Business Associate Contracts (R) Other Arrangements (R)	
Requirements for Group Health Plans	164.314(b)(1)	Implementation Specifications (R)	
Policies and Procedures and Documentation Requirements			
Policies and Procedures	164.316(a)	(R)	
Documentation	164.316(b)(1)	Time Limit (R) Availability (R) Updates (R)	

I. § 164.306 Security Standards: General Rules

The County acknowledges the general rules defined in §164.306 as they pertain to security standards for safeguarding EPHI within the County's digital infrastructure for the County's covered entities, HR and DHS. This document is intended to define and describe the policies, procedures, practices, and solutions that will:

(1) Ensure the confidentiality, integrity, and availability of all EPHI the covered entities create, receive, maintain, or transmit.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

The County acknowledges the "flexibility of approach" as it applies to safeguarding EPHI within the covered entities as follows:

(1) Covered entities may use any security measures that allow the covered entities to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, covered entities must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to EPHI.

The County acknowledges that it must comply with the standards as provided in this section and in §§ 164.308, 164.310, 164.312, 164.314, and 164.316 with respect to EPHI by **April 21, 2006**. The County acknowledges that in regards to "implementation specifications" the following is true:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the letter "R" appears in parentheses after the title of the implementation specification in Appendix A. If an implementation specification is addressable, the letter "A" appears in parentheses after the title of the implementation specification in Appendix A.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must:

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with respect to the likely contribution to protecting the entity's EPHI; and

(ii) As applicable to the entity --

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate --

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

The County also acknowledges that in regards to maintenance of its response and adherence to the HIPAA Security rule:

Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of EPHI as described in § 164.316.

II. § 164.308 Security Standards: Administrative Safeguards

1. Security Management Process

Risk Analysis and Risk Management at the County will be an on-going process, occurring five (5) years from the last risk analysis effort, absent a change in HIPAA law or regulations or a significant incident involving a breach of privacy or security.

a. Risk Analysis

An assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI was conducted by the County in 2005 and was documented in an August 2, 2005 memo by then-Assistant County Attorney Eben Clark. Subsequently, it was determined that DHS, in addition to HR, is a covered entity under HIPAA.

b. Risk Management

A risk management plan was developed, based on the August 2, 2005 risk analysis memo, and documented in a February 28, 2006 document titled "Routt County Security Rule Risk Management Plan" by Routt County Information Systems Director, Terry Barber. The Risk Management Plan was updated in January, 2011 to address the addition of DHS as a covered entity.

c. Sanction Policy

All employees will be required to sign a statement of adherence to these HIPAA security policies and procedures as part of an amendment to the current employee handbook or as part of initial employment acceptance of all policies in the Employee's Handbook. If an employee fails to comply with these policies and procedures, it is considered a violation of County policy and is grounds for disciplinary action up to and including termination.

d. Information System Activity Review

The following information will be reviewed in regards to system activities (parentheses shows department responsible for providing the report):

(1) A monthly report listing users who accessed the HIPAA-designated subfolders under the DHS and HR folders and at what times the subfolders were accessed (IS).

(2) A monthly report on any security incidents including, but not limited to, the following:

(a) Computer viruses or spyware found on any County computer that accesses EPHI data and their impact on EPHI data (IS)

(b) A list of violations of County policies and procedures associated with HIPAA security (DHS, HR & IS)

(c) Known occurrences of unauthorized access to EPHI information (DHS, HR & IS)

(d) A list of employees who were added to or removed from the DHS, HR and Domain Administrator Microsoft Domain groups (IS).

(3) A list of the names of employees who sent emails to HR containing EPHI and the dates of the emails (IS)

(4) The Security Official will review the three IS reports monthly during an IS operations meeting, in order to identify EPHI that may have been, or is at increased risk of being, used or disclosed inappropriately. All reports will be reviewed quarterly by the appropriate Privacy Official and maintained for six (6) years.

2. Assigned Security Responsibility

The Director of IS will be considered the Security Official responsible for the development and implementation of the policies and procedures required to meet the HIPAA Security Rule for the County.

3. Workforce Security

a. Authorization And/Or Supervision

The appropriate Privacy Official (herein meaning the Privacy Official appointed for the relevant department) will determine who will have access to EPHI data secured within the HIPAA folders and subfolders located on the Annex General File Server.

b. Workforce Clearance Procedure

(1) The workforce clearance process is determined by the Privacy Officials.

(2) Any employees requiring access to EPHI must have a formal, hardcopy, signed document from the appropriate Privacy Official containing the employee's name and a statement granting the employee access to EPHI, describing any limitations for EPHI access, and including a request to the Security Official to establish the correct permissions, configurations, and software installations to allow the employee to access the EPHI data subject to any imposed limitations.

(3) One copy of the document will be kept in the Privacy Official's files and the other will be sent to the Security Official.

(4) Upon receipt of the Privacy Official's request document, the Security Official will task County IS staff to complete the request no later than one (1) week from the date of reception.

EPHI will be stored in HIPAA folders within the DHS and HR departmental folders. Sub-folders within the HIPAA folder will be unique to the user's HIPAA function and secured so only required users have access to that EPHI data.

(5) Upon completion of the work by the IS staff, the Security Official will notify the Privacy Official no later than two (2) business days after the time of completion.

(6) The Privacy and Security Officials will each keep their copy of the document within their files, along with all other related documents, for a period of six (6) years from the date the employee has left employment at the County.

c. Termination Procedures

(1) For employees who no longer require access or need more restricted access to EPHI or for employees who had access to EPHI and have left employment at the County, the appropriate Privacy Official will create a formal, hardcopy, signed document containing the following:

(a) Employee's name.

(b) Description of the EPHI access restriction or removal of access to EPHI for that employee.

(c) A request to the Security Official to remove permissions, configurations, and/or software to change or deny the employee's access to the EPHI data as requested by the Privacy Official.

(2) One copy of the document will be kept in the Privacy Official's files and the other will be sent to the Security Official within two (2) business days after the employee's termination date.

(3) Upon receipt of the Privacy Official's request document to restrict or remove access to EPHI data, the Security Official will task County IS staff to complete the request no later than two (2) business days after the date of reception.

(4) Upon completion of the work by the IS staff, the Security Official will notify the Privacy Official no later than one (1) business day after the time of completion.

(5) The Privacy and Security Officials will each keep their copy of the document within their files, along with all other related documents, for a period of six (6) years from the date the employee has left employment at the County.

d. Review Procedures

(1) A list, generated by IS, of employees having access to EPHI, including Domain Administrator security groups will be reviewed annually by the Security and Privacy Officials.

(2) This list will be initialed by both the Security and Privacy Officials and stored by the Security Official for a period of six (6) years from the date of creation.

4. Information Access Management

a. Isolating Health Care Clearinghouse Functions

The County does not conduct any Health Care Clearinghouse functions.

b. Access Authorization

See Workforce Security procedures above

c. Access Establishment Modification

See Workforce Security procedures above

5. Security Awareness & Training

a. Security Reminders

(1) All employees will be required to sign a statement of adherence to these HIPAA security policies and procedures as part of an amendment to the current HR Handbook or as part of the initial employment acceptance of all policies in the HR Handbook. If an employee fails to comply with the policies and procedures stated herein, it is considered a violation of County policy and is grounds for disciplinary action up to and including termination.

(2) HR will send an annual electronic or hardcopy notice reminding all County employees of the policies and procedures herein.

(3) HR employees will send notices to employees found to be using the County's systems to transmit or receive EPHI (see Risk Management).

(4) It is the responsibility of the Privacy Officials to train employees on what is EPHI and non-EPHI related data.

b. Protection From Malicious Software

(1) The County has implemented an enterprise-wide antivirus and anti-spyware software solution that protects all Microsoft-based computer systems from malicious software. Updates are pushed out to all machines for both software solutions at least once a day on weekdays and both software solutions "scan" all the Microsoft-based computer systems once a day on weekdays. Both software solutions provide real-time protection for each Microsoft-based computer system.

(2) The County has contracted with a service provider to "preprocess" all email inbound to the County from the Internet prior to the messages being received by the County's email system. This preprocessing includes removal of all email spam and malicious software attached to the email. The malicious software detection and removal solutions used by the service provider are different than the County's solutions. This provides even greater protection by not relying on just one solution but a multi-tiered, multi-approach solution.

(3) DHS, HR and IS employees are required to leave their workstations running after business hours to allow automated processes, such as operating system and application updates, to complete.

(4) DHS, HR and IS employees will refrain from opening emails that are from unknown or suspicious senders.

(5) DHS, HR and IS employees will report to the IS Helpdesk Support ("HDS") Team or the Security Official any suspected nefarious activities caused by malware (viruses or spyware) on their workstations.

c. Log-In Monitoring

(1) As part of the County's overall Microsoft Domain software configuration, any attempts to log into the domain from any networked computer using the same userid more than 10 times will result in the user account being disabled. Only the IS technical staff can re-enable user accounts.

(2) Any DHS, HR or IS employee requiring re-enabling of their account will be reported to the Security Official.

(3) Through Microsoft Domain software, IS will maintain log files for all EPHI data access on the Annex General File Server where all County EPHI related data resides, tracking the access to data by userid, machine name, and time/date of access, and maintaining this information for a period of three (3) months from the time of the event.

d. Password Management

(1) Through a Microsoft Domain electronic policy, all employees with computer accounts are required to change their passwords every 180 days. This electronic policy also enforces password complexity (required use of 3 out of the 4 types of character sets) and a minimum password length of 8 characters when passwords are changed. The policy automatically reminds the users when they need to change their password (with a 30-day pre-notice) and automatically disables the account if the password isn't changed in 180 days (requiring the IS Department to re-enable the account). The software also instructs the user how to select an appropriate complex password.

(2) In adherence to the HIPAA security policy, employees are responsible for all activities and actions that are conducted under their userid. Therefore, in regards to password management, all employees of the County are prohibited from doing the following:

(i) Disclosing any userid or password to any other person except IS personnel providing computer support functions.

(ii) Recording their userid or application and software passwords where they may be easily obtained or accessed by others.

(3) In addition, HR and DHS employees are prohibited from disclosing any application and software passwords, used to protect EPHI information, to anyone not authorized by the Privacy Official to have access to EPHI.

6. Security Incident Procedures

a. Response and Reporting

A security incident as it relates to EPHI is defined in the Security Rule as "*the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system*." The County's process to identify and address a security incident is as follows.

b. Reporting

(1) All security incidents that affect or may affect the confidentiality, integrity, or availability of EPHI shall be reported to the Help Desk/Desktop Support (HDS) Team. The HDS Team will respond promptly to all reported security incidents.

(2) Incidents that shall be reported include, but are not limited to:

(i) Virus, worm, or other malicious code attacks found within the County that impact EPHI related systems or data

(ii) Network or system intrusions to any County network or network device

(iii) Unauthorized access to the folders that contain EPHI data

(iv) EPHI data loss due to disaster, failure, error, or theft

(v) Loss of any electronic media containing EPHI

(vi) Loss of integrity of EPHI

(vii) DHS, HR or IS employees' userid or password compromised

(viii) Unauthorized access to the Annex server room

(3) The HDS Team shall be notified immediately of any suspected or actual security incident. If it is unclear as to whether a situation is a security incident, the HDS Team shall be contacted to evaluate the situation.

c. Response and Resolution

(1) The HDS Team will report the incident to the Security Official. The Security Official will determine if the incident shall be forwarded to the appropriate Privacy Official and County Manager.

(2) If the Security Official is unavailable, the HDS Team will report the incident to the appropriate Privacy Official. If the Privacy Official is unavailable, the HDS Team will report to the County Manager.

(3) If the incident is forwarded to the appropriate Privacy Official and/or County Manager, they will evaluate the report to determine if an investigation of the incident is necessary. If an investigation is necessary, the County Manager shall determine if the County Attorney and/or law enforcement should be contacted regarding the incident.

(4) All HIPAA security-related incidents and their outcomes shall be logged and documented by the HDS Team with assistance from the Security Official.

(5) The appropriate Privacy Official shall document and log incidents and outcomes the Privacy Official or the County Manager have reviewed and investigated.

(6) Bi-annually, the Security Official will supply the Privacy Officials with a record of all incidents logged during that period. The Privacy Officials will retain these incident reports for six (6) years.

(7) The Security Official shall train IS, DHS and HR employees in their response roles and responsibilities and provide refresher training as needed.

(8) The Security Official shall test the incident response capability at least once annually.

7. Contingency Plan

a. Data Backup Plan

(1) Because EPHI data at the County is incidental information that can be recreated from business associates and insurance companies, the criticality of restoration, recovery, and emergency access to this data is actually less than other data at the County. Thus, the EPHI data contingency plan will follow the County's regular contingency plan.

(2) As part of the County's business-wide data backup plan, all EPHI data saved in the DHS and HR folders located on the County's shared general purpose file server is backed up on a nightly basis Monday – Thursday and once during the weekend. The County is using high speed disk drives and replicating the data offsite via a private network. Disk to disk backup won't be encrypted as long as the removal of a single drive on the disk to disk backup device doesn't allow for contiguous data to exist on that single drive. Any backups stored on portable media devices must be encrypted.

b. Disaster Recovery Plan

The disaster recovery plan to recover EPHI will be a part of the County's business-wide government contingency plan. As EPHI data is located on the County's shared general purpose file server, restoration of data on this server will include restoration of EPHI data. Copies of the IS section of the County's government contingency plan exists in both the Emergency Manager and IS Departments.

c. Emergency Mode Operations Plan

The County's current emergency mode operations plan is sufficient to cover what is necessary regarding EPHI.

d. Testing and Revision Procedures

Testing and revision of contingency procedures will be conducted in accordance with the County's overall contingency plan. As restoration of EPHI is no different than restoration of other files located on the County's shared general purpose file server, restoration of EPHI data from backups has been documented as part of the overall data restoration procedures inside IS.

e. Applications and Data Criticality Analysis

As EPHI data at the County is incidental data and can be recreated from other entities' systems, EPHI data at the County is considered low on the criticality of County data overall. The critical components to restore EPHI data are a correctly configured Microsoft domain, a general purpose file server, a Windows-based workstation with a copy of the current backup software installed, the EPHI data accessed and a backup device. This infrastructure will be part of the general restoration of critical data and services at the County.

8. Evaluation

All parts of the security plans and procedures will be continuously evaluated as part of the overall evaluation of the County's policies and procedures regarding the HIPAA Security Rule. Documented policy reviews and revisions will occur as needed using either internal or contracted methods.

9. Business Associate Contracts and Other Arrangements

Business Associates were identified as part of the Privacy Rule analysis effort. The contracts created to comply with the Privacy Rule standards are sufficient for the Security Rule. Business Associate contracts and other arrangements documents are maintained by the Privacy Officials. All required Business Associate contracts will be updated to comply with current privacy and security rules.

III. § 164.310 Security Standards: Physical Safeguards

1. Facility Access Controls

a. Contingency Operations

Because EPHI at the County is incidental and can be recreated from other sources external to the County, the current facility access controls for a contingency, created and maintained by the County's Building Maintenance Director, will suffice to cover the requirements for EPHI.

b. Facility Security Plan

(1) IS. Physical access to the County's general purpose file server that contains EPHI data is through two locked doors to the Annex server room. The doors are keyed, through a County-wide keying system, such that access to this room is limited to keys assigned to IS and Building Maintenance personnel and those having "master" or "super-master" keys. The main entrance to the Annex server room has signage stating that only authorized personnel are allowed into the room. Any other individual requiring access into this room is supervised by either IS or Building Maintenance personnel.

(2) HR. Physical access to HR workstations that can access EPHI data is through a single door into the HR office. The door is keyed, through a County-wide keying system, such that access to HR is limited to keys assigned to HR and Building Maintenance employees and those having "master" or "super-master" keys. The HR Director will be responsible for closing and locking this door whenever all HR employees are out of the office.

(3) DHS. There are multiple doors to enter the DHS building from the outside. All entrances are keyed through a County-wide keying system, such that access to DHS is limited to keys assigned to DHS and Building Maintenance employees and those having "master" or "supermaster" keys. The DHS Director will be responsible for closing and locking these doors whenever all DHS employees are out of the office.

c. Access Control and Validation Procedures

(1) Only employees in the IS or Building Maintenance Departments should be given keys that can access the Annex Server room. All individuals not cleared to have access to the Annex Server room will be escorted by IS or Building Maintenance personnel.

(2) Only employees in HR or DHS should be given keys to access their respective offices. The only exception is employees in the IS and Building Maintenance Departments will also be given keys for both offices.

(3) Each employee assigned a key that has access to the Annex server room, DHS, or HR must sign a statement acknowledging responsibility for the key as part of the normal employment

orientation process. Keys are not to be shared with anyone who is not part of the IS, DHS, HR, or Building Maintenance Departments.

(4) The County's Building Maintenance Director is responsible for the tracking and distribution of keys (through HR) and the final decision to re-key the Annex server room doors, DHS or HR office doors if keys are lost or not returned.

d. Maintenance Records

(1) A logbook, kept by the Security Official, will note all repairs or modifications to physical components of the Annex Server room that are related to security. A similar logbook will be kept by the appropriate Privacy Official regarding the HR and DHS offices. Log entries will also include who authorized the work. This will include, but not be limited to, repairs and modification of the following:

(i) Security hardware

(ii) Walls

(iii) Doors

(iv) Locks

(v) Re-keying doors

(2) If an employee of the IS, DHS, HR, or Building Maintenance Departments terminates employment with the County and does not return the keys that allow access to the Annex Server Room, DHS, or HR offices, or if a key with such access is lost, the Security and Privacy Officials will consult with the Building Maintenance Director to determine if door re-keying is necessary.

2. Workstation Use

a. For the purpose of this document, a "workstation" is defined as an electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

b. Because it is cost prohibitive to secure all County computer-based resources in regards to EPHI, all County employees are prohibited from using any County resource to create, transmit, receive, or store electronic documents containing EPHI about themselves or any other persons. This policy exempts DHS and HR employees if they are creating or maintaining e-documents in furtherance of County business.

c. Workstations provided to DHS and HR employees:

(1) Shall ONLY be used by those employees authorized to access EPHI data.

(2) Shall only be used in accordance with County policy.

(3) Shall be the only workstations used to access EPHI data.

(4) Shall be configured to automatically activate a screen saver program, with password protection required to exit the screen saver, when the computer has been left logged on without activity, for a period of fifteen (15) minutes.

d. DHS and HR employees shall not:

(1) Access, create, or store EPHI information using portable devices such as laptops, PDAs, notepads, or other similar devices unless the data is encrypted before being copied to the device or the device supports encryption natively.

(2) Use personal PC's or other personal devices to store EPHI data and should be made aware that any personal equipment used by the employee could be confiscated and searched by the applicable County official.

(3) Store EPHI information while "working from home," from satellite offices or on any workstation other than those approved for HIPAA use.

(4) Store EPHI data on any form of portable electronic media such as CDs, DVDs, "thumb drives," diskettes, or other similar media, unless the data on the questioned device has been encrypted to a minimum of AES128 or HIPAA approved level, whichever is greater.

(5) Download and/or install any software from the Internet or any other source on their workstation unless authorized by IS.

(6) Knowingly allow spyware to install on their workstation.

(7) Knowingly introduce a computer virus into any County computer-based device.

(8) Load data from diskettes, thumb drives, CDs, DVDs, or other portable media of unknown origin.

e. DHS and HR employees shall:

(1) Immediately contact the HDS Team if they suspect that their workstation has been infected by a virus.

(2) Immediately contact the HDS Team if they suspect that spyware may have been installed on their computer.

(3) Immediately change their user account password if they suspect it has become known to another employee and report the incident to the HDS Team.

(4) Immediately change the application and software passwords used to protect EPHI if they suspect these passwords have become known to anyone not authorized by the Privacy Official to have access to EPHI and report the incident to the HDS Team.

(5) Notify the appropriate Privacy Official if they believe the application and software passwords used to protect EPHI have become known to anyone not authorized by the Privacy Official to have access to EPHI.

(6) Screen lock or log off their computer if they will be leaving it for an extended period of time.

(7) Log off their computer at the end of each work day.

3. Workstation Security

(1) There is a single entry door into HR that is lockable. HR employees shall close and lock the office door when no HR employees are in the office. The HR Director shall be ultimately responsible for making sure the staff physically secures the office.

(2) There are multiple doors to enter the DHS building from the outside. All entrances are keyed through a County-wide keying system, such that access to DHS is limited to keys assigned to DHS and Building Maintenance employees and those having "master" or "supermaster" keys.

4. Device and Media Controls

a. Disposal and Media Re-Use

(1) Prior to transferring antiquated computer equipment to the Purchasing department for disposal or re-use, the IS Department shall wipe clean all data on all computer disks in the computer utilizing a program that meets Department of Defense standards.

(2) Backup media shall be degaussed using a professional degaussing device prior to disposal of media or re-use by another entity outside of the IS department.

(3) Backup media will be reused without any formatting or degaussing if re-used to back up County systems.

b. Accountability

As part of the County IS controllable asset inventory process, all locations of workstations used by DHS and HR are tracked and uniquely identified through make, model, serial #, and barcode #. As part of the IS data backup procedure, all locations of backup media shall be tracked.

c. Data Backup and Storage

No EPHI data shall be stored on local workstations. Therefore, no backups of local workstation data are necessary before moving workstation equipment. All EPHI data will be stored in HIPAA folders within the DHS or HR Departmental folder located on the County's shared general purpose file server. As part of normal data backup procedures, EPHI data is backed up on a nightly basis Monday – Thursday and once during the weekend. When replacing the shared general purpose file server, all data is backed up and restored exactly as is on the replacement server prior to removal of the old server.

IV. § 164.312 Security Standards: Technical Safeguards

1. Access Controls

a. Unique User Identification

Every employee that has computer access to the County Microsoft domain shall be given a unique logon account (userid) created, typically, by appending the first letter of their first name to their last name. Through this userid, a person's activities can be tracked across all County Microsoft-based resources and a user's access to networked and local workstation resources can be managed. **All employees are accountable for actions and activities conducted using their userid. An employee's associated userid and password should be known only by that employee and IS staff for support functions.**

b. Emergency Access Procedure

(1) Employees of the County who wish to access EPHI during an emergency situation can petition the appropriate Privacy Official for the required access to EPHI.

(2) In the situation where the Privacy Official is not available during an emergency, the following individuals should be petitioned in the following order based on their availability:

(i) County Manager

(ii) County Commissioner

(iii) County Attorney

(iv) County Security Official

(v) County Emergency Manager

(vi) Any employee or official of the County designated by the "person-in-charge" of the County

(3) Petitioning requires that a requestor make verbal or written request to the appropriate available individual for access to EPHI information. The appropriate available individual will respond to the requesting individual by approving or disapproving the request.

(4) The appropriate available individual should, as soon as possible, document when the request was made, who made the request, what EPHI access was requested, and the appropriate available individual to which the request was made (and why the request was made of this person). In addition, the appropriate available individual should document whether or not the request was granted; if granted, to what extent access to EPHI data was granted and when it was granted; and if denied, the reasons for the denial.

c. Automatic Logoff

(1) All workstations that have access to EPHI data will be configured, through a Microsoft Domain Active Directory policy, to automatically activate a screen saver program that requires a username and password to regain access to the workstation after fifteen (15) minutes of user inactivity.

(2) The Annex backup server and general purpose file server that
store the EPHI data will be configured, through a Microsoft Domain Active Directory policy, to automatically activate a screen saver program that requires a username and password to regain access to the servers after fifteen (15) minutes of user inactivity.

(3) If either server does not have such a feature, it will be configured to automatically log the user off after fifteen (15) minutes of inactivity.

(4) If either server does not have a password-protected screen lock program or a way to automatically log a user out after fifteen (15) minutes of inactivity, all users who log into the server(s) will be required to log out before leaving the keyboard (remote or local) they are using to access the server.

d. Encryption and Decryption

(1) All EPHI information created and maintained at the County by DHS or HR shall be stored, unencrypted, in the HIPAA subfolder located under that office's Departmental subfolder located on the County's shared general purpose file server.

(2) Electronic transmission of EPHI data should only be conducted by DHS and HR employees doing business with external entities regarding an employee or client. Both DHS and HR shall transmit EPHI data only if it has been encrypted to the minimum of AES-128 or HIPAA standard.

2. Audit Controls

a. All users other than those approved by the appropriate Privacy Officer within DHS or Human Resources will be denied access to log into workstations locally.

b. IS will configure the Microsoft Domain to log an event every time a user accesses EPHI data, noting which userid was used to log in, which workstation or networked piece of equipment was used to gain access to the server, and when the user logged out. At least three (3) months' worth of accessible events will be maintained in order to generate the reports necessary to comply with the IS Activity Review policies and procedures.

c. IS will configure the Microsoft Domain to log an event every time the HIPAA subfolder under the DHS or HR Departmental folder (where all EPHI information is stored) is accessed, noting which userid was used to access it and the time it was accessed. At least three (3) months' worth of accessible events will be maintained in order to generate the reports necessary to comply with the IS Activity Review policies and procedures.

3. Integrity

Routt County's EPHI information is "incidental" information and used for information purposes only by DHS and HR. If the information is altered or destroyed in an unauthorized manner, the data can be regenerated through other sources. Therefore, the County will not implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

4. Person or Entity Authentication

All EPHI inside the County is isolated in HIPAA subfolders under the DHS or HR Departmental folders on the Annex General Purpose File Server. This folder is set up, through Microsoft domain permissions, to restrict access (for any function or user) to those subfolders and every file and subfolder within, allowing access only to employees and automated administrative

accounts that are members of three Microsoft domain security groups: DHS, HR and Domain Administrators.

5. Transmission Security

a. Integrity Controls

County policy prohibits employees from using County computer-based equipment to electronically transmit or cause to receive transmission of EPHI using any transmission method such as (but not limited to) email, ftp, web, or instant messaging. DHS and HR employees are exempt from these policies if they are conducting such transmission in furtherance of County business and in accordance with the policies set forth herein. The use of encryption for all electronically transmitted EPHI information will guarantee, by its nature, that the EPHI has not been improperly altered without detection during transmission. If the recipient of the transmission cannot decrypt the information or if the information, decrypted, is unreadable, then the transmission may have been altered improperly.

b. Encryption

HR and DHS will use the following procedures to electronically transmit EPHI data to external Business Associates, medical providers, or other parties entitled to receive such data:

(1) If the external Business Associate, medical provider, or other party has its own free-to-use HIPAA approved transmission interception risk management solution (such as encrypted web-based email), DHS and HR employees will use that entity's solution to transmit EPHI.

(2) If the external Business Associate, medical provider, or other party has its own HIPAA approved transmission interception risk management solution but it is not free to use, DHS or HR employees will make the determination to use one of the following:

(i) Pay to use the solution

(ii) Transmit the data through another agreed-upon secure means (such as a Business Associate encryption service)

(iii) Transmit the data through a non-electronic means such as posted mail or fax

(3) If the external Business Associate, medical provider, or other party does not have its own EPHI transmission interception risk management solution, DHS and HR employees will decide to either:

(i) Transmit the data through another agreed-upon secure means (such as a Business Associate encryption service)

(ii) Transmit the data through a non-electronic means such as posted mail or fax

V. § 164.314 Security Standards: Organizational Requirements

1. Business Associate Contracts or Other Arrangements

a. The County acknowledges that:

(i) The contract or other arrangement between the covered entity (DHS or HR) and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(I) or (a)(2)(ii) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful --

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary (of the Department of Health and Human Services.)

b. Business Associate Contracts

DHS and HR, through the appropriate Privacy Official, will create the proper business associate contracts such that they are substantially similar to the Sample Business Associate Contract attached as Exhibit A to the Statement of Routt County Privacy Policy.

c. Other Arrangements

DHS and HR, through the Privacy Official, will create appropriate other arrangements such that:

(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if --

(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(I) of this section; or

(2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(I) of this section.

(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit EPHI on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

(C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

2. **Requirements for Group Health Plans**

The County provides medical benefits through a self-insured health planand, thus is a Group Health Plan. United Health Care administers the County's plan and the County has retained a third-party employee benefits consultant. Both United Health Care and the third-party employee benefits consultant will be required to comply with the requirements of this section through the use of business associate contracts that are substantially similar to the Sample Business Associate Contract attached as Exhibit A to the Statement of Routt County Privacy Policy.

VI. § 164.316 Security Standards: Policies and Procedures and Documentation Requirements

1. Policies and Procedures

The County acknowledges it will:

Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

2. Documentation

a. The County acknowledges it will:

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

b. Time Limit

The County will retain all documentation required to address the HIPAA Security Rule for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

c. Availability

The County will make such documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

d. Updates

The County will review such documentation no later than four (4) years from the date when it was created or last reviewed, and update as needed in response to environmental or operational changes affecting the security of EPHI.

This policy shall be effective immediately upon adoption.

Adopted by the Routt County Board of Commissioners on the 4th day of April, 2006. Reviewed and revised on the 24th day of May, 2022.

Routt County Board of County
Commissioners

By: _____
M. Elizabeth Melton, Chair