with the expanding growth and implementation of new and emerging technology in general, and electronic data interchange (EDI) in particular, misconceptions and fears about adherence to existing privacy and confidentiality requirements have arisen. While privacy and confidentiality require constant vigilance on our part, EDI presents very little in the way of new challenges. Existing legal protection currently speaks to this. The fact that we’re using a new technology, in this case EDI, is not a threat unto itself. It’s another tool of information management. The obligations to privacy and confidentiality remain, regardless of the technology.

EDI has been in use in the private sector since the early 1970s. In 1988 the American Association of Collegiate Registrars and Admissions Officers (AACRAO) began work on transaction set 130, the student record, later adopted as an official standard by the American National Standards Institute (ANSI). During this time post-secondary education has adopted computer-based record systems, microfilm, touchtone/voice-response technology, FAX, e-mail, World Wide Web, kiosks, and imaging systems, among others, as well as EDI. Why EDI in particular is being singled out as a threat to privacy and confidentiality of student information is unclear to me.

EDI is currently used by other industries to transmit your financial history, your medical history, your insurance history, your census information, your tax information, and a significant portion of Department of Defense purchase requests, among others. Educational institutions, with over twenty years of experience with legal obligations and constraints in the collection, maintenance, and release of protected information, has begun to transmit its information utilizing EDI technology. Is there suddenly a problem?

Much of the fear and misunderstanding is based, in part, I believe, on the misconception that we will suddenly ignore our current policies and procedures and begin the release of protected information simply because new and emerging technology provides another technical capability to do so. Many if not most of the fears about EDI and privacy/confidentiality often begin with “what if” statements. What if the data/information are released to unauthorized third parties, or what if secondary usage is not controlled? How is the EDI transmission of student data, aggregate or personally identifiable, less secure or more threatening than current methods, e.g., tape exchange? Currently we send hardcopy records into that great unknown called the U.S. Postal System. Does the record actually arrive, does it arrive in time, is it actually handled by the appropriate person? (Never mind what address or addressee you’ve indicated, mail handling procedures are concerned with speed and sorting, not security and confidentiality.)

The irony is that new technology, especially EDI, can provide far superior protection of information than that which is currently in use. Currently we are perfectly willing (and within legal obligations) to accept anonymous mail requests signed with signatures we don’t recognize from people we don’t know. We then expeditiously send protected information to people we don’t know at an address we’re not familiar with for purposes unknown to us, and not knowing if it ever arrived in the hands of the correct person. In the same scenario using EDI, possibly with the use of public/private keys, the request for the student record might arrive in encrypted format, be authenticated, the student record encrypted, sent to a previously agreed upon address, and its receipt acknowledged.

(continued on page 53)
surance that the presentation accurately reflects trends in a real-time fashion. For example, previously run reports—such as those that reveal student satisfaction with CBA/GSB and student ratings of teaching performance—can be compared to current results to track the school’s trajectory toward its goal of consistently high satisfaction. This kind of analysis and reporting is important, because faculty rewards and tenure are tied to merit and demonstrated performance. Furthermore, news that can be readily understood, in pie-chart form for example, is ideally suitable for public dissemination via student and alumni newsletters, the local news media, and so forth.

Another representative use of the ERDW is helping to take the once-a-semester frustration out of course planning. As departments construct schedules of courses, the dean’s office must evaluate the entire schedule. A review by the dean’s office assures students that they will not find required classes offered by the different departments scheduled at conflicting times. Previously, these conflicts were identified and resolved by a tedious manual process that involved office staff posting notes for each class to the office wall and checking for same-day, same-time conflicts. This process is now completed quickly and accurately using the new system.

Early results like these demonstrate the value of continuing our investment in the data warehouse concept and additional phases of implementation. As one of the next steps, we will again collaborate with administrators, who have now become familiar with the potential of the ERDW, in order to develop pre-built objects that will handle as much as 75 percent of most administrators’ querying needs and greatly increase the convenience of the system. The balance of ad hoc queries will be done by users themselves using the query tools. In Phase 2, we will add to the library of queries and bring in all relevant student data, followed by the addition of financial data in Phase 3.

Conclusion

One of the key lessons learned is that the system should be designed in such a way that it can be expanded or enhanced later in increments. In addition, the vendor’s commitment at the very beginning of the process is an important key to a successful, ninety-day launching. We were gratified that our software vendor shared our commitment to spending the time necessary to clearly research and understand the University’s needs before beginning to devise new hardware/software recommendations. Following a standard but flexible approach thereafter enabled us to consistently meet project milestones and the ninety-day completion target. The collaborative approach and focus on the original goals, phase by phase, helped us avoid distractions that can easily sabotage projects of this nature.

The authors would like to thank Sara Gill, Lead Systems Analyst for the CBA/GSB Computer Services, who was team leader for the ERDW project.

Electronic Messenger...

(continued from page 43)

However, increased levels of protection of information is analogous to protection of your home. It’s a balance, an attempt to find an appropriate comfort level. Using bars on your home windows (like using high level/complex encryption algorithms on data transmission) provides security, but limits the number and types of communication exchanges. Institutions will make determinations as to their comfort level with new technology just as they currently do with phone, e-mail, FAX, etc. The greatest threats to privacy/confidentiality are similar to the greatest threats to security of any correspondence or information. That is, the greatest threat is not in the transmission or interception of the information/correspondence, but rather with the particular level of integrity and commitment of staff in the originating and receiving offices.

Unfortunately, some people are demanding that new and emerging technology interpret and establish new and more expansive policies and procedures surrounding privacy and confidentiality. We seem to be ready to hold technology hostage while we try to come to consensus on matters of privacy and confidentiality. The application of technology within privacy and confidentiality context is somewhat analogous to writing instructions for the computer: It will do your bidding; you only need be clear as to what exactly it is that you think you’re asking for.

Educational institutions, quite often in the locus of the Registrar’s Office, have routinely made decisions and evaluations regarding the collection, maintenance, and release of information within the context of privacy and confidentiality. New and emerging technology, particularly EDI, does not change the way we’ve been “doing business” for the past twenty years. As long as the stewards of protected information continue to act in their heretofore responsible manner, new and emerging technology should be considered an opportunity and not a threat.