**TITLE: IT URAC standards compliance**

**VERSION DATE: XX/XX/20XX**

**Page 1 of 7 Standard Operating Policy**

POLICY:

<insert practice name> strives to provide appropriate and timely services to its customers/clients by securely collecting only the necessary information to carry out the services <insert practice name> provides. <insert practice name> places the highest priority on the protection of consumer’s Protected Health Information (PHI). To that end, <insert practice name> strives to maintain consistent and accurate information flow through proactive information management systems. Various processes and mechanisms have been implemented to provide for:

√ Data integrity **[Pharm Core 13]**

√ Data Storage, Maintenance, and Destruction **[Pharm Core 13]**

√ Business Continuity/Disaster Recovery **[Pharm Core 14]**

√ Information Confidentiality and Security **[Pharm Core 15]**

√ Confidentiality of Individual-Identifiable Health Information **[Pharm Core 16]**

√ Responsibility and Requirement to Preserve Confidentiality **[Pharm Core 16]**

PURPOSE: To clarify <insert practice name>’s compliance with URAC Specialty Pharmacy

Including, but not limited to URAC standards: PHARM Core 13, 14, 15, 16, PM 15, 17, PHARM-OP 4, 13, 14

SCOPE: <insert practice name> IT Department and Pharmacy

DEFINITIONS:

* **URAC** – Utilization Review Accreditation Commission. URAC, an independent, nonprofit organization, is a well-known leader in promoting healthcare quality through its accreditation, education, and measurement programs. URAC offers a wide range of quality benchmarking programs and services that model the rapid changes in the healthcare system and provide a symbol of excellence for organizations to validate their commitment to quality and accountability. Through its broad-based governance structure and an inclusive standards development process, URAC ensures that all stakeholders are represented in establishing meaningful quality measures for the entire healthcare industry.
* **PHI –** PHI – Protected Health Information

Identifiers

1. Names;   
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.  
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;  
4. Phone numbers;   
5. Fax numbers;   
6. Electronic mail (E-Mail) addresses;   
7. Social Security numbers;   
8. Medical record numbers;   
9. Health plan beneficiary numbers;   
10. Account numbers;   
11. Certificate/license numbers;   
12. Vehicle identifiers and serial numbers, including license plate numbers;   
13. Device identifiers and serial numbers;   
14. Web Universal Resource Locators (URLs);   
15. Internet Protocol (IP) address numbers;   
16. Biometric identifiers, including finger and voice prints;   
17. Full face photographic images and any comparable images; and  
18. Any other unique identifying number, characteristic, or code

PERSONNEL RESPONSIBLE: <insert practice name> pharmacy, and IT department

POLICY STATEMENT:

<insert practice name> conducts specialty pharmacy services on behalf of healthcare organizations that enter into contractual relationships with <insert practice name> to provide these services. <insert practice name> complies with all relevant regulatory agencies and the relevant standards of URAC.

PROCESS/PROCEDURES:

# Data Integrity [Pharm Core 13 (a)]

Data integrity means data accuracy and trace-ability. <insert practice name> has systems in place to ensure a high level of confidence that the record retrieved is, indeed, the correct record and that the information documented therein is accurate. <insert practice name> utilizes both paper and electronic systems which coordinate with each other. For electronic data, <insert practice name> utilizes <insert EMR> and <insert pharmacy computer system>. These systems have persuasive guards to ensure data integrity, which include (but not limited to):

* Data Entry controls for accuracy – <insert practice name> has built-in features in its electronic systems to restrict the users’ entry of data into appropriate fields. This includes the use of drop down menus and calendars to control the data entry process. This ensures that the data entered is appropriate for the data being requested.
* Cross-checking databases for consistency – Data structures which store the data have been developed to ensure consistency throughout the database, for example, a data field may only contain date information or numeric fields may not contain text information.
* Using unique identifiers for consumer data – A system generated unique number is created for each individual consumer and script.
* Prevention of and checking for duplicate entries – Routine system cross check reports reviews DOB and name to identify possible duplicate entries.

# Data Storage, Maintenance, and Destruction [Pharm Core 13 (b)] [Pharm-Op 13 (b-i)]

<insert practice name> maintains servers which store electronic information to multiple hard drives. The hard drives are functioning at all times to verify data and have a “mirroring” (RAID) function in case of failure. System maintenance is performed on a daily basis. <insert practice name> relies on electronic systems to store most PHI however paper prescriptions are filed and securely stored onsite. <insert practice name> delegates destruction of paper materials to State Record Keepers which complies with all HIPPA requirements for shredding and disposal. Backups are performed nightly and real time replication occurs throughout the day. IT staff are responsible for maintenance, storage and destruction of this information.

<Insert computer system> Server:

* + This server is located offsite at <computer company> headquarters in <insert location>. **[PHARM-OP 13 (b-i)]**
  + Backups and DR services for this system are done by QS/1 as this is a Cloud based system and all data resides at their location.

<insert EMR> Server:

* This server is located onsite as <insert practice name> in <city, state> in a secure data center.
* A complete server backup is performed every weekend and incremental backups are performed nightly. Backups are encrypted and picked up Monday-Friday and stored offsite by State Record Keepers in a nuclear bomb proof shelter.
* Real-time synchronization of data occurs to a separate server.

Only <insert practice name> personnel with a “need-to-know,” have access to the electronic or paper records. In order to retrieve electronic information, <insert practice name> personnel must access the information using unique user ID’s and Passwords. The <insert practice name> system administrator assigns passwords and access rights according to each program staff’s job responsibility, ensuring that staff only have access to PHI that is necessary to fulfill their role. **[PHARM-OP 13 (b-i)]**

Prompt removals take place of login credentials of staff who leave <insert practice name> or who no longer need access to <insert practice name> data resources. Staff is prohibited from sharing login credentials with other staff. <insert practice name> maintains all electronic records permanently.

When <insert practice name> deems electronic equipment obsolete such as cell phones or computer equipment such as a CPU which may contain confidential information <insert practice name> ensures that the hard drive or memory card is wiped clean of all data. <insert practice name> IT wipes computer hard drives using Acronis Drive Cleaner which does a multi-level overwrite algorithm used by the US Department of Defense. <insert practice name> then either stores the retired equipment on premises or selects a vendor to destroy the equipment. The equipment will not be resold or given away.

# Interoperability [Pharm Core 13 (c-i, c-ii)]

<insert practice name> facilitates interoperability by scanning all new patient orders into the patient’s profile. Each patient profile is managed in <EMR> Pharmacy Management. Information on new patient order processing activities and patient care management for existing patients is easily accessed by all authorized employees through document management systems. <insert practice name> is able to receive e-prescriptions via Surescripts into the <EMR> Pharmacy Management system. In addition, <insert practice name> uses <EMR> Management System’s service to communicate with pharmacy benefit management systems.

# Business Continuity / Disaster Recovery [Pharm Core 14 (a, b, c (c-i, c-ii), e)] [Pharm-Op 4 (e)] [Pharm-Op 13 (b-ii)]

<insert practice name> is primarily reliant on its telephone system and server to access data and provide services. These systems are critical to maintain in order for <insert practice name> to effectively deliver services. Sustained outages to these systems could impact <insert practice name>’s ability to promptly provide services.

In the event of a natural disaster, power outage, or an interruption in connectivity <insert practice name> has a plan to maintain business continuity. <insert practice name> has an on-site natural gas powered electrical generator that restores power to the entire enterprise after a 2 – 5 second interruption of power from the local electric company. As this back-up generator is powered by natural gas, it offers long-term electrical supply. This system is tested weekly on Tuesdays by the <insert practice name> maintenance department who maintains all maintenance and other logs. <insert practice name> has redundant internet and telephone services (Multi path digital fiber lines). When one provider experiences a service interruption, services is switched to the other provider.

In the unlikely event that both telephone systems should fail, <insert practice name> will have calls rerouted to individual business owned cell phones (of which there are five) by its telephone service provider.

If there is an outage in the network/server, <insert practice name> contacts the network service providers to determine the reason and cause and estimated restoration of the system. If there is a sustained outage (more than four hours), business will continue according to the following back-up procedures:

* + <insert practice name> staff will continue to process requests via phone, and/or secure fax or e-mail and manually record data.
  + Staff will document all necessary information in a Word document and save in a secured electronic folder.
  + When the network is restored, the information is then transferred into the electronic system and the word document is deleted.

In the event of damage to the physical server occurs; the IT department can restore 100% of data within 6 hours.

The IT Department maintains a recovery plan which enables reproduction of any lost information in the event of a disaster. The recovery plan is tested at least once every two years. Testing results are documented clearly and issues identified are corrected as soon as possible. **[Pharm Core 14 (d)]**

# Information Confidentiality and Security [Pharm Core 15 (a, b, c)] [PM 15, 17]

<insert practice name> understands the importance of securing confidential information and preventing security breaches. <insert practice name> works with their various customers/clients to ensure information is sent to <insert practice name> using only HIPAA compliant mechanisms. For example, <insert practice name> receives information from clients via secure systems when needed, <insert practice name> also utilizes a HIPAA-complaint facsimile. Additionally, <insert practice name> uses the following mechanisms to ensure security of its systems:

* Emails
  + <insert practice name> initiates e-mails with PHI only when absolutely necessary. All e-mails that contain PHI are sent and received using Sophos encryption.
* Voicemail
  + <insert practice name> staff may receive PHI via their voice mail boxes which are secured through password access and deleted once received. <insert practice name> staff do not leave voice mails containing PHI.
* Computers
  + <insert practice name> networks contain a firewall. Staff ensures the storage and use of their computer adhere to HIPAA requirements in regards to password policies. All computers utilized at <insert practice name> are password protected, maintained out of the direct view of passersby, and screens are locked when not in use. All pharmacy PHI data is maintained in the secure <insert pharmacy computer system> system which also requires a separate password to access.

<insert practice name> also utilizes Sophos antivirus software to detect and contain viruses. <insert practice name> ensures all applicable contracts with IT support and storage companies require that antivirus software be installed and new signature files are loaded and up-to-date.

<insert practice name> maintains intrusion software to detect, contain and correct security breaches. <insert practice name> also requires the maintenance of intrusion software of all its applicable IT support and storage contracts. Additionally, to help ensure continuous security of confidential information, <insert practice name> conducts an annual assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of information systems. In addition to conducting an annual assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of information systems <insert practice name> also conducts an assessment of the potential risks and vulnerabilities to the confidentiality and integrity of its physical location. A third-party vendor is used to conduct annual security audits. **[PHARM Core 15 (a)]**

# Breach Response

All suspected or actual security breaches are reported immediately to the HIPAA Security Officer. The officer will initiate the investigation within 2 business days of the report and respond to the compliance issues in adherence with all applicable regulations. The IT Vendor will actively participate in the investigation, response, and implementation of corrective actions related to the security breach. For all founded breach incidents the following response steps will be enacted by the IT Vendor or designee in collaboration with the IT Security Officer:

* 1. Take immediate steps to contain the breach and mitigate risk. The IT Vendor will evaluate the need and engage an IT Security company that offers incident response services if deemed necessary.
  2. Conduct a thorough Incident Specific Risk Assessment that evaluates all involved systems and operational practices within 30 days of the breach discovery.
  3. Develop and oversee the implementation of a corrective action plan within 60 days of the breach discovery to remedy all identified issue, including the revision of policies, workflows, and staff re-training as necessary.
  4. Draft and send breach notification to the required recipients within 60 days of the breach discovery or sooner if indicated by state regulations. This breach notice will follow the most stringent requirements of HIPAA, HITECH, and state regulations, including notification timeliness, content, and route of delivery.

# Confidentiality of Patient Health Information [Pharm Core 16 (a, b, c, d)]

Use of PHI

<insert practice name> personnel utilize PHI only to the extent necessary to carry out their assigned role. Only those individuals directly involved in the pharmacy process are allowed system access to sensitive information. Other <insert practice name> personnel are denied access to PHI via system security levels. Login and security level are at the job level, and access is only assigned to a job level if it is required to perform the job function.

Personnel Access to PHI

<insert practice name> personnel having access to Pharmacy PHI include:

* + Pharmacist Managers
  + Pharmacists
  + Pharmacy Tech
  + Administrative Staff
  + IT System administrator for system maintenance and reporting

<insert practice name> files and securely stores paper prescriptions; no other paper files are maintained. Any paper generated containing PHI is placed in secure shred bins and appropriately disposed of by the vendor, State Record Keepers. Tape recordings of telephone conversations where consumer health issues are discussed are strictly forbidden. Voice mail messages on <insert practice name>’s telephone system are deleted by users upon receipt.

# Responsibility and Requirement to Preserve Confidentiality [Pharm Core 16 (e, f)]

<insert practice name> has created a culture of respect for all persons and most importantly, respect for the personal health and other information of all persons. All <insert practice name> personnel receive training on HIPAA and HITECH compliance annually and all personnel sign confidentiality attestations. All <insert practice name> personnel understand that the responsibility of <insert practice name> to preserve the confidentiality of individually- patient health information is implemented by each and every <insert practice name> employee, contractor, and board member. <insert practice name> personnel, and board members understand that failure to comply with the preservation of confidentiality may result in disciplinary actions that may include termination and additionally they could be held personally liable for criminal prosecution and financial penalties.

RESOURCES:

AMENDMENT/TERMINATION: This policy may be amended or terminated at any time. Here is the revision history.

|  |  |  |
| --- | --- | --- |
| **DATE:** | **REVISED BY:** | **REVISION:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |