# Commonwealth of Massachusetts

OFFICE OF THE COMPTROLLER

ONE ASHBURTON PLACE, 9TH FLOOR
BOSTON, MASSACHUSETTS 02108
TELEPHONE (617) 727-5000
WWW.MASS.GOV/COMPTROLLER

THOMAS G. SHACK III, ESQ.
COMPTROLLER


To: Department Heads, Chief Fiscal Officers, General Counsels, Department Security Officers and Internal Control Officers

From: Thomas G. Shack III, Esq.
Comptroller of the Commonwealth

Date: March 13, 2017

RE: Public Records Response Guidelines and Increased Security Reviews

**New Guidelines for Disclosure of State Financial Data**

The following guidance is being issued pursuant to M.G.L. c. 66, § 20 which authorizes the Comptroller to provide guidelines for requests of payroll, financial and other data residing in the Statewide Enterprise Accounting and Payroll Systems (MMARS and HR/CMS), and the security of these systems, or any associated data repository and how agencies may access and disclose public financial information while ensuring that exempted data is prohibited from disclosure and/or not wrongfully disclosed.

**Implementation of Increased Security Reviews and Security Access Controls**

The Comptroller has full authority to reduce, limit, halt or otherwise manage security access and records access in the MMARS and HR/CMS or any associated repository, including the Commonwealth Information Warehouse (CIW) or any Departmental or third-party hosted repository.

CTR is in the process of evaluating security profiles and may be reducing security access accordingly. Departments that require continued access to substantial personally identifiable information (PII) or sensitive information (SI) together known as “protected data” must demonstrate a documented need for the security. In addition, Departments may be required to show that they cannot conduct their business in another manner, and that they have documented internal controls that limit the number of individuals who have access to protected data.

As state and federal mandates increase the responsibility of Departments to secure protected data, the Comptroller will be identifying a broad range of information that Departments have an obligation to protect. Protected Data may be broader than what Departments are currently identifying as PII or personal information.

Protected Data includes information that can be used on its own or with other information to identify, contact, or locate a single person, or to distinguish or trace the individual's identity in context and any other information that is linked or linkable to an individual. Protected Data includes, but is not limited to, personally identifiable information (PII) under M.G.L. c. 93H and Executive Order 504, individual identifiable health information under HIPPA, State and federal tax information, student information under the Family Educational Rights and Privacy Act (FERPA), credit card information under the Payment Card Industry Data Security Standard (PCI-DSS), and other Protected Data as defined by NIST Special Publication 800-122, or as amended.

The Comptroller will continue to issue guidance for the appropriate handling of State Financial Data and protected data in accordance with proper internal control standards and information technology best practices.

**Public Records Requests Made To Departments or CTR for State Financial Data Posted on Transparency Site (CTHRU)**

Any Public Records requests made seeking State Financial Data records that reside on the Comptroller's transparency site CTHRU or another publicly available site, shall be directed to those sites for the requested records pursuant to M.G.L. c. 66, § 20 and c. 66, § 6A. Departments and CTR do not have to reproduce these records separately or create a new record to collate a response to a request for these records.

Departments are responsible for ensuring that protected data is not included in any Data field in MMARS or HR/CMS which is made available for release on the CTHRU site or pursuant to other Public Records Law requests.

If protected data is inadvertently included in a Public Data field in CTHRU, the Department must immediately notify CTR at **ctr-pir@MassMail.State.MA.US** to determine how to properly redact the Protected Data in CTHRU and make the necessary corrections in the source Enterprise systems (MMARS and HR/CMS).

**State Financial Data Not Posted on Transparency Site (CTHRU).**

Any public records request seeking State Financial Data records that do not reside on the Transparency Site CTHRU, or another site publicly available, pursuant to M.G.L. c. 66, § 6A, should be forwarded to CTR at **ctr-pir@MassMail.State.MA.US** to ensure that the records are public records subject to disclosure, and to confirm with Departments subject to the request that any required redactions are completed for protected data.

**Transaction Review Supporting Documentation**

If a record request is made for Department supporting documentation for transactions in either MMARS or HR/CMS that Departments are required to maintain in accordance with 815 CMR 10.00 or for other requirements, the Department must ensure that vigilant internal controls are in place to review responses to ensure that protected data is properly redacted, and is not merely hidden or masked in spreadsheets or other electronic records, to prevent wrongful access or disclosure.

Duplicate paper or electronic copies of records of State Financial Transaction supporting documentation submitted to CTR for secondary review are normally destroyed after administrative use when secondary review is completed. Public Records requests made to CTR for these records will be referred to the Department for disclosure of the official record pursuant to 815 CMR 10.00.

**Responses to Subpoenas and other Investigatory Orders submitted to CTR**

CTR may receive subpoenas or other investigatory orders to provide data from the State Enterprise Systems. In some cases these orders prevent notification to Departments. In permissible situations, CTR will notify Departments of the subpoena or other investigatory order.

Departments that receive subpoenas or other investigatory orders to provide data from the State Enterprise Systems should immediately notify CTR at **ctr-pir@MassMail.State.MA.US** to ensure that the data extracted is accurate and that protected data is not provided unless it is mandated by law, and that any protected data is segregated and secured in an appropriate manner to prevent potential data breach or compromise.

**Immediate Notice to the Comptroller**

In the event of a data breach or any suspected attack, attempted fraud, theft or other anomaly related to MMARS, HR/CMS or any associated systems, the Department must immediately notify the Comptroller the same day as the discovery, in addition to any internal reporting protocols and other reporting as required by law.

Questions and notices should be directed to **ctr-pir@MassMail.State.MA.US** for the fastest response.