Confidentiality in the digital age

PRACTICE POINTER

Confidentiality in the digital age

Bradley H Crotty,[1] Arash Mostaghimi[2]

[1]Division of Clinical Informatics, Beth Israel Deaconess Medical Center and Harvard Medical School, Brookline MA 02446, USA
[2]Department of Dermatology, Brigham and Women's Hospital and Harvard Medical School, Boston, MA, USA
Correspondence to: B H Crotty
bcrotty@bidmc.harvard.edu

Cite this as: *BMJ* 2014;348:g2943
doi: 10.1136/bmj.g2943

bmj.com/multimedia
Listen to a podcast relating to this article

Digital technology introduces new concerns for confidentiality and information security. This review outlines the regulations governing confidentiality and medical privacy and provide practical advice on how to safeguard patient information

Confidentiality is a pillar of our profession. The patient-physician relationship is built on trust that enables patients to share intimate details. When deciding how to secure and transmit patient information, clinicians must apply professional judgment, informed by policies set forth by regulators and enumerated in local guidelines.[1] Electronic communication of patient information can facilitate clinical care, while mobile technologies and cloud computing boost productivity. However, these technologic innovations introduce new concerns for confidentiality and information security.[2]

We review "practice pointers" for clinicians to help them safeguard patient information in the digital age. We will focus on the professional setting while highlighting best practices for personal technology use. Where applicable, we point out current regulatory mandates, highlight grey areas, and offer practical advice for clinicians.

Regulations

Although the responsibility to keep patient information confidential may be rooted in professional ethics, governmental bodies regulate confidentiality and medical privacy in most countries. Laws such as the Data Protection Act in the United Kingdom,[3] the Data Protection Directive in the European Union,[4] and the Health Insurance Protection and Portability Act (HIPAA)[5] in the United States stipulate stringent rules for data security.

Privacy regulations are constantly in flux. Regulators routinely update rules, as seen recently in the US with the 2013 HIPAA Omnibus Regulations.[6 7] These new regulations stipulate that all entities involved with protected health information are subject to HIPAA regulations and must assume liability for breaches of protected health information. With every new change, physicians must review their business practices and agreements with vendors who have access to personal health information, making sure that these business partners are safeguarding data appropriately and are compliant with applicable regulations.

Regulations also specify how individual physicians may use and transmit protected health information (box). Sensitive data transmitted through the internet must be encrypted to prevent prying eyes during transmission. Likewise, sensitive data on laptops or USB flash drives should be encrypted in case of loss or theft. Encryption scrambles data so that only those who have a decoding "key" can access the file. The loss of unencrypted information requires physicians to assume that recovered data will be used for malicious or fraudulent purposes and to warn patients accordingly. Data that are lost, but appropriately encrypted, are not considered to put patients at risk. Physicians can install programs that encrypt laptops and use flash drives that offer encryption. Most smartphones can be encrypted by setting a passcode.

However, guidance from regulatory agencies will never be able to cover all situations and developing technologies.[8] For example, text (also known as short messaging service) messages are often not specifically covered by regulatory guidance, but because messages are sent without assurances of encryption, it can be inferred that they are not appropriate for transmission of protected health information.[9 10] Companies now offer secure text messaging as a service to medical providers, whereby they assume responsibility for encryption, data security, and user authentication. When guidance is lacking, we recommend that physicians turn to legal consultations and develop practice level policies and procedures to ensure that they have taken all reasonable steps to protect security.

Electronic communication

The use of email has limitations in healthcare. Inside most hospitals, clinicians and associated staff commonly communicate about patient care by email. Once an email message leaves a network, however, its contents generally travel unencrypted through the internet to the recipient, similar to a postcard traveling through the mail. To ensure

Recommendations for clinicians

Security awareness
Regularly review guidelines from local medical societies or professional organisations regarding information security

Personal technology
Use separate passwords for clinical systems and personal web services
Encrypt any mobile devices used for clinical work, including laptops, tablets, smartphones, external hard drives, and flash drives
For tablets and smartphones, encrypt devices by using the passcode feature within the device settings
Disable automatic photo "backup" on devices used to take pictures of patients

Cloud computing
Before using cloud computing services, assess whether the company offers secure data storage and sign a business associate agreement

Patient communication
Use secure communication, such as a patient web portal, when communicating with patients
If a patient requests traditional email over secure alternatives, provide and document informed consent regarding privacy risks and data security

Social media
Where feasible and appropriate, separate professional use of social media from personal use
Consider all postings public and permanent, regardless of settings
Avoid discussing individual cases online without patient permission

bmj.com

Previous articles in this series

- Assessing risk of suicide or self harm in adults (*BMJ* 2013;347:f4572)
- Diabetic ketoacidosis: not always due to type 1 diabetes (*BMJ* 2013;346:f3501)
- Necrotising fasciitis (*BMJ* 2012;345:e4274)
- Perioperative fluid therapy (*BMJ* 2012;344:e2865)
- Investigating the pregnant woman exposed to a child with a rash (*BMJ* 2012;344:e1790)

secure data exchange between practices or health systems, organizations are developing secure systems for information exchange.[11]

Until such systems are more generally adopted, fax machines will still be commonly used to communicate between practices. The use of fax machines is a holdover of past business practices and reflects exemptions from many regulations governing the transmission of electronic data. Online fax services cater to clinicians looking to bridge the gap between fax and email, and clinicians will want to use services that offer encryption and a business agreement that complies with regulations governing protected health information.

Physicians wishing to communicate with patients electronically can now send encrypted messages through commercially available patient web portals and related services. If such services are not available to the patient or the patient does not wish to use them, physicians can exchange information using traditional email, provided the patient knows about the privacy risks and agrees with the plan.[12]

As access to high speed internet connections expands, clinicians and patients may communicate through videoconferencing. Clinicians can choose from corporate telemedicine solutions to personal technologies, such as Microsoft's Skype or Apple's FaceTime, both of which can provide encrypted communication channels. However, regulatory guidance about videoconferencing is limited, and clinicians should work with their practices, in consultation with legal or compliance personnel, to choose a service and develop policies for its use.

Personal devices

The rapid evolution of personal computing increasingly blurs the lines between work and home use, and clinicians now routinely use the same devices for both professional and personal purposes. Although convenient, there is a danger of information breaches if proper safeguards are not used.[13] For example, if viruses or malicious software (malware) infect a device, user credentials and other information may be compromised, allowing access to confidential data. It is possible to use personal equipment, but physicians must be constantly vigilant about their device settings and personal usage patterns.

Physicians can take a few simple steps to safeguard data on their personal devices. All mobile devices used for clinical purposes must be encrypted, which involves setting a passcode to access the device. Devices can also be configured to be remotely "wiped" if lost or stolen. Clinicians should assess any new features to ensure that protected health information is not transmitted inadvertently. For example, a clinician who uses his or her mobile device to take a picture of a dermatologic finding should disable any automatic photo sharing through services such as Apple's Photo Stream, Dropbox, or Google+. Lastly, physicians should avoid unsecured networks, such as free wireless networks in coffee shops, to access sensitive websites on their mobile devices because usernames and passwords may be stolen.

Clinicians who use personal devices for work may wish to separate personal and professional information. For example, many email programs offer a "unified" inbox that allows email from multiple accounts to be viewed in one place. Although convenient, this combination may lead to professional messages being delivered accidentally through a non-secured personal mail account.

Cloud computing

Cloud computing refers to the storage and processing of digital information on remote computer servers.[14] This concept includes email storage, file storage, and web hosting, where a user can access the most up to date files through the internet, instead of carrying files locally on USB drives or laptops. Some companies extend cloud computing to facilitate analytic processing of data or the hosting of entire electronic health records on remote servers.

Cloud storage and other services are attractive because of convenience and low cost. The benefits are clear for busy clinicians who want access to their files from any location—home, office, or ward. However, physicians and organizations using cloud computing for protected health information need to assess their compliance with regulations. Business agreements should be in place with any third party companies that will be storing data; the agreements should specify that transmission to and from the cloud is secured and encrypted, and that appropriate user access controls are implemented.[15]

Social media

Several professional societies, including the American College of Physicians,[16] the American Medical Association,[17] and the General Medical Council in the UK, have recently published guidance for clinicians on the use of social media.[18] These recommendations discuss online physician identity, professional behaviour, and information security. In general, physicians should avoid using social media for direct patient care and contact, given that information may not be stored in an encrypted manner, may be inadvertently accessible to others, and may be controlled by a third party.

Physicians who use social media personally must be careful that they do not inadvertently expose information about patients. For example, blogging or posting the details of a case may allow patients to be identified. We have likened social media to a crowded elevator, where others can easily overhear conversations without the benefit of context.[19] Clinicians who want to write about patients online can avoid many problems by securing the patient's permission to write about his or her story in a public forum.

Physicians can take advantage of social media professionally to promote healthy behaviours among patients.[20] Practices may curate web content, or "push" out information about new health guidelines to communities of patients through their online profiles. From a confidentiality perspective, use of such a system would be best left to facilitate conversation around matters of public health or availability of services, rather than matters related to a specific patient. Patients should be given notice that such a system is not meant for clinical communication. If such a system is used, staff should routinely monitor social media accounts; if patients post sensitive information, staff should take these conversations offline and follow up with the patient by telephone.

Conclusions

As clinicians, we are stewards of our patients' personal information, and we have a professional duty to safeguard such information through the proper use of technology. We must be vigilant about the technology and systems that we use and take precautions to prevent inappropriate disclosure of patient information. As the amount and use of digital information increase, so does the risk of a data breach. Clinicians will be best able to protect information by being cognisant of the basic concepts of keeping data secure. These include device encryption, understanding local policies and regulations about information storage and transfer, and maintaining awareness of the settings on their devices. In areas where guidance is limited, clinicians should consult local experts.

The authors gratefully acknowledge John Halamka for his helpful insights when reviewing the manuscript.

Competing interests: We have read and understood BMJ policy on declaration of interests and declare the following interests: None.

Contributors: Both authors contributed to the conception and drafting of this article, gave their final approval, and will act as guarantors.

Provenance and peer review: Commissioned; externally peer reviewed.

1 Lo B, Dornbrand L, Dubler NN. HIPAA and patient care: the role for professional judgment. *JAMA* 2005;293:1766-71.
2 Slack WV. The issue of privacy. *MD Comput* 1997;14:8-11.
3 National Archives. Data Protection Act (c.29). 1998. www.legislation.gov.uk/ukpga/1998/29/contents.
4 The European Parliament and the Council of the European Union. Data Protection Directive 95/46/EC. *Stud Health Technol Inform* 1996;27:83-118.
5 Department of Health Human Services. Office of the Secretary. Standards for privacy of individually identifiable health information. Federal Register 2002:1-93. www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/introdution.html.
6 Mitka M. New HIPAA rule aims to improve privacy and security of patient records. *JAMA* 2013;309:861-2.
7 Department of Health and Human Services. Rules and regulations. Federal Register, 2013:5566-702. www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
8 Wang CJ, Huang DJ. The HIPAA conundrum in the era of mobile health and communications. *JAMA* 2013;310:1121-22.
9 Greene AH. HIPAA compliance for clinician texting. *J AHIMA* 2012;83:34-6.
10 Karasz HN, Eiden A, Bogan S. Text messaging to communicate with public health audiences: how the HIPAA security rule affects practice. *Am J Public Health* 2013;103:617-22.
11 Williams C, Mostashari F, Mertz K, Hogin E, Atwal P. From the Office of the National Coordinator: the strategy for advancing the exchange of health information. *Health Aff (Millwood)* 2012;31:527-36.
12 Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA internet working group, task force on guidelines for the use of clinic-patient electronic mail. *J Am Med Inform Assoc* 1998;5:104-11.
13 Kopytoff V. More offices let workers choose their own devices. *New York Times* 2011www.nytimes.com/2011/09/23/technology/workers-own-cellphones-and-ipads-find-a-role-at-the-office.html?pagewanted=all&_r=0.
14 Rosenthal DA, Layman EJ. Utilization of information technology in eastern North Carolina physician practices: determining the existence of a digital divide. *Perspect Health Inf Manag* 2008;5:3.
15 Department of Health and Human Services. Health information privacy: business associate contracts. 2013. www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
16 Farnan JM, Snyder Sulmasy L, Worster BK, Chaudhry HJ, Rhyne JA, Arora VM, et al. Online medical professionalism: patient and public relationships: policy statement from the American College of Physicians and the Federation of State Medical Boards. *Ann Intern Med* 2013;158:620-7.
17 American Medical Association. Opinion 9.124. Professionalism in the use of social media. 2011. www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9124.page.
18 General Medical Council. Doctors' use of social media. 2013. www.gmc-uk.org/guidance/ethical_guidance/21186.asp.
19 Mostaghimi A, Crotty BH. Professionalism in the digital age. *Ann Intern Med* 2011;154:560-2.
20 Hawn C. Take two aspirin and tweet me in the morning: how Twitter, Facebook, and other social media are reshaping health care. *Health Aff (Millwood)* 2009;28:361-8.

RATIONAL TESTING

Using haemoglobin A1c to diagnose type 2 diabetes or to identify people at high risk of diabetes

Eric S Kilpatrick,[1] Stephen L Atkin[2]

[1]Department of Clinical Biochemistry, Hull Royal Infirmary and Hull York Medical School, Hull HU3 2JZ, UK
[2]Weill Cornell Medical College Qatar, Doha, Qatar
Correspondence to: E S Kilpatrick Eric.Kilpatrick@hey.nhs.uk

Cite this as: *BMJ* 2014;348:g2867
doi: 10.1136/bmj.g2867

This series of occasional articles provides an update on the best use of key diagnostic tests in the initial investigation of common or important clinical presentations. The series advisers are Steve Atkin, professor of medicine, Weill Cornell Medical College Qatar; and Eric Kilpatrick, honorary professor, department of clinical biochemistry, Hull Royal Infirmary, Hull York Medical School. To suggest a topic for this series, please email us at practice@bmj.com.

A 48 year old man presented to his general practitioner with a 12 month history of fatigue (which he put down to long office hours) and with urinary frequency. He had no previous health problems, his blood pressure was 145/85 mm Hg, and his body mass index was 29. His father had developed type 2 diabetes at the age of 65 years, and his paternal grandmother had been found to have diabetes at the age of about 60 following the development of a gangrenous toe. The patient's dipstick urine test showed no glycosuria, ketonuria, proteinuria, blood, leucocytes, or nitrites.

What is the next investigation?

All the possible causes of fatigue should be considered,[1] but given the patient's symptoms and his risk factors for developing type 2 diabetes, including family history and being overweight, a diagnosis of diabetes certainly needs to be excluded. Tests for diabetes are used to evaluate both patients with symptoms (as in this case) and asymptomatic patients who have been identified by a validated risk assessment tool as being at high risk of developing type 2 diabetes.[2]

LEARNING POINTS

Haemoglobin A_{1c} (HbA_{1c}) can now be used as an alternative test to glucose concentration for diagnosing type 2 diabetes or identifying people at high risk of developing the disease

Be aware of the conditions in which use of HbA_{1c} would be inappropriate, including suspected type 1 diabetes, pregnancy, acute medical illness, and kidney failure

Also be mindful of conditions that might affect HbA_{1c}, such as abnormal haemoglobins and anaemia

Do not routinely test both glucose and HbA_{1c} in the same patient

Using glucose to diagnose diabetes

Since the early 20th century, the diagnosis of diabetes has been based on the measurement of glucose concentrations in the blood. This usually takes the form of laboratory measured fasting plasma glucose concentration and, when indicated, a glucose concentration two hours after an oral glucose load. However, "random" (post-prandial) measurement can suffice if it is unequivocally raised, especially in a patient with symptoms. The diagnostic thresh-

bmj.com
Previous articles in this series
- Ordering and interpreting hepatitis B serology (*BMJ* 2014;348:g2522)
- Investigating an incidental finding of lymphopenia (*BMJ* 2014;348:g1721)
- Estimated glomerular filtration rate (*BMJ* 2014;348:g264)
- Investigating polyuria (*BMJ* 2013;347:f6772)
- Investigating low thyroid stimulating hormone (TSH) level (*BMJ* 2013;347:f6842)

old concentrations for glucose in use by the World Health Organization are defined as those above which it is known that a person will be at high risk of developing, if they are not already present, the microvascular complications of diabetes, particularly retinopathy.[3] In non-pregnant adults, the main indication for an oral glucose tolerance test is when the fasting plasma glucose concentration lies between the values suggestive of normality and overt diabetes—namely, in the impaired fasting glucose range of 6.1-6.9 mmol/L inclusive. The two hour post-glucose load measurement can then help to distinguish patients who have solely impaired fasting glucose from those who have both impaired fasting glucose and impaired glucose tolerance (plasma glucose concentration 7.8 to <11.1 mmol/L) and from those who can be diagnosed as having diabetes purely on the basis of their two hour glucose result being 11.1 mmol/L or above (box 1).

Box 1 | Venous plasma glucose thresholds[3]

Diabetes mellitus
Fasting glucose ≥7.0 mmol/L or
Two hour post-glucose load ≥11.1 mmol/L or
Random glucose ≥11.1 mmol/L

Impaired glucose tolerance
Fasting (if measured) <7.0 mmol/L and
Two hour post-glucose load ≥7.8 to <11.1 mmol/L

Impaired fasting glucose
Fasting glucose ≥6.1 to <7.0 mmol/L and
(If measured) two hour post-glucose load <7.8 mmol/L

For asymptomatic patients, at least one additional glucose test result with a value in diabetic range is essential for diagnosis. Impaired glucose regulation refers to a patient who has either impaired fasting glucose or impaired glucose tolerance

Using haemoglobin A_{1c} to diagnose type 2 diabetes

As can be seen, measuring glucose in the blood to diagnose diabetes can be inconvenient for patients, as they are usually required to fast overnight; if an oral glucose tolerance test is needed, the procedure is laborious, time consuming, and costly. For this reason, in recent years, more consideration has been given to whether measurement of glycated haemoglobin—haemoglobin A_{1c} (HbA_{1c})—might be a valid alternative to glucose as a diagnostic test for diabetes, although this concept has led to controversy.[4] Quite apart from not requiring a patient to fast overnight, HbA_{1c} measurement has several other potential advantages over glucose (box 2), including its property of giving an indication of glycaemia over several preceding weeks rather than at a single time point and, partly as a consequence, reduced day to day variation within an individual compared with glucose.[5]

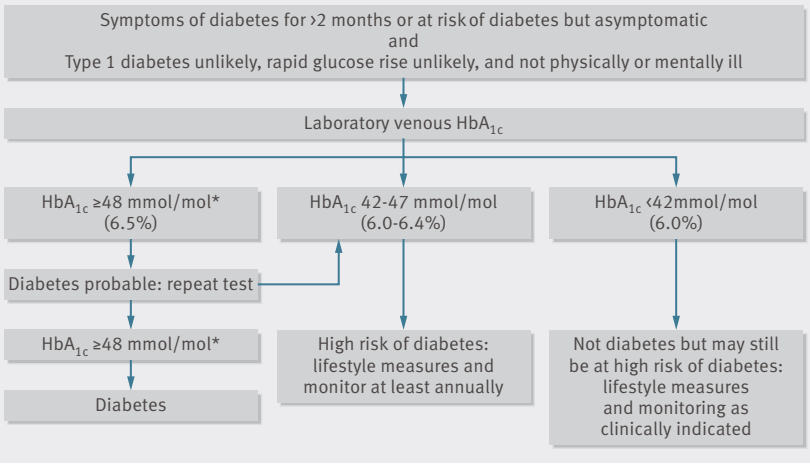
Advances in the global standardisation of HbA_{1c} measurement culminated in WHO publishing advice in 2011 that recommends an HbA_{1c} threshold of 48 mmol/mol (6.5%) or above for the diagnosis of type 2 diabetes but does not give specific guidance below this single value.[6] Since then, an expert committee in the United Kingdom, which included seven clinical professional bodies and National Health Service organisations, came to a consensus recommending that a diagnosis of diabetes should be made only after a confirmed raised HbA_{1c} value. The committee also introduced a new category of patients who are judged as being at high risk of developing diabetes solely on the basis of an HbA_{1c} value of 42-47 mmol/mol (6.0-6.4%) (figure).[7]

Box 2 | Advantages of HbA_{1c} over glucose in diagnosing type 2 diabetes

Does not require patients to fast, take a glucose solution (which can sometimes cause nausea), or return for second blood test after two hours
Assesses glycaemia over previous weeks or months
Lower biological variability than fasting glucose or two hour post-glucose load concentration
Fewer pre-analytical concerns, including time to analysis
Already used to guide management of diabetes
Standardisation of HbA_{1c} measurement should help with harmonising results between laboratories

When not to use HbA_{1c} to diagnose diabetes

One of the main advantages of HbA_{1c}—that it can give an indication of previous glycaemia—is also a disadvantage when hyperglycaemia could have developed rapidly, as



Using haemoglobin A_{1c} (HbA_{1c}) to diagnose type 2 diabetes in non-urgent situations. *HbA_{1c} values >120 mmol/mol (13.1%) are likely to indicate marked hyperglycaemia that may need urgent assessment

Box 3 | When not to use HbA_{1c} for diagnosis and when to be cautious

Do not use HbA_{1c}
All children and young people
Pregnancy—current or recent (<2 months)
Suspected type 1 diabetes, at any age
Short duration of symptoms of diabetes (<2 months)
Patients at high risk of diabetes who are acutely ill
Patients newly taking drug that may cause rapid rise in glucose, such as corticosteroids, antipsychotic drugs
Acute pancreatic damage or pancreatic surgery
Kidney failure
Patients being treated for HIV infection

Be cautious in requesting or interpreting HbA_{1c}
Patient has or may have abnormal haemoglobin
Patient is anaemic (any cause)
Patient is likely to have altered red cell lifespan (for example, post-splenectomy)
Patient has had recent blood transfusion

rises in HbA_{1c} will lag behind those of glucose. This is why the test is unsuitable in clinical situations such as suspected type 1 diabetes, as well as many of the others described in box 3. Also, most laboratories are able to analyse glucose much more rapidly than HbA_{1c}, so requesting HbA_{1c} could introduce delay in an acute situation. In kidney failure (chronic kidney disease stage 5), the picture is complicated by patients often having a combination of haemolytic, iron deficiency, and chronic inflammation anaemias as well as forming urea derived carbamylated HbA_{1c}, which can also affect some HbA_{1c} analyses. Several treatments for HIV are also known to influence the HbA_{1c} value independently of glycaemia. Measurement of HbA_{1c} is not recommended when determining whether a pregnant woman has gestational diabetes, as it seems to be a poorer predictor of adverse fetal outcome than is glucose.[8]

Other cautions with using HbA_{1c}

Although HbA_{1c} should not be used in the situations already described, caution must also be exercised when using HbA_{1c} in the presence of an abnormal haemoglobin or in conditions that may affect red cell survival (box 3).[7] For example, haemoglobin E will form HbE_{1c} instead of HbA_{1c}, which may lead to an incorrect assessment of HbA_{1c} depending on the particular measurement method used by the local laboratory. Haemolytic anaemia can cause low HbA_{1c} values compared with glucose measurements, and iron deficiency anaemia can cause a raised HbA_{1c}, although how much influence iron deficiency might have at the diagnostic threshold is not yet clear. After a splenectomy, the lifespan of red blood cells is often increased and so could lead to HbA_{1c} values that are higher than would be anticipated for the level of glycaemia.

HbA_{1c} increases with age beyond what can be explained by any changes in fasting glucose or two hour post-glucose load concentrations, and people with Afro-Caribbean or Asian heritage have higher HbA_{1c} values than do those from Europid descent, which also cannot be accounted for by differences in oral glucose tolerance test results. However, the relevance of these observations to the use of HbA_{1c} as a diagnostic test remains uncertain.[7]

Glucose or HbA_{1c} for diagnosis?

The diagnosis of type 2 diabetes can be made on the basis of either HbA_{1c} or blood glucose criteria being met. However, these will not identify an identical population of people, as they are not completely concordant with one another.[4] For this reason, UK recommendations advise that only one or other test is used to follow the same patient and not a mixture of the two. So if HbA_{1c} shows a patient to be at high risk of diabetes, he or she should be followed up using the same test rather than blood glucose also being measured at the same time or later. The exception is if HbA_{1c} measurement is initially or subsequently identified as being inappropriate for that person, in which case a change to glucose measurement is warranted.

Laboratory or point of care measurement?

Several instruments for rapid point of care testing of HbA_{1c} are available for the monitoring of patients known to have diabetes, but most of these analysers do not perform sufficiently well to be used for diagnostic purposes.[9] If they are used, the analytical quality needs to be able to match that of clinical laboratories.[6]

Outcome

This patient had his HbA_{1c} measured and found to be 44 mmol/mol (6.2%). As this placed him into the category of being at increased risk of diabetes, he was given lifestyle and dietetic advice and had an assessment of other cardiovascular risk factors. He was asked to report any worsening in his symptoms of diabetes should this happen before the annual HbA_{1c} measurements now planned.

Contributors: ESK and SLA both contributed to the writing of the article. ESK is the guarantor.

Competing interests: None declared.

Provenance: Commissioned; externally peer reviewed.

Patient consent: Patient consent not required (patient anonymised, dead, or hypothetical).

References are in the version on bmj.com..

Accepted: 2 April 2014

Who can diagnose Sheehan's?

Many years ago near the Turkish-Syrian border, a woman was brought to me by her husband, an illiterate farmer, because she was always complaining of fatigue. Attempts to take her medical history were not very productive, as the patient could speak no Turkish and her husband could speak only a little.

Her thyroid function tests showed secondary hypothyroidism. Further investigations suggested the diagnosis of Sheehan's syndrome, and her history of postpartum bleeding, provided by her husband, supported the diagnosis. Corticosteroids and thyroxine produced a dramatic improvement, and the patient and her husband were delighted by the treatment.

A few weeks later, I saw the husband again, but this time accompanied by a relative. "Doctor, this woman has the same disease," he announced. Did this mean I was expected to treat every woman in his village who complained of fatigue, tiredness, or generalised pain with steroids and thyroxine? Nevertheless, I requested tests after a physical examination. It turned out that this patient also had panhypopituitarism, and a similar obstetric history was obtained on further questioning. She received the same treatment as my first patient.

That is how I saw that an illiterate farmer may suspect and nearly diagnose Sheehan's syndrome based on the symptoms and medical history.

Serife Mehlika Isildak Başkent University, Ankara, Turkey
mehlikaisildak@gmail.com

Patient consent not required (patient anonymised, dead, or hypothetical).

Cite this as: *BMJ* 2012;345:e6437