

# CENTRAL MICHIGAN UNIVERSITY

[DATE]

OFFICE OF THE GENERAL COUNSEL  
1303 WEST CAMPUS DRIVE  
MT. PLEASANT, MI 48859  
989-774-3971  
FAX: 989-774-2477

TO: Members of the HIPAA Task Force  
FROM: Eileen Jennings  
SUBJECT: Application of all or part of HIPAA to various units of the University

We have had a number of conversations over the months about the application of the HIPAA regulations to various units within the University. I believe that we have all continued to have some degree of confusion about this. As you will see, our confusion is well founded.

All of HIPAA applies only to Covered Entities. For CMU, Covered Entities include health plans and health care providers who transmit any information in electronic form in connection with a covered transaction. Dennis has been correct in noting that, once an entity is Covered, the rules apply to the entire organization. However, at least for the Privacy regulations, the University considers itself a Hybrid Entity, which allows us to *define for ourselves* what units are included and excluded from our definition of CMU as Covered Entity. This definition is being developed, under the leadership of the Privacy Subcommittee. On the health care provider side, it basically includes Health Services and Communication Disorders and those other units of the University that would be Business Associates, if they were located outside the University. From our discussions, it appears that the other units included as part of CMU as Covered Entity (this Hybrid Entity) will be Receivable Accounting, Payable Accounting (possibly), Risk Management, Internal Audit, General Counsel, and possibly a few more.

The problem in applying the regulations arises because the concept of a Hybrid Entity is discussed only in the Privacy regulations. It is not carried over into the proposed regulations on Security. Dennis is correct when he uses only the definitions contained in the proposed Security regulations to define the extent of the application of those rules. Under the current proposed regulations, the Security rules would apply to the entire university, that is, to "all health information pertaining to an individual that is electronically maintained or electronically transmitted" at the University.

However, the proposed Security regulations are 4 years old. The Privacy and Electronic Transmission regulations were extensively revised before they were finalized, and it is expected that the same will occur with the Security regulations. For example, many of the definitions in the Security regulations have already been re-written for the other rules.

Chris Tellner and I talked with Marcia Malouin about this recently. She said that issuance of the Security regulations is still expected this October. She said that they must be

June 6, 2002

Page 2

issued 2 years before they can become effective. So the University will have at least until October of 2004 to comply with whatever is published. (After they are issued in final form, they can be amended once a year, as the Privacy regulations were, with only a 6 months grace period to comply.)

Ms. Malouin recommended that we assume that the Hybrid concept will apply to the Security regulations. Given all the uncertainties with the proposed Security regulations, I concur. At least until the final Security regulations are issued, I believe we should only apply the proposed regulations to those units considered part of the Hybrid Entity.

I recommend that **we consistently define Covered Entity as our Hybrid Entity**. When deciding whether any part of the HIPAA regulations apply to a unit or a transaction, the first step is to consider whether that unit is part of the Covered Entity, as we have defined it. *If the unit is not part of the Covered Entity, then HIPAA does not apply at all.* Exceptions to coverage based on FERPA or employment records maintained by the employer do not come into play at all. Those exceptions only apply to units that *are* part of the Covered Entity/Hybrid. This means that we will need to finalize (tentatively) the units that are included in the Covered Entity/Hybrid for the health plan as well as the health providers soon.

Example: Residence Life is not part of the Covered Entity. Its records are not covered by any part of HIPAA. It is not subject to the electronic transmission, the privacy or the security regulations. While it is not subject to those regulations, it also cannot have access to any of the health related records that are held by the Covered Entity (Health Services, etc.). Health Services, Receivable Accounting, etc. will be restricted in their ability to share information they obtain from Health Services of Compensation and Benefits with Residence Life. But for our initial "coverage of HIPAA" purposes, Residence Life is not a unit with which our Task Force must deal B at all.

Ms. Malouin noted that the University may wish to consider including some non-Covered Entity units within many of the security features we establish for HIPAA. Dennis has mentioned this several times. To the extent that it is possible to make some of the security features available to non-Covered Entity departments, that would be ideal. But the primary focus of our compliance should be on the Covered Entity/Hybrid units.

There are certainly risks in taking this approach, but they seem worth taking. I have asked Chris to include this item on the agenda for our next Task Force meeting for further discussion.

cc: Marcia Malouin