ADMINISTRATIVE PROCEDURES

SECTION: 600 – Information Technology	**PROCEDURE #:** 601 - A
TITLE: Texting	**IMPLEMENTS POLICY #:** 601
SPONSORING DEPARTMENT/DIV: Support Services/Information Technology	
EFFECTIVE DATE:	**REVIEWED:** 10/18/2016

OBJECTIVE: To establish procedures for protecting and maintaining the County's public records and other information from the risks created through use of text messaging.

PROCEDURES:

1. Risks of Texting.
   The County is legally required to maintain public records and to protect confidential, sensitive and protected information. Transmitting information by wireless text messaging, utilizing carrier supplied standard apps, poses a number of risks, including:
   - 1.1. Text messages are not encrypted.
   - 1.2. Text messages can be circulated by recipients or forwarded and may be stored.
   - 1.3. Text messages can be received by unintended recipients.
   - 1.4. Text message senders can misdirect text messages.
   - 1.5. Text messages can be used as evidence in legal proceedings.
   - 1.6. Text messages are public records that must be maintained but are not stored on the County network.
   - 1.7. There is no centralized system for archiving text messages subject to Public Records retention requirements. Employees and volunteers ("Users") using text messaging assume the responsibility of assuring the content is retained.
2. Secure Text Messaging Client.
   Tiger Text is the County approved secure text messaging client. Texting within Tiger Text assures message encryption and retention compliance objectives are fulfilled. Tiger Text provides default retention of two years for all text messages processed. Access to the Tiger Text client is facilitated by ITS.
3. Acceptable Use.

3.1. Users must obtain approval from the User's supervisor to use texting in the conduct of County business. The approval should include the specific types of situations in which texting will be deployed as a communication tool.

3.2. Users are responsible for ensuring recipient phone numbers are accurate and to periodically contact text message recipients to determine if they want to continue to communicate via text messaging.

3.3. As a best practice, Users should avoid sending or receiving text messages that:

3.3.1. Are subject to public retention laws; and/or

3.3.2. Include confidential, sensitive, and protected information.

3.4. Users considering the risks associated with text messaging who determine it prudent or job essential to utilize text messaging, are obligated to assure compliance with Public Records retention requirements and to protect confidential, sensitive and protected information.

4. <u>Guidelines for Public Records Retention - Managing and Retaining Public Records Stored on Mobile Devices.</u>

4.1. Text and Instant Messages.

4.1.1. Text messages sent and received in the course of conducting County business must be retained in accordance with Public Records retention rules. Mobile devices intentionally used for generating and receiving texts relating to County business, requiring either retention or secure processing, are to be enrolled in the County approved secure texting service. This service provides an app which secures messages during transmission, limits the life span of messages on the mobile device, and provides an automatic, secure retention service on a hosted server.

4.1.2. The County standard text messaging app (Tiger Text) provides two years of retention for all messages. Users are obligated to find alternate longer term retention solutions when that two year threshold is insufficient for fulfilling the retention requirement for a text message due to content. The guidelines for complying when messages requiring retention are received outside of the secure text messaging app outlined in the next section are applicable as options for Users when retention requirements exceed two-years.

4.1.3. See Attachment B for an overview of "Tiger Text," the County approved Secure Text service.

4.2. Responding to Messages Requiring Retention and Security Received Through Carrier Provided Text Messaging Service.

It is recognized that despite the User's intentions to avoid generating and receiving messages, subject to retention policies, it is not possible to prevent the receipt of messages containing such content from senders through the standard carrier provided text messaging client outside of the secure text messaging service. The User's

obligations extend to assuring that retention and security requirements are addressed. The following options to assure appropriate retention are outlined:

Option 1 – (when the information received requires retention, but is not sensitive) Text-to-Text . Forward the text messaging from the standard client to the County provided secure text messaging environment. Resending sensitive information text-to-text with the non-secure texting client is not appropriate – see Option 4.
Option 2 – Copy/Paste information from the standard client into the County provided secure text environment and send it to appropriate personnel.

Option 3 – Email Transfer (when the information received requires retention, but is not sensitive) - Select and copy the message content, paste it into an e-mail addressed to County e-mail account, send the e-mail, and retain it in your email archive in accordance with the applicable document retention schedule. The e-mail automatically records the date, time, and message recipient identity. Resending sensitive information text-to-email is not appropriate – see Option 4.

Option 4 – Manual. Transcribe the message content and retain such transcription(s) in accordance with the applicable document retention schedule. Record the date, time, and identity of the message recipient in the transcription. This is the only appropriate option for retaining sensitive information received outside of the secure texting service as it avoids the rebroadcast of sensitive information in plain text format.

4.3. Documents, Photographs, Audio, Video and Other Files.
For documents, photographs, audio, video, and other files that constitute public records, that are created or updated on a mobile device, transfer all such files as e-mail attachments to the User's County e-mail account and retain them in accordance with the applicable document retention schedule. If the files are too large for an e-mail attachment, contact the IT Help Desk for assistance.

5. Guidelines for Safeguarding Text Messages Containing Confidential, Sensitive or Protected Information.
Users should take precautionary measures to ensure that the User's device is safeguarded against theft or unauthorized access to stored data. This includes but is not limited to:
   5.1. Ensure the device is password protected and is configured to timeout after no more than 10 minutes of inactivity.
   5.2. Delete messages at the earliest opportunity.
   5.3. Report theft of a device as soon as possible. To report the loss of a device, or any security concern, contact the ITS Helpdesk during business hours or the Sheriff's Office Records Division after-hours.

Attachment A

Texting Examples

Acceptable Texting:

Example 1: Text is used to communicate factual and logistic information that is NOT subject to public records retention requirements, or other information related to County business.

County Sender: Hi John, Can we do lunch today 1 pm?

Internal or External Recipient: Nice to hear from you Dave, that sounds good to me. See you at Buster's Rib house.

Example 2: Text used to communicate information related to County business that is (a) NOT confidential, sensitive and/or protected part of the County's work, and (b) that has been documented, or can necessarily be documented, in separate public record.

County Sender: Did you read the email from John Smith about the new road project?

Internal or External Recipient: Yes. I am concerned. I have transmitted my concerns in a reply email to him and we are working it out. [NOTE: Recipient is documenting his contact with John Smith in another format]

Texting requiring the secure texting service to assure content security and appropriate retention:

Example 1: Text used to communicate information related to County business (a) that IS confidential, sensitive and/or a protected part of the County's work,

County Sender: I just got back from my public health home visit with Gwen Smith. She is really hooked on [name of prescription medication].

Internal or External Recipient: Gosh, in all my years as a public health nurse, I've never seen a worse case. At this rate, she will die soon. I feel bad for her little one.

Example 2: Text to communicate information related to County business that is confidential AND subject to public records retention a requirement that has NOT been documented in separate public record.

In this example, the exchange contains confidential information AND is subject to public records retention requirements; however the sender IS NOT documenting their communication on this matter in a separate record.

County Sender: John, I really need you to make your clinic appointment today or there will be consequences.

John: I don't feel good today. Can we reschedule :\

County Sender: Okay, let's do it tomorrow at the same time, but I'm not going to reschedule again. You are missing many appointments not just with me but with your Anger Management and AA.

John: Okay man. I'll try to do better.

Attachment B

Tigertext Secure Messaging Fact Sheet

TigerText is a secure cloud-based instant messaging application that is focused on enterprises, healthcare, and financial service organizations that must comply with industry regulations such as HIPPA, SOX and FINRA. This solution offers major improvements in secure communication for enterprises, financial services institutions, governments, and healthcare providers.

The app includes the following features:

- Secure messaging with full encryption end-to-end
- Delivery confirmation showing when TigerText messages have been sent, delivered, and read
- Integration with Active Directory (AD) and Lightweight Directory Access Protocol (LDAP)
- Record, attach, and send voice files for more detailed messages
- Do Not Disturb feature with custom auto-replies
- Multiple Inbox Support enabling you to use multiple TigerText accounts from the same device
- Pin Lock support with 4-digit numeric PIN settings (currently disabled, using MDM policies for device locking)
- Apple Touch ID support for unlocking the TigerText app (currently disabled)
- Message forwarding which is managed at the administrative level (currently disabled)
- Message deletion from both the sender and receiver devices after a set period of time or after reading

TigerText is compatible with any iOS, Android or Windows based devices

- iOS users can download the app from the Apple App store
- Android users can download the app from the Google Play Store
- Windows users can access their messages by using their web browser

- TigerText also provides an archiving service for text messages for up to 2 years that is in compliance with the County's retention policies
- TigerText users will log into the app on their mobile device or from a Windows web browser by using their County login ID and password

Instruction material will be made available at a later date.