Introduction

California State University (CSU) and SF State campus IT policy strongly recommends that all Level 1 data be encrypted. Loss or breach of Level 1, HIPAA and Personal Identifiable Information (PII) data usually requires breach notification to impacted individuals as well as federal and state oversight entities including the State Attorney General.

CA State law requires encryption at rest and in transit to avoid a breach disclosure notification. Federal and State breach disclosure requirements may be triggered if Level 1 data is lost or accessed by unauthorized individuals. To learn more about data elements that trigger additional security controls and breach disclosure please refer to SF State IT policy on Confidential Data.

If Level 1 data is unencrypted there needs to be justification or alternative risk mitigation for not encrypting the data. This exception is considered a high impact change request. SF State guidelines on Configuration and Patch Management Implementation require MPP-level approval for all high impact changes.

Breach Liability Estimate/Calculation

Average cost for loss of Level 1 data: $200 per record*.

The Average Loss Expectancy = Number of records with PII or FERPA restricted (CSU Level 1) data x $200 x average number of breach incidents

Example: if the number of Level 1 records is 5000:

Average Loss Expectancy = 5000 X 200

= $1000,000

- In additional to the above costs, it is common to provide impacted individuals with credit monitoring and restitution services.
- Loss of Electronic Protected Health Information (ePHI) data elements may incur additional fines, which could be as high as $1.5 million per violation.
- Breach of Level 2 data may require notification and Red Flag investigation of the incident. Cost for loss Level 2 data is estimated to be $10 per record.

*Based on industry averages and is subject to change.

Justification/Risk Mitigation
Risk Acceptance Form for Unencrypted Level 1 Data
Division of Information Technology (DoIT)

By signing below, I am accepting the business risk associated with unencrypted data.

_____________________________________________________
Name, AVP/Dean

_____________________________________________________
Name, Data Owner

Please Note: To be in effect, this document requires the signature of the AVP and the Data Owner whose Level 1 data is unencrypted. A completed signed copy of this form needs to be sent via email to the Mig Hofmann (Information Security Officer), Phoebe Kwan (Associate Vice President & Chief Technology Officer, Division of Information Technology) and Michael J Martin (Associate Vice President, Enterprise Risk Management).

References:

1. SF State Information Security program: http://tech.sfsu.edu/guides/information-security-program
2. Poneman Institute: http://www.ponemon.org/
4. HIPAA omnibus and HITECH civil penalty changes: http://healthitsecurity.com/2013/01/23/hipaa-omnibus-and-hitech-civil-penalty-changes/