Email Management: A Legal Perspective

The Texas A&M University System Office of
General Counsel

Agenda

1) Applicable Disclosure Requirements

2) Records Retention for Email

3) Confidentiality Obligations

4) Email Management Strategies

Applicable Disclosure Requirements

Applicable Disclosure Requirements

A. Texas Public Information Act

B. Audits and Investigations

C. Litigation (ESI)

D. Private Email Accounts

Scope of Texas Public Information Act

The Texas Public Information Act (PIA) guarantees copies/access to "**public information**." This means information that is collected, assembled, or maintained in connection with the transaction of official business.

1) Emails maintained by the university (**business emails**); or

2) Certain emails not maintained by the university if the university owns the information or has a right of access to it. (**business emails on private accounts**)

PIA Process Requirements

•The PIA's basic requirement is to provide copies or access to requested information promptly.

•Within 10 business days of receiving the request, the university must provide the information, inform the requestor of when the information will be provided, or request a decision from the state Office of the Attorney General.

•Information cannot generally be withheld unless the OAG determines an exception to disclosure applies.

•The Office of General Counsel writes decision request letters to OAG.

Process Requirements

- An email request for information does not become a request under the PIA unless **sent to designated public information officer/coordinator**. Refer requestor to this individual and do not forward the request!

- Every responsive email (including attachments) must be reviewed for confidential information or exceptions to disclosure.

Exceptions to Disclosure

•Exceptions to disclosure are either permissive or mandatory (confidential).

•We cannot decide to disclose confidential information.

•Usually, confidential information relates to a person's privacy.

•Usually, an AG decision is required. Some exceptions allow withholding/redaction without a decision.

Exceptions to Disclosure

- Examples
  - Confidential employee personal information (SSNs, DLs, account numbers, home contact information, medical information, etc.)
  - Confidential student information (FERPA)
  - Certain compliance investigations (civil rights, regulatory, laws, policies)
  - Certain UPD records
  - Third-party proprietary information

Exceptions to Disclosure, Cont'd

- Examples
  - Confidential research information
  - Privileged attorney-client communications
  - Private email addresses
  - Information harmful to university's competitive position re: contracting/bidding
  - Third-party proprietary information
  - Audit working papers

Audits and Investigations

- System Internal Audit (Scheduled Audits and Fraud, Waste, Abuse Investigations)
- Internal Civil Rights Investigations (Discrimination, Sexual Harassment, Related Retaliation)
- External Civil Rights and Compliance Investigations
- Criminal Investigations

Litigation

- After a suit is filed, a formal process for receiving information from the other parties in the case called **Discovery** begins.
- The discovery process has strict timelines and procedural rules. Discovery of electronically-stored information (ESI) has special rules.
- Similar process for state and federal court.

Types of Discovery Requests

- Interrogatories - questions to parties
- Requests for Disclosure - parties exchange basic information
- Requests for Admissions - reduces the number of facts each side must prove
- **Requests for Production - documents and ESI**
- Depositions (sworn testimony)- oral or written

Email as ESI

- Printed emails may be treated as documents during discovery.

- Emails stored electronically are ESI.

"Emails and deleted emails stored in electronic or magnetic form (as opposed to being printed out) are clearly 'electronic information.'" *In re Weekly Homes, L.P.*, 295 S.W.3d 309, 314 (Tex. 2009).

Discovery of ESI

- Scope of discovery is VERY broad!
- Preservation of discoverable ESI at outset of suit is critical.
- Formal process for preservation of documents and ESI is called a litigation hold.
- Producing ESI in native format is becoming standard.
- Backup tapes are discoverable!

Private Emails

- Emails sent to or from university email accounts that are **not** related to university business may not be subject to the PIA, but may be subject to disclosure under an audit, investigation, or discovery request (in litigation).

- Emails sent to or from private email accounts that relate to university business may be subject to disclosure under PIA, audit/investigation, AND discovery, regardless of where the emails are maintained.

In Summary

"University employees have no expectation of privacy in the use of email for University business. For instance, email messages relating to the conduct of University business that are maintained by the University and its employees, or in certain instances, its contractors, are subject to the Texas Public Information Act (Act)."

TAMU SAP 29.01.99.M2.01, *Employee Email*, § 1.1

In Summary

"Also, employee and student email messages may be subject to disclosure in audits, investigations, legal or regulatory proceedings. Therefore, employees should exercise care and good judgment in the use of email."

TAMU SAP 29.01.99.M2.01, *Employee Email*, § 1.1.

In Summary

"Private email accounts should not be used for conducting University business. In order to satisfy its obligations under the Act, an audit, investigation, or official proceeding, the University may require an employee to disclose any email messages residing in an employee's private email account(s) relating to University business. An employee failing to comply with such a request from the University will be subject to disciplinary action, up to and including dismissal."

TAMU SAP 29.01.99.M2.01, *Employee Email*, § 1.2.

Records Retention for Email

Records Retention

- State and System records retention requirements apply only to **state records**.
- This process is to ensure that records are kept for the appropriate amount of time prior to being destroyed or disposed.
- The term “state records” generally includes any information documenting university business, but only includes the official record copy kept for retention purposes.

Records Retention

- All copies of a record other than the record copy are "convenience copies" not subject to formal records retention.
- "Transitory information" is defined as records of temporary usefulness not ordinarily kept with state records preserved through records retention.
- Records not subject to records retention must be thoughtfully managed (created, maintained, destroyed).

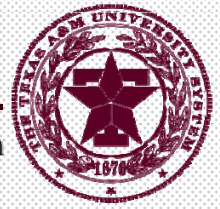
Records Retention and Email

- Content and function determines whether an email is a state record. Most emails are not state records subject to records retention. Most are transitory information or convenience copies.

- If an email truly is the record copy of a state record, it should be preserved accordingly as an electronic state record, including metadata.

- Transition of email should be part of out-processing employees.

Confidentiality Obligations



Confidentiality Obligations

- Emails that are truly confidential may not be disclosed unless required by the above processes and/or in accordance with law!

- Examples:

Student Education Records (FERPA), Medical Information, Common-Law Privacy, Confidential Personal Financial Information, Certain Research Information, 3rd-Party Proprietary Information

Email Management Strategies

Email Management Strategies

Institutions should:

1) Have a thoughtful email policy addressing disclosure and retention requirements and private email accounts (*cf*. TAMU SAP);

2) Require that auto-delete is used to purge emails from inbox, sent, junk, deleted folders after the smallest number of days practicable;

3) Have an established process to gather, preserve and review emails for disclosure under above processes; and

4) Have an electronic storage system for emails qualifying as state records. An email system or backup system is NOT sufficient!

Email Management Strategies

Faculty and staff should:

1) Avoid using personal email account(s) for business;

2) Segregate emails relating to research or student information into folders to enable quick identification, disclosure, preservation;

3) Be thoughtful in sending and forwarding emails, especially in copying to "all;"

4) Strongly consider enabling "auto-delete" if department or unit does not; and

5) Identify and preserve emails qualifying as state records.

Contact information

R. Brooks Moore

Managing Counsel, Governance

(979) 458-6144 (direct)

rbm@tamus.edu