White Paper ■

Guidelines for the Clinical Use of Electronic Mail with Patients

Beverley Kane, MD, and Daniel Z. Sands, MD, MPH, for the AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic–Patient Electronic Mail.

A b s t r a c t   Guidelines regarding patient–provider electronic mail are presented. The intent is to provide guidance concerning computer-based communications between clinicians and patients within a contractual relationship in which the health-care provider has taken on an explicit measure of responsibility for the client's care. The guidelines address two interrelated aspects: effective interaction between the clinician and patient, and observance of medicolegal prudence. Recommendations for site-specific policy formulation are included.

■ **JAMIA.** 1998;5:104–111.

The purpose of this document is to guide clinicians and health care delivery organizations in the use of electronic mail (e-mail) communication with patients so that this method of communication might enhance the value of, rather than introduce complications into, the provider–patient relationship.

Health care organizations differ in the methods they adopt to communicate with patients. The task force acknowledges that it is not realistic to prescribe a detailed set of practices for universal implementation. The guidelines that we present are based upon our accumulated experience and the current literature. All recommendations should be adapted to individual circumstances. Ongoing evaluation of the guidelines is needed within a variety of institutions and relationships.

Definition

Patient–provider electronic mail is defined as computer-based communication between clinicians and patients within a contractual relationship in which the health care provider has taken on an explicit measure of responsibility for the client's care. This guideline does not address communication between providers and consumers in which no contractual relationship exists, as in an online discussion group in a public support forum.[1]

Background

Although there is some literature in praise of electronic messaging between providers,[2–5] there is a paucity of published research on the subject of patient–provider e-mail, and no long-term studies of which we are aware.

The Nature of E-Mail

E-mail is a hybrid between letter writing and the spoken word. It is more spontaneous than letter writing and offers more permanence than oral conversations. Words in e-mail can be more carefully chosen than in telephone conversation. While unencrypted electronic messages may, in theory, provide less privacy than postal mail or telephone calls, in practice e-mail replaces and is used more like the telephone but with less urgency. Because of its asynchronous nature (vol-

leying back and forth over hours or days), e-mail helps prevent "telephone tag" and avoids the interruptions associated with telephone calls or electronic pages.

E-mail follow-up allows retention and clarification of advice provided in clinic. Often patients under the duress of illness forget to ask important questions. Self-care instructions might not be fully understood or retained. E-mail creates a written record that removes doubt as to what information was conveyed.

E-mail is especially useful for information the patient would have to commit to writing if it were given orally. Examples include addresses and telephone numbers of other facilities to which the patient is referred; test results with interpretation and advice; instructions on how to take medications or apply dressings; pre- and postoperative instructions; and other forms of patient education. Some frequently used educational handouts can be ported to an e-mailer template or formatted for the provider's home page on the World Wide Web.

E-mail messages can embed links to educational materials and other resources on the clinic's Web site or on external sites. In some electronic mail applications, clicking on a "live" universal resource locator (URL) link inside a mail message launches a web browser and takes the user directly to the indicated resource. Clinics can provide lists of URLs on a particular topic, such as pregnancy, and create e-mail reply templates with pointers to frequently used reference sites.

While telephone messages are often overlooked, forgotten, or lost under piles of charts, e-mail messages are less likely to accidentally fall through the cracks of a busy practice. Voice mail systems can be plagued with irksome branching menus, lapses on hold, and the threat of telephone tag. Many callers hang up in frustration. With or without annoying automated systems, telephone messages are typically relayed along the "sneakernet"—a physical chain of human transmission from receptionist, to nurse, to doctor—with many "While you were out . . ." slips lost in the process.

In contrast with telephone conversations, e-mail is self-documenting: Copies of e-mail can be printed or attached to the patient's electronic record.

Finally, since many malpractice claims can be traced to faulty communication, good communication is part of good insurance.

E-mail at the Millennium

Technically minded, electronically equipped health care consumers have accelerated the demand for e-mail access to their health care providers.[6] The use of e-mail has dramatically increased from 100,000 users in the late 1970s to about 50 million users in 1997, with over 100 million users predicted by the year 2000.[7] This trend correlates with the advent of low-cost Internet access, mass-marketed online services, and employer-provided e-mail accounts to an estimated 30 to 40 million employees.[8] Thus, 15% of the population of the United States is currently using e-mail, and this number will naturally continue to increase.

Estimates of physician use are not as readily available. In 1996 one author[9] estimated that over half the physicians in the United States had personal computers, and at least 20% had gone online. A conservative estimate would be that the percentage of e-mail use among physicians is at least that of the overall population. As more health care organizations provide e-mail accounts to physicians, this proportion will rise.

In many locales, consumer-driven demand is urging health care providers, both individuals and institutions, to establish a mechanism for e-mail exchanges. Electronic access to a clinic's providers and educational resources is also likely to be a market differentiator in the health care industry.[10]

Clinician–Provider E-mail

Neill et al.[11] surveyed 117 e-mail–equipped patients at a university-based family practice center. Less than one-third of the patients reported that their physicians had an e-mail address, and only about one-third of those (10 patients) had used e-mail to communicate with their physicians. Of those who did not use e-mail with their doctors, half had never considered it, one-third reported no need to do so, one cited confidentiality concerns, and one felt uncomfortable. Almost all who had used e-mail for this purpose felt satisfied. A significant majority felt that e-mail would be a useful way to communicate with their physicians. They cited speed, convenience, utility for managing simple problems, efficiency, improved documentation, and avoidance of telephone tag as positive characteristics.

In another university-based practice, Fridsma et al.[6] studied patient attitudes toward patient–provider communication. In this Silicon Valley locale, almost half the patients had access to e-mail, most through their workplaces. About one-quarter were already using e-mail to communicate with their providers, and another quarter said they would do so if e-mail were available. The respondents expressed concerns about confidentiality, especially when e-mail access was through their employers.

Table 1 ■

Summary of Communication Guidelines

- Establish turnaround time for messages. Do not use e-mail for urgent matters.

- Inform patients about privacy issues. Patients should know:
    Who besides addressee processes messages
        During addressee's usual business hours.
        During addressee's vacation or illness.
    That message is to be included as part of the medical record.

- Establish types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc.) permitted over e-mail.

- Instruct patients to put category of transaction in subject line of message for filtering: "prescription," "appointment," "medical advice," "billing question."

- Request that patients put their name and patient identification number in the body of the message.

- Configure automatic reply to acknowledge receipt of messages.

- Print all messages, with replies and confirmation of receipt, and place in patient's paper chart.

- Send a new message to inform patient of completion of request.

- Request that patients use autoreply feature to acknowledge reading provider's message.

- Maintain a mailing list of patients, but do not send group mailings where recipients are visible to each other. Use blind copy feature in software.

- Avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages.

Other reports are anecdotal. Green[12] described proper use of e-mail and mentioned the more cost-effective management of capitated patients. In an interview with Green and two other physicians who use e-mail to communicate with their patients, Ojalvo[13] discussed the benefits and addressed privacy issues. Some authors also suggest guidelines for use.[14,15]

Guidelines

Guidelines for using e-mail in a clinical setting address two interrelated aspects: effective interaction between the clinician and patient (Table 1) and the observance of medicolegal prudence (Table 2).

In these times of increasingly impersonal, truncated, and regulated care, clinic time with patients is often compromised. If a provider anticipates a need to contact a patient again soon with regard to test results or other follow-up, he or she should inquire about the patient's communication preferences. Informally, the provider can ascertain preference for e-mail, telephone or voice mail, or postal exchange at the time of the visit, and document it in the chart. A more formal arrangement entails the use of informed consent, discussed below. Patients might elect e-mail, telephone or voice mail, personal meeting, or the postal route at different times for different purposes. The provider should confirm on a periodic basis which route to use for communication.

Prescription refills, lab results, appointment reminders, insurance questions, and routine follow-up inquiries are well suited to e-mail. It also provides the patient with a convenient way to report home health measurements, such as blood pressure and glucose determinations.

Issues of a time-sensitive nature, such as medical emergencies, do not lend themselves to discussion via e-mail, since the time when an e-mail message will be read and acted upon cannot be ascertained. Sensitive and highly confidential subjects should not be discussed through most e-mail systems because of the potential for interception of the messages and the po-

Table 2 ■

Medicolegal and Administrative Guidelines

- Consider obtaining patient's informed consent for use of e-mail. Written forms should:
    Itemize terms in Communication Guidelines.
    Provide instructions for when and how to escalate to phone calls and office visits.
    Describe security mechanisms in place.
    Indemnify the health care institution for information loss due to technical failures.
    Waive encryption requirement, if any, at patient's insistence.

- Use password-protected screen savers for all desktop workstations in the office, hospital, and at home.

- Never forward patient-identifiable information to a third party without the patient's express permission.

- Never use patient's e-mail address in a marketing scheme.

- Do not share professional e-mail accounts with family members.

- Use encryption for all messages when encryption technology becomes widely available, user-friendly, and practical.

- Do not use unencrypted wireless communications with patient-identifiable information.

- Double-check all "To:" fields prior to sending messages.

- Perform at least weekly backups of mail onto long-term storage. Define "long-term" as the term applicable to paper records.

- Commit policy decisions to writing and electronic form.

tential for transmission of messages to unintended recipients.

Patient–Provider Agreement

In general, the use of e-mail depends upon negotiation between patient and provider. Negotiation should focus on the following issues:

- *Turnaround time.* Ascertain how often both parties retrieve e-mail, and establish a maximal turnaround time for patient-initiated messages. In some messaging cultures, natural selection has evolved a one-business-day turnaround for nonurgent phone calls, and a two- to three-business-day turnaround for e-mail. As e-mail gains ascendancy as a preferred medium, messages may need to be checked and sorted by priority (triaged) several times a day.

  Often, the context of the patient's message will indicate the expected turnaround time. A patient who inquires about the results of a routine cervical smear will tolerate a longer messaging interval than one who is experiencing even mild side effects from a medication.

- *Privacy*. Indicate whether the office staff or nursing staff will triage messages, or whether mail addressed to the provider's private account will be read exclusively by the addressee. Also, establish with whom the physician may share a patient's e-mail message and under what circumstances, such as when consulting with another physician.

- *Permissible transactions and content*. Especially if other clinic staff will be processing e-mail from patients, establish the extent of action permitted over e-mail—prescription refills, medical advice, test results, release of records, etc.—and the topics. Stanford University Medical Clinic, for instance, forbids discussion of HIV status, mental illness, and workers compensation claims in electronic mail.

- *Categorial subject headers*. Instruct patients to specify a transaction type in the "Subject:" field of their messages. This convention will facilitate redirection of messages, by software with filtering capabilities, to the pharmacy, lab, nurse, or appointment clerk. Since many e-mail addresses consist of nicknames, patients should also be asked to write their full names and a patient identification number, if any, in the body of the message.

- *Discreet subject headers*. Providers should use discretion in their outgoing message titles. Patients may have fewer safeguards on their desktops than they need for their own privacy. "About Your HIV Test" is not an acceptable subject header.

These points should be discussed with the patient and the discussion documented in the record. A more conservative approach would be to commit the agreement to writing. In that case, have the patient sign the document, give a copy to the patient, and place a copy in the patient's chart. A summary of the policies and standards should be available on the clinic's web site. For example, the Stanford Medical Group's external web page on Electronic Mail Services illustrates how these policies can be conveyed to patients.[16]

Handling of Messages

- *Automatic reply to incoming messages*. E-mail software should be configured to send automatic replies in response to all incoming messages from patients. Replies should be of the form, "Your message has been received by Dr. Leslie Smith. I will attempt to process your request within one business day. If you need immediate assistance, please call Pat, my nurse, at 444-555-6666."

  In addition, out-of-the-office replies should be activated on any e-mail account that will not be serviced by staff or covering physicians during an absence that exceeds the established e-mail response time. Such messages should include the provider's estimated date of return and instructions on whom to contact for immediate assistance.

  Some e-mail programs have sophisticated filtering mechanisms that trigger different automated replies for patients, colleagues, and unknown correspondents. At this writing, about half of the 12 most commonly used e-mail applications provide filtered automatic reply capability.[17] The UNIX ".vacation" script affords simple auto-reply but requires UNIX shell privileges, is too cumbersome for the average user, and sends the same message to all parties.

- *Archiving of e-mail transactions*. E-mail exchanges constitute a form of progress note. Unless the provider is using an electronic patient record that allows the inclusion of e-mail messages, each e-mail message should be printed in full and a copy placed in the patient's paper record.

  The following steps result in efficient archiving: (1) Include the full text of the patient's query in the e-mail reply. (2) Copy the reply to the sender (provider). When the Internet delivers the provider's copy, which now includes both the original message and the provider's reply, the message should be printed and filed in the chart. Printers must operate in an area that is accessible only to staff and not to other patients.

■ *Confirmation of action on patient's request*. A new reply message should be sent out upon completion of patient's request for prescription refills, records transfer, and other transactions.

■ *Acknowledgment of messages*. For messages containing important medical advice, patients should be instructed to acknowledge messages by sending a brief reply. When such acknowledgment is expected, the printed (chart) copy should not be filed until this confirmation is received.'

In the absence of such confirmation, it cannot be assumed that the patient has received, much less read, important instructions. When in doubt, confirm delivery by telephone.

■ *Escalation of communication*. E-mail from providers should include a footer (signature file) that invites patients to escalate communication to a phone call or office visit, should they feel that e-mail is insufficient. The footer should give the appropriate contact information. Providers may need to actively discourage the use of e-mail as a substitute for clinical examination.

■ *Address book and group mailings*. Each provider should maintain a list of patients who communicate with him or her electronically. The address book feature of nearly all e-mail software permits easy maintenance of such a list. If it becomes necessary to notify the general patient population, or a group of patients, of an impending shutdown for network maintenance, recent mail blackouts, new clinic services, or a change of address, the clinic will have a ready-made mailing list. However, group-addressing, where those in the group see each other's names, should never be used to send mail to patients. Even the fact that a person sees a particular health care provider is confidential information. In addition, patients have become indignant about open inclusion on lists like the age-revealing list of women who are due for mammograms.

When sending out group mailings, use the "blind cc:" (blind carbon copy, or blind courtesy copy) software feature to keep recipients invisible to each other. When using this feature, enter the provider's own name in the "To:" field and place the list of recipients in the "bcc:" field.

■ *Emotional content of e-mail*. Irony, sarcasm, and harsh criticism should not be attempted in e-mail messages. The impersonal nature and ambiguity of e-mail often results in real or imagined exaggeration of animosity toward the recipient. Providers must realize that sick, anxious, or angry patients might indeed express stronger sentiments with e-mail than they would face-to-face or over the phone. Clinicians should make an effort to restrain their language despite their own stress and fatigue.

Clinicians should be aware that e-mail messages are typically stored for months or years on backup tapes. Pressing the delete button on the keyboards doesn't necessarily erase the message from the system. Such "deleted" messages containing disparaging, flippant, or incriminating remarks have come back to haunt physicians.

Medicolegal Issues

Aspects of electronic messaging of particular interest to risk management and legal departments concern data security and liability for advice. Medicolegal anxiety, however, should not be allowed to disable open communication as the basis for a healthy provider–patient relationship.

The most wary, not necessarily the best, approach dictates that patients be asked to sign printed guidelines by way of informed consent at the time an electronic relationship is established. In addition to the points detailed above, electronic messaging agreements should include, in nontechnical language:

■ *Description of security mechanisms in place*: an explanation of the general nature of the network and its level of security. Is the clinic using an intranet with a firewall? Is the provider or the institution directly on the Internet, or is there an intermediary Internet service provider (ISP) who conceivably monitors transmission? Is encryption software in use?

■ *Indemnity for technical features*: a clause to limit liability for network infractions beyond the control of the health care providers. Examples include system crashes, power outages, and overloads at the ISP level.

■ *Waiver of encryption requirement*: a mechanism for patients to opt out of the use of encryption if they do not wish (or are unable) to comply with the extra processing required. As of this writing there is no widely available, inexpensive, easy-to-use, highly secure, cross-platform encryption program suitable for global use.

Additional Recommendations

■ *Workstation screen*. Avoid leaving open e-mail on the computer screen. If the computer is in the same room as other patients, use a password-activated screen saver so that patient files are not visible to

other patients, especially if the provider is called out of the room.

- *Forwarding.* Never forward a patient's message or patient-identifiable information to a third party without the express permission of the patient. Text forwarded to a colleague for the purpose of consultation should not contain the patient's name or e-mail address.

- *Mailing lists.* Never use a patient's e-mail address in clinic marketing schemes or supply such addresses to third parties for advertising or any other use.

- *Headers.* Consider the use of a banner at the top of each e-mail message such as:

  –
  This is a CONFIDENTIAL medical communication.
  –

  Many commercial e-mail programs allow creation of stationery templates. Even simple UNIX-based mail programs such as *pine* can be scripted to create headers and footers.

- *Offsite processing of patient mail.* As with other parts of the medical record, patient-identifiable e-mail must not be taken out of the office. If providers answer e-mail from home, they must take special precautions to prevent other household members from intercepting messages from patients. Providers must not share e-mail accounts or passwords with friends, family, or nonmedical coworkers. Providers who communicate with patients should have their own accounts for professional use. Providers must see to it that e-mail processed off site on home systems or portable computing devices is subsequently printed in the office and included in the medical record.

- *Encryption.* As soon as practicable, clinics should establish a means of secure communication using the data encryption methods described below. Commercial encryption programs, encryption capabilities in commercially available e-mail software, and security features provided by the vendors of major clinical systems are becoming more common. The United States Post Office is testing a postmarking and encoding system specifically aimed at medical, legal, and financial transactions.[18] At least one semiconductor corporation is marketing a decoder ring device that provides security and encryption in a combination of wearable hardware and computer software.[19]

In March 1997 the Committee on Maintaining Pri-

vacy and Security in Health Care Applications of the National Information Infrastructure, under the National Research Council, released a comprehensive preliminary report on the privacy and security of health information.[20] Although the authors did not specifically address e-mail as a separate entity for security purposes, all their findings and recommendations are germane to this topic.

With regard to encryption the authors state: "... [S]ecurity tools based on cryptography are still largely undeployed anywhere in the public computing industry, much less in health care. In the sites visited, the committee found almost no use of encryption technologies except in a few localized experimental settings. . . ." Of additional interest is that the Committee acknowledges the tension that will always exist between the need for access and free flow of information and the need for security. Providers should be prepared to encounter patients who are sophisticated Internet users, aware of its privacy limitations, who nevertheless initiate unencrypted e-mail discussions of a surprisingly intimate medical nature. Wireless communications should never be used to transmit unencrypted patient data.

- *Avoidance of computer–human interaction error.* Mistakes due to poor interface design and lack of failsafe mechanisms are particularly troublesome in medical communications. By late 1996, there was litigation pending in the United States courts alleging that a physician inadvertently posted his patient's diagnosis of breast cancer to the public area of a major commercial online service. As the doctor and patient had had prior e-mail exchanges, the mistake was almost certainly due to an interface design characteristic in the client software. Such an error can occur when an e-mail application defaults to a "reply to all" feature rather than the "reply to sender (only)" option. Until foolproof software is available, and until e-mail is routinely encrypted, correspondents must habitually double-check the "To:" box in every message prior to sending.

Site-specific Policy Formulation

There is growing evidence to suggest that electronic resources, both e-mail and Web-based self-help documents, will result in substantial cost savings to clinics. Savings of time spent on the telephone will result from a reduction in telephone tag and a reduction of repetitious instructions. Many clinics, especially those with capitated plans, anticipate replacing inappropriate office visits with online support, including teleconferencing.

Health care institutions will need to develop written policies to address communication, technical, and medicolegal issues. Questions that must be answered include:

- *Triage*. Who will triage e-mail, and what is to be the response time?

- *Clerical overhead*. Who will print messages and place them in patients' charts?

- *Categorization and redirection of mail*. Will each provider have her own account, or will there be categoric accounts for all billing questions, medical questions, and scheduling questions?

- *Selective access for patients*. Should all patients be given the provider's e-mail address or can the provider give it out on a selective basis?

- *Archiving and backup*. How is e-mail cleared from the server? Does it stay on the provider's local machine or on the clinic or ISP mail server, or both? How are both repositories archived and cleared? How long should e-mail be stored on backup systems? How will messages be indexed for retrieval?

- *Forbidden topics*. Will the clinic disallow discussion of certain highly sensitive topics such as an AIDS diagnosis or psychiatric conditions?

- *Selective confidentiality*. Will patients be given a choice as to what content from their e-mail messages appears in the chart? If patients can opt to exclude material from the chart, will the clinic establish a secure repository, either electronic or paper-based, to recall the text of the original message? Or will the transaction be more like a phone call where the conversation is relegated to second-hand progress notes? How will providers handle a patient's request to omit material from his or her record when it is the clinic's policy to print all mail? Be aware that altering or expurgating a message, or sequestering an archive of private material, may be against state law and leave the clinic on shaky legal ground.

- *Encryption*. Will encryption systems be required? If so, how soon and what kind? Will patients be given the encryption software by the clinic?

- *Clinic-provided e-mail accounts*. Should clinics provide patients with e-mail accounts on the institutional server? Will such accounts be inside or outside the clinic's firewall?

- *Outcomes evaluation*. How will the efficacy and usefulness of e-mail with patients be evaluated? Will it be possible to determine utilities based on a monetary cost-benefit analysis, patient satisfaction, provider perception, or clinical outcomes?

A survey or focus group conducted among both staff and patients before instituting an e-mail policy will reveal important additional considerations innate to each venue. Seeking buy-in from all users and stakeholders will foster maximal cooperation with the new directives.

All policy decisions regarding electronic mail should be placed in the institution's policies and procedures manual, given to all staff in paper form, and be available in electronic form on individual workstations or on the clinic's internal Web site.

E-mail storage and retrieval must eventually be integrated with a comprehensive electronic medical record (EMR) and with patient education resources, some of them Web-based. EMRs over secure internal Internet sites, called intranets, seen destined to be the future of clinical computing services, and they will subsume e-mail functions. E-mail and other computer-based resources are not an entirely satisfactory substitute for face-to-face clinical evaluation, however. Ultimately, quality-of-care outcome assessments of adjunctive forms of communication must be benchmarked against physical contact.

References ■

1. Ferguson T. Health Online: How to Find Health Information, Support Groups, and Self-Help Communities in Cyberspace. Reading, MA: Addison-Wesley, 1996. See also: Ferguson T. A guided tour of self-help cyberspace. 1996. ⟨http://www.healthy.net/selfcare⟩.
2. Branger PJ, van der Wouden JC, Verboog E, Duisterhout JS, van der Lei J, van Bemmel JH. British Med J. 1992;305:1068–70.
3. Sands DZ, Safran C, Slack WV, Bleich HL. Electronic mail use in a teaching hospital. Proc Symp Comput App Med Care. 1993;306–10.
4. Pallen M. Electronic mail. Brit Med J. 1995;311:1487–90.
5. Nelson R, Stewart P. Use of electronic mail as a clinical tool. J Healthcare Information and Management Society 1996;8:33–6.
6. Fridsma DB, Ford P, Altman R. A survey of patient access to electronic mail: attitudes, barriers, and opportunities. Proc Annu Symp Comput App Med Care. 1994;15–9.

7. Forrester Research, Inc. The e-mail explosion. January 7, 1997. ⟨http://www.forrester.com/pressrel/970107PT.htm⟩.

8. Cavanagh MF. Workplace privacy in an era of new technologies. Messaging Magazine 2. May/June 1996. ⟨http://www.ema.org/html/pubs/mmv2n3/workpriv.htm⟩.

9. Bielski V. Modem malpractice. Hippocrates. November/December 1996.

10. Engstrom P. Can you afford not to travel the Internet? Med Econ 1996;73(13):173–80.

11. Neill RA, Mainous AG, Clark JR, Hagen MD. The utility of electronic mail as a medium for patient–physician communication. Arch Fam Med. 3(3):268–71.

12. Green L. A better way to keep in touch with patients. Med Econ. 1996;73(20):153–6.

13. Ojalvo HE. Take two, e-mail me in the morning. ACP Observer. December 1994;8–9.

14. Gareiss R. Electronic triage. Am Med News. April 23, 1994; 23–7.

15. Borzoi G. The ABCs of e-mailing patients. Am Med News. September 11, 1995;38:34–7.

16. Stanford Medical Group. Electronic Mail Services. ⟨http://www-med.stanford.edu/shs/smg/email.html⟩.

17. Venditto G. E-mail face-off. Internet World. December 1996; 7:12. ⟨http://pubs.iworld.com/⟩ (search on "e-mail face off").

18. Marketing News. U.S. post office testing electronic postmarks. 1996;30(22):16.

19. Dallas Semicomputer. ⟨http://www.ibutton.com/⟩.

20. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For the record: protecting electronic health information. Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics, and Applications; National Research Council. Washington, DC: National Academy Press, 1997. ⟨http://www.nap.edu/readingroom/books/ftr/⟩.