STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.01	Page 1 of 2
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Information Security Strategy	

Effective Date: October 9, 2012

Policy:
DEPARTMENT will implement safeguards determined to be reasonable and appropriate to protect its information assets to maintain the confidentiality, integrity, and availability (CIA) of those assets.

Security policies, plans, and procedures created in support of this Information Security Policy, are organized in five categories (sections) and address at a minimum:

- Administrative safeguards:
  - Security management process
  - Risk analysis
  - Risk management
  - Sanction policy
  - Information system activity review
  - Assigned security responsibility
  - Workforce security
  - Authorization and/or supervision
  - Workforce clearance procedure
  - Termination procedures
  - Information access management
  - Access authorization
  - Access establishment and modification
  - Security awareness and training
  - Security reminders
  - Protection from malicious software
  - Log-in monitoring
  - Password management
  - Security incident procedures
  - Response and reporting
  - Contingency plan
  - Data backup plan
  - Disaster recovery plan
  - Emergency mode operation plan
  - Testing and revision procedures
  - Applications and data criticality analysis
  - Evaluation
  - Business associate agreement and other arrangements
  - Written contract or other arrangement

- Physical safeguards
  - Facility access controls
  - Contingency operations
  - Facility security plan

    - Access control and validation procedures
    - Maintenance records
    - Workstation use
    - Workstation security
    - Disposal
    - Media re-use
    - Accountability
    - Data backup and storage

- Technical safeguards
    - Access control
    - Unique user identification
    - Emergency access procedure
    - Automatic logoff
    - Encryption and decryption
    - Audit controls
    - Integrity
    - Mechanism to authenticate sensitive information
    - Person or entity authentication
    - Transmission security
    - Integrity controls
    - Encryption

- Organizational Framework
    - Policies and Procedures requirement
    - Documentation requirement

- Data Breach
    - Data Breach Management
    - Data Breach Notification
    - Data Breach Notification to HHS
    - Data Breach Notification to Member
    - Data Breach Notification to Media

- Other Policies
    - Information classification
    - Network security
    - Email security
    - Wireless security

In addition, all security policies, and procedures shall be reviewed and evaluated (based on any environmental and operational changes) on an annual basis by the Information Security Officer and team.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.02	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Security Management Process Policy	

Effective Date: October 9, 2012

Policy:
DEPARTMENT will create, administer and oversee policies to ensure the prevention, detection, containment and correction of security violations.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.03	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Risk Analysis & Risk Management Policy	

Effective Date: October 9, 2012

Policy:

Risk analysis and risk management is recognized as an important part of The Utah Department of Health's (UDOH) Office of Health Information and Data Security. In accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the Evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(l)(ii)(A), 164.308(a)(l)(ii)(B), 164.308(a)(l)(i), and 164.308(a)(8), it is the policy of UDOH to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health information (PHI) (and other confidential electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.04	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: HIPAA Security Oversight	

Effective Date: October 9, 2012

Policy:

In accordance with the standards set forth in the HIPAA Security Rule, Utah Department of Health (UDOH) is committed to ensuring the confidentiality, integrity, and availability of all electronic protected health information (ePHI) it creates, receives, maintains, and/or transmits. To provide for the appropriate development, implementation, and oversight of UDOH's efforts toward compliance of the HIPAA security regulations, UDOH has a Security Officer [164.308(a)(2)] responsible for facilitating the training and supervision of all DEPARTMENT covered functions' workforce members [164,308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any workforce member that is in non-compliance with the HIPAA security regulations [164.308(a)(l)(ii)(c)], and writing, implementing, and maintaining all policies, procedures, and documentation related to efforts toward HIPAA security compliance [164.316(a-b)].

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.05	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Information System Activity Review	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will clearly identify all critical systems that process sensitive information. DEPARTMENT will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.06	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Workforce Security	

Effective Date: October 9, 2012

Policy:

DEPARTMENT shall ensure that members of the workforce as well as contractors and others are only accessing those systems and information to which they are authorized.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.07	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: System Access	

Effective Date: October 9, 2012

Policy:

It is the policy of the -DEPARTMENT covered functions to safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. Access to information systems to all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to digital and/or electronic protected health information (ePHI) within the organization's information systems and are extended even after termination or other conclusion of access. These safeguards have been established to address the HIPAA Security regulations including the following:

- 164.3 0 8 a4iiC Access Establishment and Modification
- 164.308a3iiB Workforce Clearance Procedures
- 164.308a4iiB Access Authorization
- 164.312d Person or Entity Authentication
- 164.312a2i Unique User Identification
- 164.308a5iiD Password Management
- 164.312a2iii Automatic Logoff
- 164.310b Workstation Use
- 164.310c Workstation Security
- 164.308a3iiC Termination Procedures
- 164.308a4iiA Isolating Healthcare Clearinghouse Function

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.08	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Information Access Management	

Effective Date: October 9, 2012

Policy:

DEPARTMENT members of the workforce are granted access only to that sensitive information to which they are authorized in order to perform their job role or associated job function.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.09	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Security Reminders	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will periodically send out security reminders to all members of the workforce.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.10	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Protection from Malicious Software	

Effective Date: October 9, 2012

Policy:

DEPARTMENT, in collaboration with the Department of Technology Services (DTS), will deploy malicious software identification, prevention, and removal technology at the perimeter of its network, on all servers (including email servers), and on individual end-user systems.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.11	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Log-In Monitoring	

Effective Date: October 9, 2012

Policy:

The DEPARTMENT will configure all critical components that process, store or transmit sensitive information to record log-in attempts – both successful and unsuccessful – as well as automatic lock out and reporting after a designated number of failed attempts.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.12	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Security Incident Procedures	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will create processes for the identification, reporting, and timely response to real or potential violations of information security or a material breach of any part of DEPARTMENT's security policy.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.13	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Response and Reporting	

Policy:

DEPARTMENT will:

- Identify, research, and respond to any suspected security incidents;
- Mitigate, to the extent practicable, any harmful effects of any suspected or actual security incidents; and
- Maintain appropriate documentation for all security incidents.

Effective Date: October 9, 2012

Policy:

DEPARTMENT will develop, maintain, and test a contingency plan. The plan shall be routinely updated plan and include activities for responding to a system emergency including performing backups, preparing critical facilities, and appropriately detailed migration plans that can be used to facilitate continuity of operations in the event of an emergency and recovering from a disaster.

It is the policy of DEPARTMENT that the computer system be attached to a back-up power source (i.e. emergency power and/or UPS) in case of electrical failure.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.15	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Data Backup Plan	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will create and maintain exact, retrievable copies of sensitive information.

DEPARTMENT will ensure that sensitive data is backed up to disk, tape, or a combination of those technologies on a regular basis so as to minimize the loss of data in the event of an incident or disaster.

DEPARTMENT will ensure that backup media is periodically tested to ensure suitable quality and reliable data restoration.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.16	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Disaster Recovery Plan	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will develop and maintain a Disaster Recovery Plan. The Information Security Officer will ensure the development of a Disaster Recovery Plan document.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.17	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Emergency Mode Operation Plan	

Effective Date: October 9, 2012

Policy:

The Information Security Officer must identify the levels of emergencies and associated responses. The Information Security Officer must develop specific components of the Emergency Mode Operation Plan, maintain those components, and periodically test the plan.

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure that all contingency and disaster recovery plans are tested and revised, as necessary, on a periodic basis, not to exceed annually.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.19	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Applications and Data Criticality Analysis	

Effective Date: October 9, 2012

Policy:

DEPARTMENT shall assess the relative criticality of applications and data in support of the contingency and disaster recovery plans.

The relative criticality shall be documented and approved by executive management in order to establish the priority of recovery capabilities and activities.

Effective Date: October 9, 2012

Policy:

DEPARTMENT will evaluate the technical and non-technical implementations of its Security Policies and procedures.

This evaluation will be completed on a regular basis, at least annually, and in response to environmental or operational changes affecting the security of sensitive information.

The evaluation will determine the effectiveness of, and adherence to, DEPARTMENT policies as well as to ensure compliance with U.S. State and Federal regulations.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.21	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Business Associate Agreements	

Effective Date: October 9, 2012

Policy:

To establish guidelines for the Utah Department of Health covered functions (DEPARTMENT) to identify those vendor/business relationships which meet the HIPAA definition of a "business associate" and provide direction in establishing formalized business associate agreements. DEPARTMENT shall implement the required procedures and ensure documentation to establish satisfactory assurance of compliance. HIPAA requirements for business associates are addressed in the following standards:

- 45 CFR § 164.308(b)(l) - HIPAA Security Rule Administrative Safeguards Business Associate Contracts and Other Arrangements
- 45 CFR §164.314 - HIPAA Security Rule Departmental Requirements Business Associate Contracts or Other Arrangements
- 45 CFR § 164.502(e)(l) - HIPAA Privacy Rule Uses and Disclosures of Protected Health Information: General Rules - Disclosures to Business Associates
- 45 CFR §164.504 - HIPAA Privacy Rule Uses and Disclosures: Departmental Requirements

The standards define the concept of a business associate relationship and outline the required elements to be addressed in a business associate agreement (as addressed in this policy).

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.22	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Facility Access	

Effective Date: October 9, 2012

Policy:
To safeguard the confidentiality, integrity, and availability of protected health information (PHI), business, and Proprietary information within the Utah Department of Health covered function's (DEPARTMENT) information systems/applications by controlling access to the physical buildings/facilities that house these systems/applications in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. Physical Access to all of DEPARTMENT's facilities is limited to only those authorized in this policy. In an effort to safeguard PHI, the facility(s), and systems/applications from unauthorized access, tampering, and theft, access is allowed to designated areas only to those persons authorized to be in them, and with escorts for unauthorized persons. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to DEPARTMENT's facility(s) to areas containing information systems/applications.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.23	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Contingency Operations	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will develop contingency operation procedures to facilitate access for emergency response.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.24	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Facility Security Plan	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will develop a Facility Security Plan to safeguard the facilities and premises from unauthorized physical access, tampering or theft including the equipment present in all such facilities.

All equipment that collects, stores, processes, or transmits EPHI will be protected from unauthorized access at all times.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.25	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Access Control and Validation Procedures	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will configure facility access controls to validate all access by members of the workforce to facilities and systems. Access controls will be enforced to ensure that the only access to sensitive information is by authorized members of the workforce.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.26	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Maintenance Records	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will document all repairs and modifications to the facility that could affect the confidentiality, integrity, or availability of EPHI. All records will be securely retained for a time period as dictated in the DEPARTMENT document retention policy.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.27	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Device and Media Controls	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure compliance with the Device and Media Controls standard (164.310(d)(1)) and its associated implementation specifications of: Disposal, Media Re-use, Accountability and Data Backup and Storage.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.28	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Destruction, Disposal, and Reuse of Protected Health Information Media	

Effective Date: October 9, 2012

Purpose:

It is the policy of Utah Department of Health covered functions (DEPARTMENT) to ensure the privacy and security of protected patient health, information (PHI) in the maintenance, retention, and eventual destruction/disposal of such media. The DEPARTMENT also recognizes that media containing PHI may be reused when appropriate steps are taken to ensure that all stored PHI has been effectively removed. Destruction/disposal of patient health information shall be carried out in accordance with federal and state law and as defined in the Departmental retention policy. The schedule for destruction/disposal shall be suspended for records involved in any open investigation, audit, or litigation.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.29	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Accountability	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure that a record is maintained to identify movements of sensitive information including all related hardware and devices.

Effective Date: October 9**,** 2012

Policy:

DEPARTMENT will determine when backups are needed and this will be done prior to the movement of any required systems collecting, storing, processing, or transmitting sensitive information.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.31	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Access Control	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will control access to its information assets and systems. Only individuals that have been formally authorized to view or change sensitive information will be granted access to that information.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.32	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Emergency Access Procedure	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will establish an Emergency Access Procedure for gaining properly authorized access to sensitive information, such as EPHI, during an emergency.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.33	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Encryption and Decryption	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will identify systems that require sensitive information to be encrypted.

DEPARTMENT will identify members of the workforce, processes, and devices that require encryption capabilities and will implement those capabilities and test their proper functioning.

DEPARTMENT will only provide encryption keys to members of the workforce whose job role requires knowledge of encryption keys.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.34	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Audit Controls	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will identify critical systems that require event auditing capabilities.

DEPARTMENT will define the events to be audited on all such systems.

DEPARTMENT will protect all collected logs from alteration or destruction.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.35	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Integrity	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will review the results of risk analysis to identify the data that must be protected from improper alteration or destruction.

DEPARTMENT will ensure that data is only altered by properly authorized members of the workforce or automated processes.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.36	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Mechanism to Authenticate Sensitive Information	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will review the use of digital signature and/or checksum technology to corroborate that sensitive information has not been altered or destroyed in any unauthorized manner.

DEPARTMENT will evaluate the need for and use of encryption to maintain the integrity of sensitive information.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.37	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Transmission Security	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will develop security policies to identify core activities for the Integrity Controls and Encryption implementation specifications.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.38	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Integrity Controls	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will maintain integrity controls to ensure the validity of information transmitted over the network infrastructure. DEPARTMENT will implement measures to ensure that sensitive information is not improperly modified without detection until disposed of by an authorized member of the workforce.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.39	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Encryption	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will evaluate the need for and use of encryption to maintain the confidentiality and integrity of sensitive information being transmitted over a network.

<table>
<tr><td rowspan="2">STATE OF UTAH
DEPARTMENT OF HEALTH</td><td>Number: 13.40</td><td>Page 1 of 1</td></tr>
<tr><td>Original Issue Date:10/09/2012</td><td>Revision Date:</td></tr>
<tr><td>POLICIES & PROCEDURES</td><td colspan="2">Authorized By: W. David Patton</td></tr>
<tr><td>Section: Security Policies</td><td colspan="2">Subject: Policies and Procedures Standard</td></tr>
</table>

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure the development of all policies and procedures required by the regulations.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.41	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Documentation Standard	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will retain the documentation required by the regulation for six (6) years or longer, from the date of its creation or the date when it was last in effect, whichever is later.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.42	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Information Classification	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will classify information as appropriate and according to its level of sensitivity.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.43	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Network Security	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will evaluate the need for secure communication on all networks, public and private, that are utilized to transmit DEPARTMENT sensitive information.

Where secure communications are required, technology and processes will be put in place to ensure the confidentiality and integrity of sensitive information.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.44	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Email Security	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will identify whether sensitive information is permitted to be transmitted over email, and secure all email transmissions of sensitive information whenever the transmission is permitted.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.45	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Remote Access	

Effective Date: October 9, 2012

Policy:

DEPARTMENT covered functions will take all reasonable and appropriate steps to ensure the secure and authorized use of all remote access capabilities and solutions.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.46	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Portable Devices	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure that wherever and whenever the use of portable devices is deemed necessary, these devices will be appropriately secured and used only by properly authorized members of the workforce.

DEPARTMENT will ensure that all portable devices will be used according to the guidelines defined in this policy.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.47	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: VPN	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure the VPN is appropriately secured at all times, and will adhere to the requirements defined in this policy.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.48	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Wireless Security	

Effective Date: October 9, 2012

Policy Statement:

DEPARTMENT will operate all wireless networks in a secure manner so as to ensure the confidentiality, integrity, and availability of all sensitive information transmitted over wireless networks.

DEPARTMENT will ensure that all wireless devices are configured and operated according to the requirements set forth in this policy.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.49	Page 1 of 1
	Original Issue Date:10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Wireless IP Phones	

Effective Date: October 9, 2012

Policy:

DEPARTMENT will ensure the reasonable and appropriate use of wireless IP telephones and will provide guidance for the use of such devices.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.50	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Social Media	

Effective Date: October 9, 2012

Policy:

DEPARTMENT and its workforce members will maintain effective electronic communications that are consistent with the DEPARTMENT beliefs and workforce standards. The guidelines contained within this policy apply whether or not you are using DEPARTMENT tools to IM, text or email, or whether you are using the Internet as part of your job or for personal social networking that involves DEPARTMENT references.

This policy is based on DEPARTMENT's "3 Rs of Electronic Engagement":

- Be clear about whom you are **Representing**.
- Take **Responsibility** for ensuring that any references to DEPARTMENT are factually correct and do not breach confidentiality requirements.
- Show **Respect** for the individuals and communities with whom/which you interact.

STATE OF UTAH DEPARTMENT OF HEALTH	Number: 13.51	Page 1 of 1
	Original Issue Date: 10/09/2012	Revision Date:
POLICIES & PROCEDURES	Authorized By: W. David Patton	
Section: Security Policies	Subject: Cell Phone and Smartphone Policy	

Effective Date: October 9, 2012

Policy:

It is the policy of DEPARTMENT to implement reasonable safeguards while using cell phones, smartphones, or similar equipment. These safeguards relate to protecting confidential information, equipment security, and security of data. Please refer to Policy #13.50, Social Media Policy.