MEDECINS EUROPEENS
EUROPEAN DOCTORS

Excerpt Results of Survey on Medical Confidentiality

24 February 2026

Excerpt Results of Survey on Medical Confidentiality

Background

- Two-tiered survey:
  - Aimed at National Medical Associations (NMAs) and European Medical Organisations (EMOs)
  - Complementary anonymous survey for individual doctors (to follow)
- Launched between 13/02/2025 – 20/06/2025
- **Disclaimers**
  - Survey is limited in time and number of responses
  - Responses are subjective, but allow capturing perceptions, attitudes, practices and main legal framework on medical confidentiality
  - This is an excerpt of the survey results for publication and dissemination.

Responses received from 20 countries:

Austria		Hungary	
Belgium		Ireland	
Bulgaria		Lithuania	
Croatia		Malta	
Czech Republic		The Netherlands	
Denmark		Norway	
Estonia		Portugal	
Finland		Slovenia	
France		Sweden	
Greece		United Kingdom	

Excerpt Results of Survey on Medical Confidentiality

Objectives

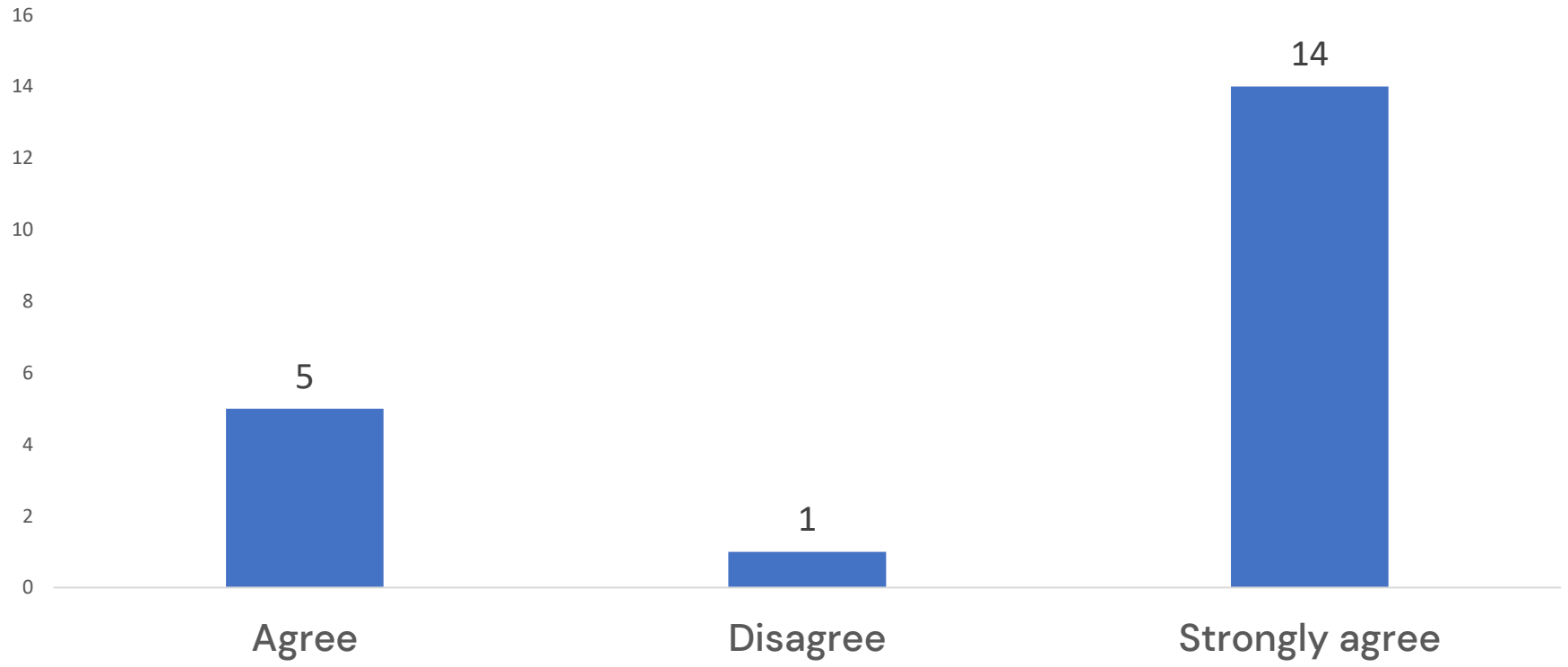
- Understand how countries are responding to the impact of healthcare digitisation, electronic health data sharing and emerging principle of data availability, on medical confidentiality
- Raise awareness to the “principle of health professional-patient confidentiality” identified in recital 24 of the European Health Data Space Regulation (EU) 2025/327

Historical importance

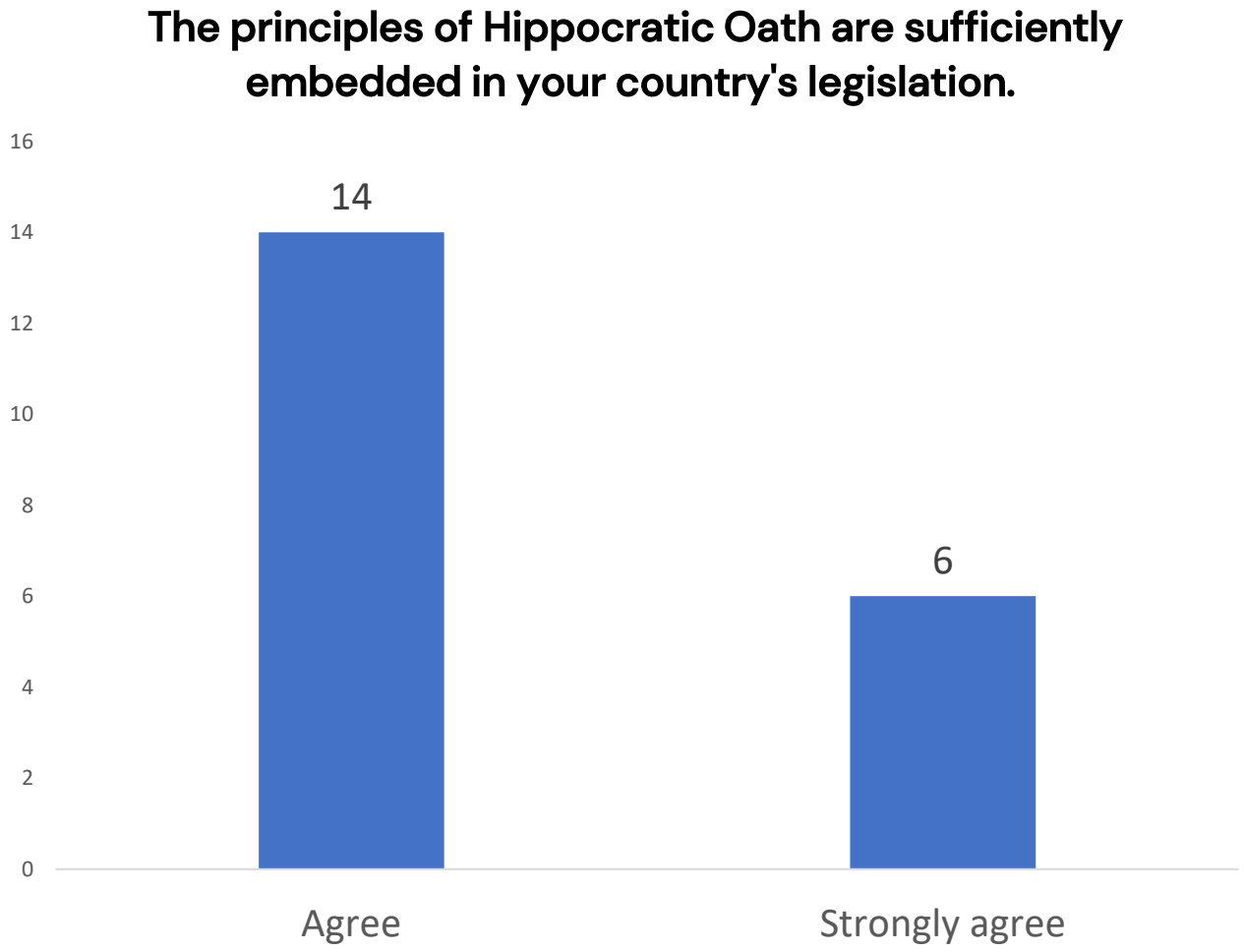
- No common definition on medical confidentiality
- Definition evolved with time
- World Medical Association’s role in safeguarding a common understanding of medical confidentiality and its application
- Doctors’ role from guardians of patient data to custodians

Excerpt Results of NMAs Survey on Medical Confidentiality

The **Hippocratic Oath** is important for medical confidentiality in your country.



Excerpt Results of Survey on Medical Confidentiality



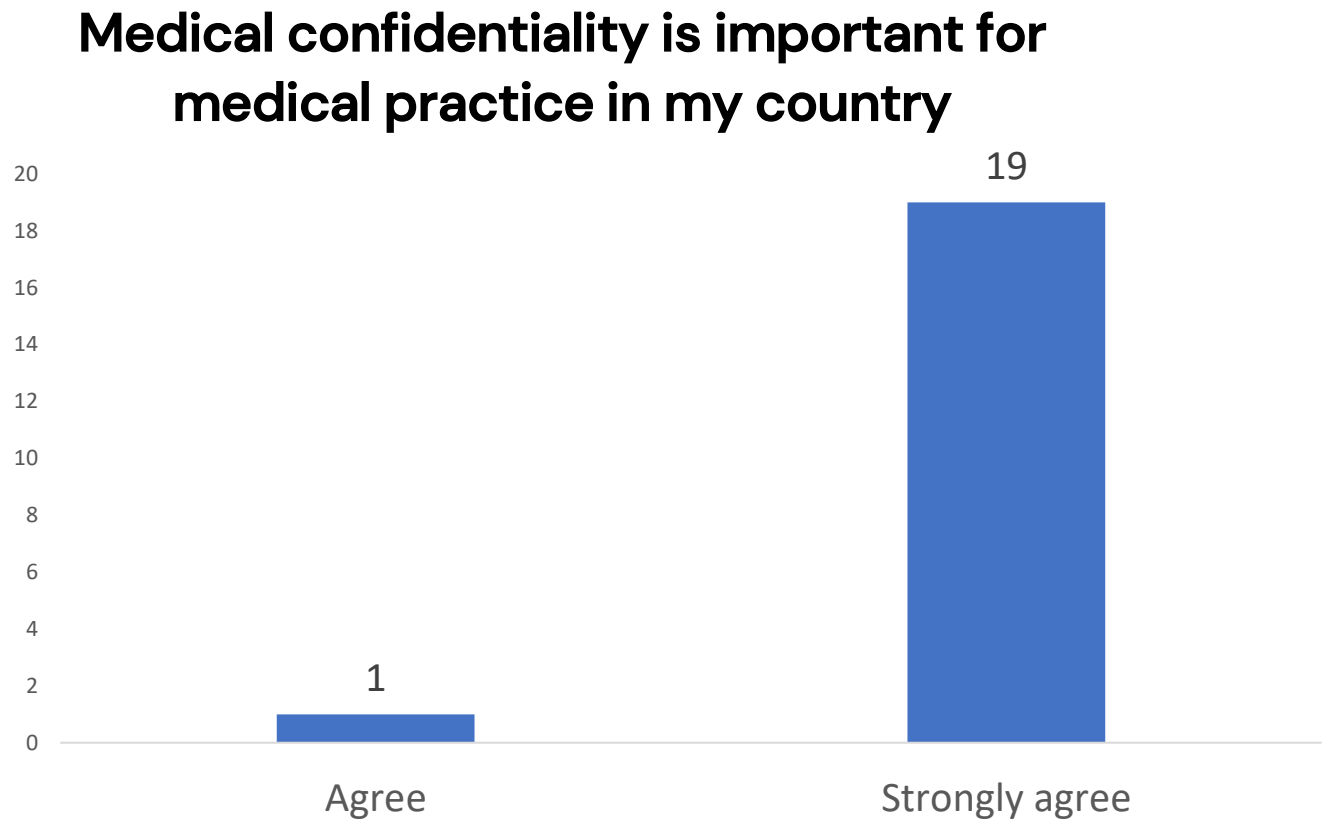
Comments:

- One national medical association commented that the original Hippocratic oath is **no longer used as it is outdated.** Basic ethical principles regarding confidentiality are found in the Medical Association's Code of Medical Ethics. Medical confidentiality is regulated in national law in legislation related to public access to information and secrecy Act, to patient data and to patient safety.

- One national medical association commented that the legal framework which applies to confidential information combines common law and statutes. The legal framework is supplemented by ethical and professional guidance from regulatory bodies and obligations under contracts of employment. When considering questions about confidentiality, healthcare professionals must look at the overall effect of the law, ethical guidance and their contractual obligations, not just each aspect in isolation. **The duty of confidentiality is not absolute, and confidential information can be disclosed** when one of the following circumstances applies:
    - the patient has capacity to consent and consents to the disclosure. This can be either: implied consent for an individual's direct care; or explicit consent;
    - the law requires disclosure;
    - the duty of confidentiality has been set aside by specific law; or
    - where there is an overriding public interest, that is, where disclosure is essential to prevent serious harm to the individual or a third party or to prevent or detect a serious crime in accordance with the professional ethical guidance.

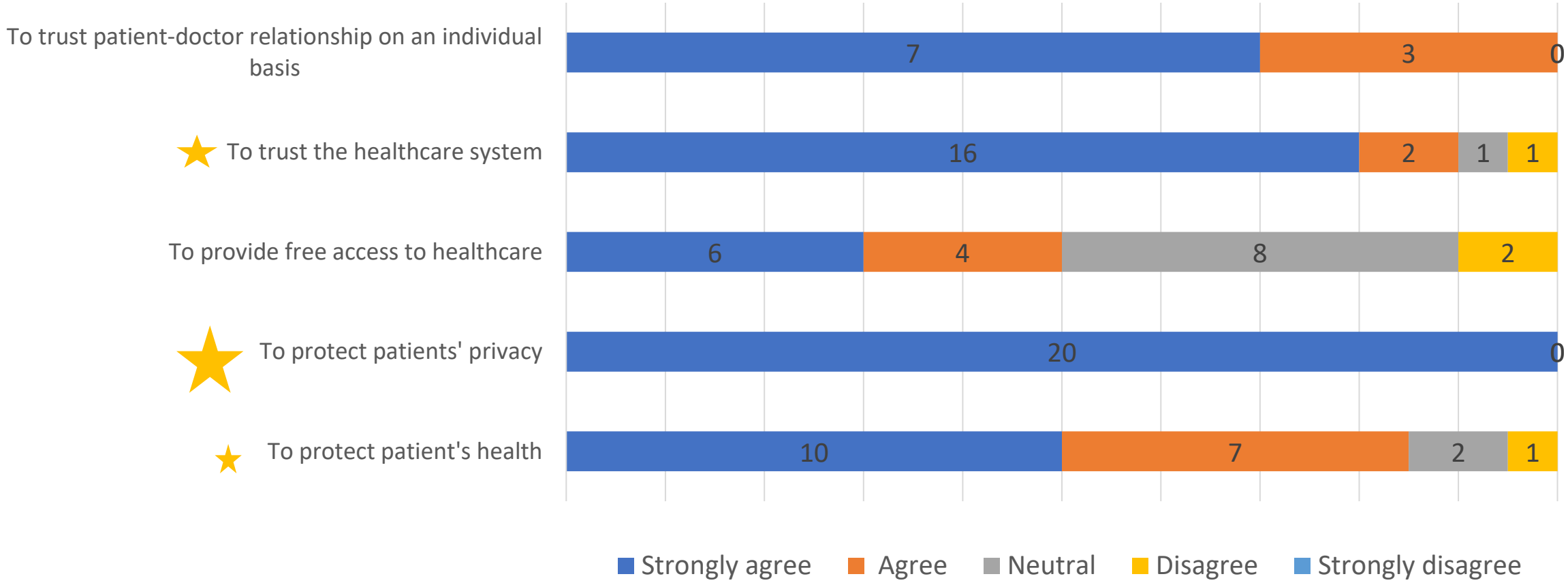
Excerpt Results of Survey on Medical Confidentiality

- All respondents either **agree or strongly agree** that MC is important for medical practice.



Excerpt Results of Survey on Medical Confidentiality

For which reasons should medical confidentiality be safeguarded?



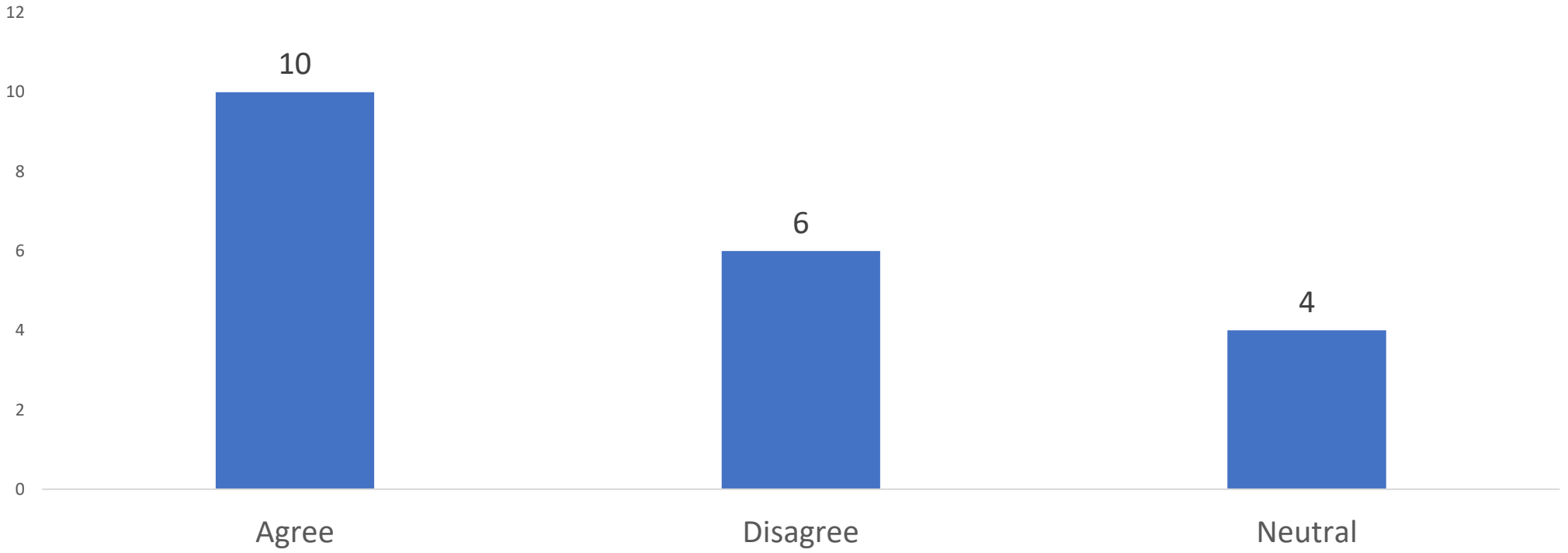
Excerpt Results of Survey on Medical Confidentiality

Other reasons for which medical confidentiality should be safeguarded:

- ❑ to avoid discrimination on health status
- ❑ to protect doctor's autonomy
- ❑ national security issues
- ❑ to socially guarantee trust in the medical profession.
- ❑ to ensure patients are willing to give away their personal and private information
- ❑ to fulfil the Hippocratic Oath
- ❑ to avoid harms:
    - patients' willingness to seek care; or when seeking care, patients' willingness to provide full and accurate information – detrimental of the safety and effectiveness of their treatment.
    - system planning, research, and innovation, which rely on the availability of accurate and representative data and which benefit wider society.

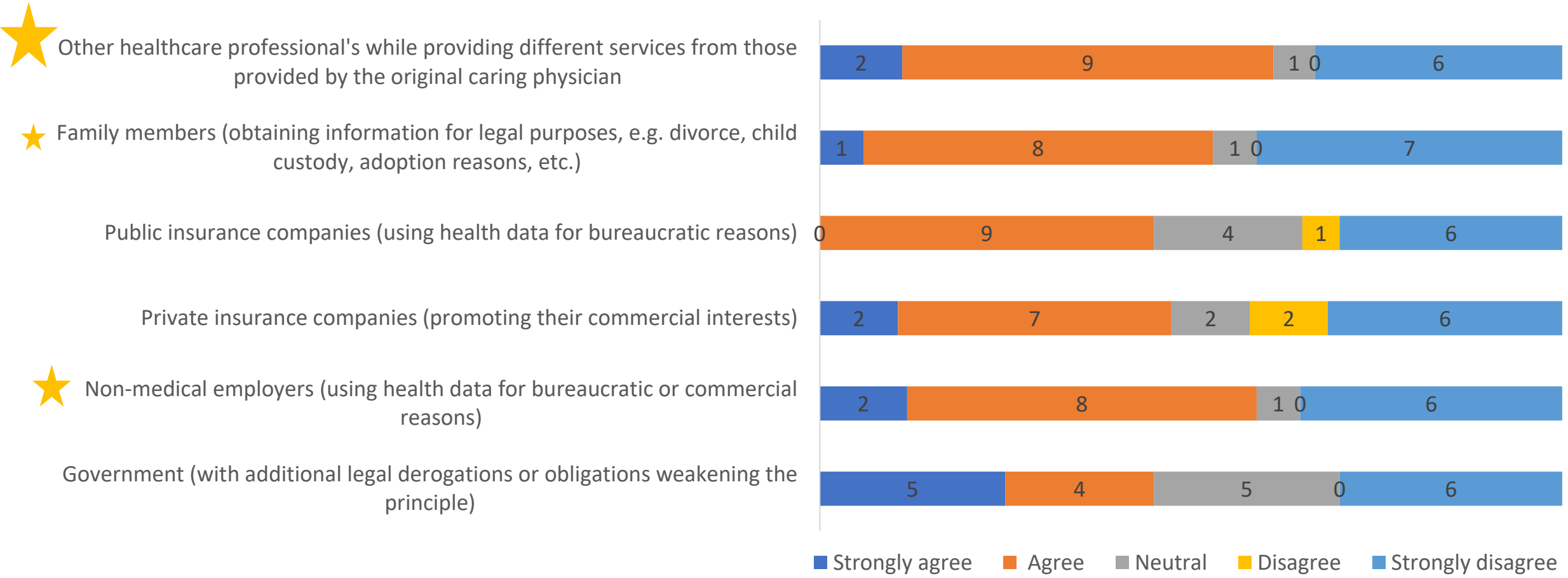
Excerpt Results of Survey on Medical Confidentiality

Medical confidentiality may be compromised with the use of electronic health records in my country.



Excerpt Results of Survey on Medical Confidentiality

By whom may medical confidentiality be compromised with the use of electronic health records?*



Excerpt Results of Survey on Medical Confidentiality

Other entities which can compromise medical confidentiality:

- Criminal organisations, foreign governments/ political blocks
- Media
- Legislation which requires physicians to inform authorities on issues related to child protection, [human] trafficking, though not directly linked to the form of EHRs
- Legal access is very limited for the groups mentioned in the previous question and it does not differ from paper medical records.

Excerpt Results of Survey on Medical Confidentiality

What are the most common grounds for disclosing patients' data in your country?

Perceptions or personal experience were considered in the absence of official data

Three **primary ranking reasons** for disclosing patient data:

- **Patient voluntary consent**,
- **Legal obligation** (duty to disclose) and
- **Legal authorisation** (voluntary to disclose)

Lowest-ranking reason:

- **Defend doctor's dignity or honour**

  [Note: In the UK, defending dignity or honour of doctors would not be a lawful or ethical ground for disclosure]

Excerpt Results of Survey on Medical Confidentiality

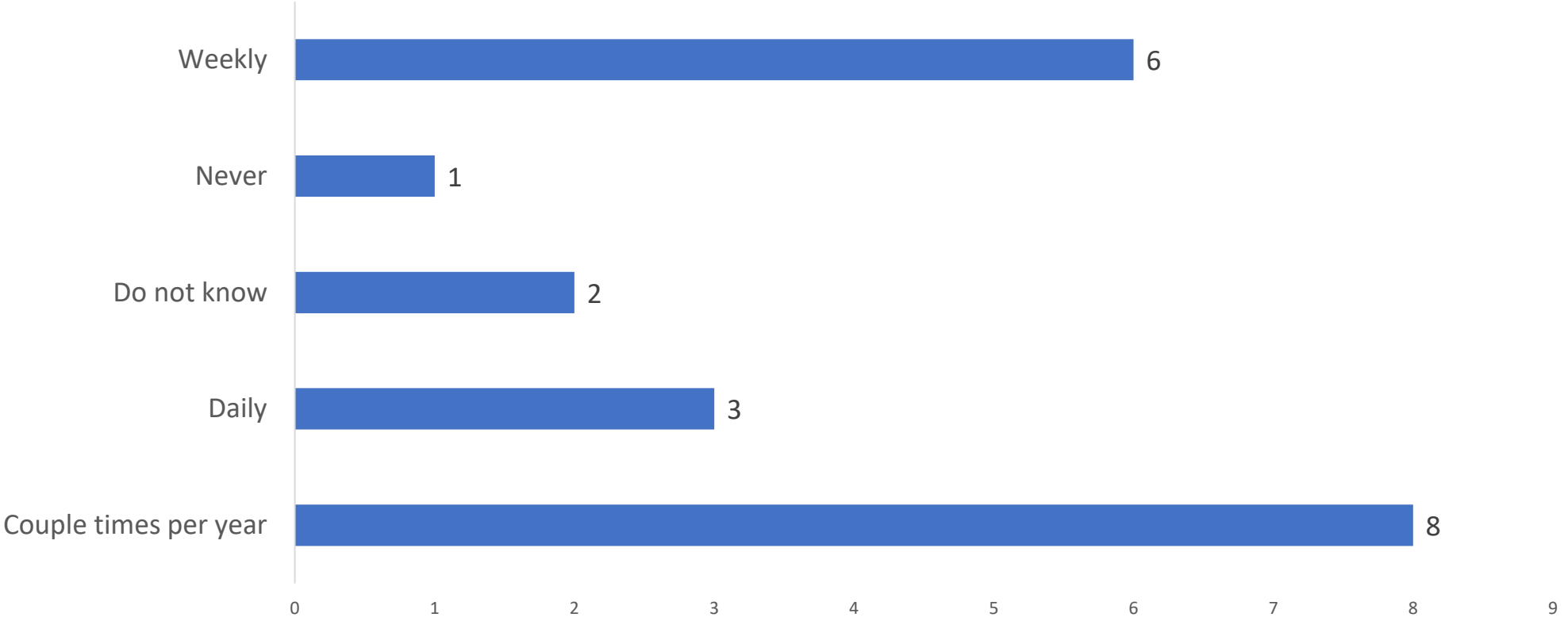
Other grounds for disclosing patient data:

- Law and professional standards refer to the **'public interest'** test for disclosures without consent which are necessary to prevent serious harm or prevent/detect serious crime.
- To investigate and control **notifiable diseases** in line with international legislative requirements.
- To help a patient or **protect health of children**, though uncertainty exist among doctors on these rules.

Excerpt Results of Survey on Medical Confidentiality

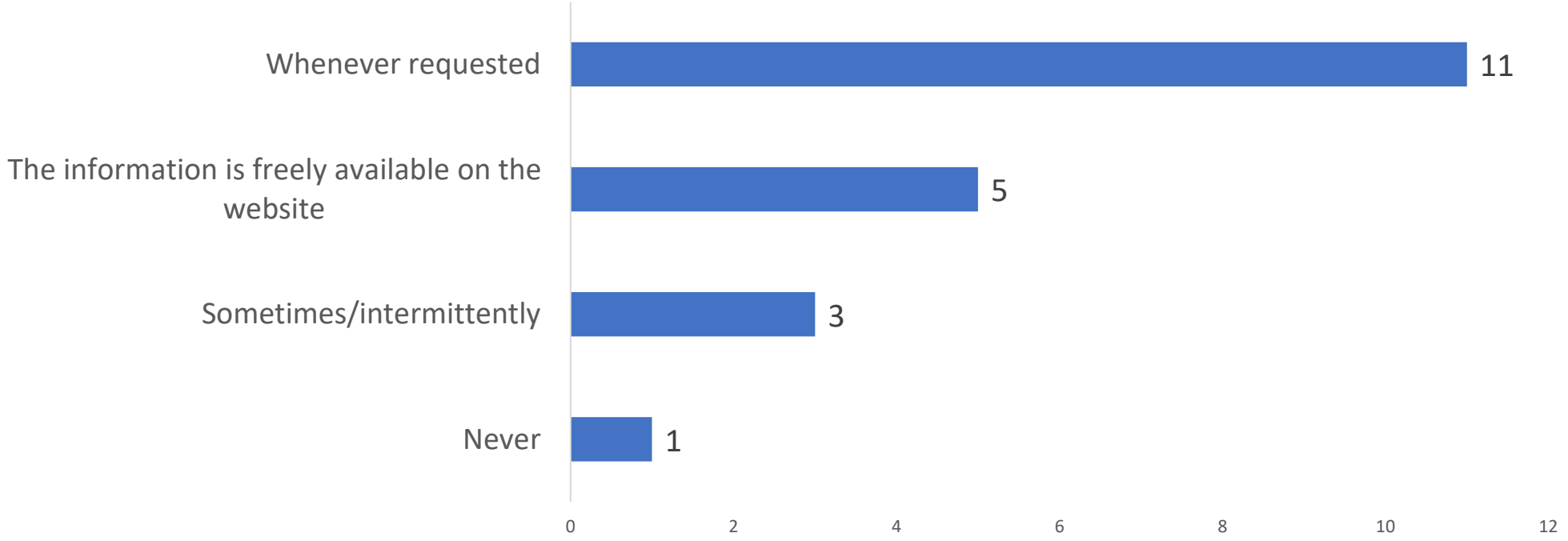
How often is the **NMA contacted by doctors** with questions on how to **disclose patients' information to third parties** according to derogations from national law?

In the absence of official data, perception or personal experience were sufficient



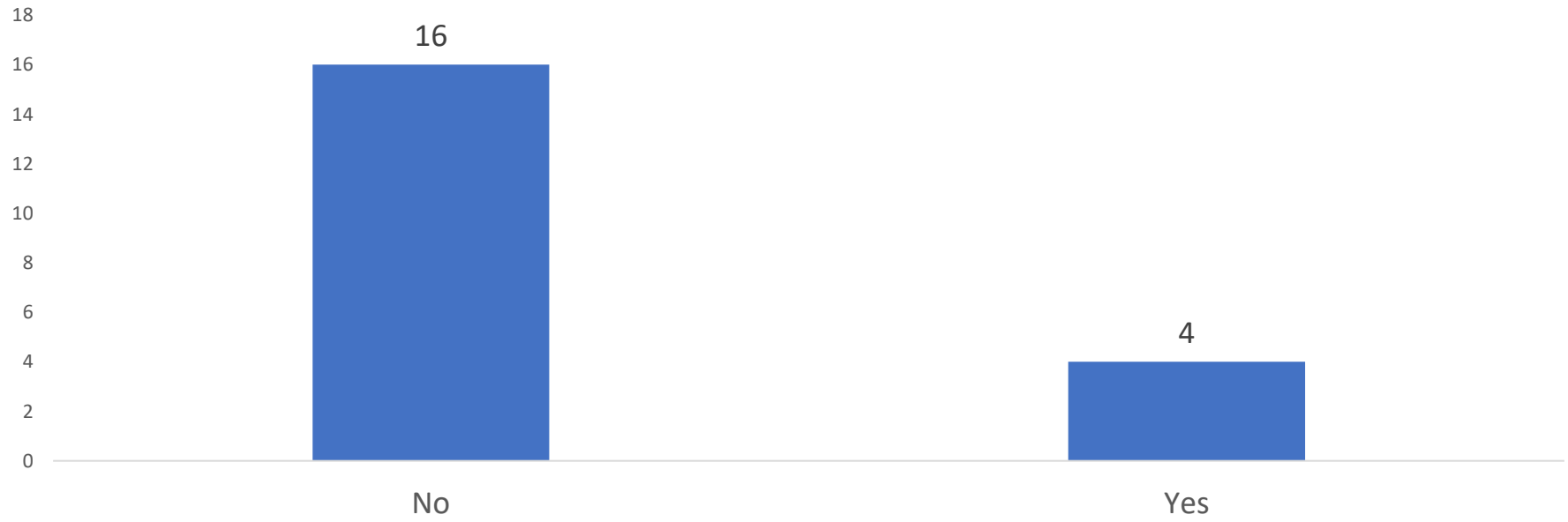
Excerpt Results of Survey on Medical Confidentiality

Does your NMA provide **guidelines/legal assistance** to doctors on when they are **allowed to disclose information** about a patient to third parties?



Excerpt Results of Survey on Medical Confidentiality

Do you find any **discrepancies between national law and deontology** (rules of professional conduct/ethical self-regulation) in relation to medical confidentiality?



Excerpt Results of NMAs Survey on Medical Confidentiality

Among those who found discrepancies in relation to medical confidentiality, the following discrepancies were noted:

- **Technological means to protect medical confidentiality are insufficient**

One national medical association calls for a legislative framework that provides clarity for sharing sensitive health information and ensuring core principles of doctor/patient confidentiality are respected.

- **Legal definition and legal derogations are outdated**

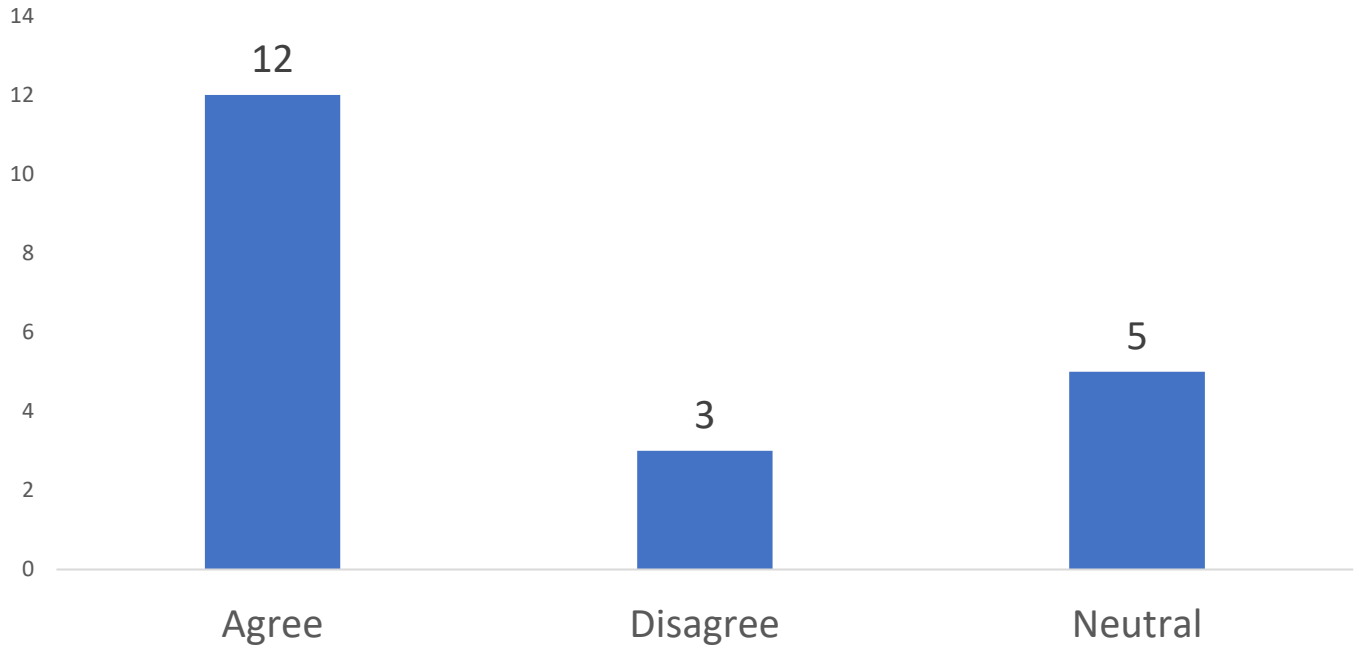
- **Legal definition is stricter than the deontological code**

One national medical association reported that competent authorities at national level interpret the GDPR and national legislation very strictly, making reasonable practical action difficult and thus can impact patient safety.

- **Patient does not want his/her health status to be recorded**, but doctors are obliged to do so

Results of Survey on Medical Confidentiality

I am satisfied with how medical practices are applying the principle of medical confidentiality when using electronic health records.
In the absence of official data, your perception or personal experience is sufficient.



One national medical association commented that the fragmentation of EHR systems does not allow a qualified statement, though medical confidentiality is strictly upheld regardless of the transmission or acquisition method of information to provide healthcare. **Secure channels for transmitting medical information are needed.**

Excerpt Results of Survey on Medical Confidentiality

For countries who "agree"

Please specify a few best practice measures medical practices have adopted to safeguard medical confidentiality when using electronic health records, if possible

Four main areas can be distinguished:

Legal aspects	• Legislation establishing conditions (restrictions) to access to patients' health records • Rules on EHRs (e.g. "Norm for information security in healthcare")
Patient's role	• Restricting access from different entities
Operational aspects	• A data matrix must be respected as who can be recipient of medical information • Education • Doctors are unaware of effective security mechanisms and have no control over EHRs, particularly in hospital settings

Results of Survey on Medical Confidentiality

Cont.

Technical aspects

- ❑ Implementing log systems
- ❑ Unique health identifiers, double factor authentication, secure information sharing channels
- ❑ Locking when idle, revision tracks and audits
- ❑ Public service EHRs - centralised systems equipped against hacking, password protected access, time limitation;
- ❑ Private practices opt for EHRs contracts with reputable companies offering appropriate safeguards
- ❑ Role-based access controls (RBAC) and use of smart cards in conjunction with personal passcode
  - RBAC model allows HCPs proportionate access to relevant information in the EHRs where needed, and only when they are involved in their care. Role-based access models can control: i) Who has access to information; ii) What information can be accessed; and iii) Under what circumstances information can be accessed.
  - Use of smart cards – health staff and HCPs who have a justified need to view personal and clinical information appropriate to their role are issued with a smartcard which allows them access to the appropriate level of patient information. Smartcards are used in conjunction with a passcode known only to the smartcard holder. They provide secure and auditable access to clinical systems. Each smartcard has RBAC assigned which allows the user to be electronically authenticated each time they view a patient record. This role will determine what each user can see and what they can do in a patient record.

Excerpt Results of Survey on Medical Confidentiality

For countries who were "neutral"

Please indicate any suggestions for medical practices to safeguard medical confidentiality when using electronic health records, if possible

Legal aspects	• Limit scope of authorised entities accessing medical records without medical education (e.g. access only to doctors and strictly defined HCPs identified by national legislation) • Develop data sharing policies (strict rules for sharing with 3rd parties and storage on servers must meet security standards) • Ensure legal compliance with GDPR
Patient's role	• Increase patient awareness about how their data is used and ability to control access to their records
Operational aspects	• Medical doctors should better protect their credentials for access to electronic records. • Roles and permissions better defined (e.g admin staff should not have access to full medical records); • Regularly train staff on data privacy and security (e.g. identifying cyber threats and protecting sensitive data); • Implement secure data sharing practices; • Develop a data back-up and recovery plan (e.g. emergencies plans, in the event of attack or other emergencies)

Excerpt Results of Survey on Medical Confidentiality

Cont.

Technical Aspects

- **Roles and permissions** (based on job roles, e.g admin staff should not have access to full medical records);
- Regularly **train staff** on data privacy and security (e.g. identifying cyber threats and protecting sensitive data);
- Implement **secure data sharing practices**;
- Develop a **data back-up and**
- **recovery plan (e.g.** emergencies plans, in the event of attack or other emergencies)

Excerpt Results of Survey on Medical Confidentiality

For countries who "disagree":
Please specify a few measures which in your view medical practices should adopt to safeguard medical confidentiality when using electronic health records, if possible

- ❑ Strict cyber security measures, training on cyber security for medical professionals
- ❑ Secure access to the system with a robust authentication policy;
- ❑ Secure communication with other healthcare professionals and patients;
- ❑ Protect premises.
- ❑ Patients must be informed of how their data is processed and how they can exercise their rights.
- ❑ Provide for specific authorisations ("clearances") so that each health care professional or member of staff of the health care institution has access only to the files that he or she needs.

Excerpt Results of Survey on Medical Confidentiality

Which risks are most likely to compromise medical confidentiality when using electronic health records?

Please rank from top (higher risk) to bottom (lowest risk). Perceptions or personal experience were considered in the absence of official data

Out of 20 responses:

- The **most likely risks** are 'ransomware', 'hacking of health information', 'lack of training on health data management'
- The **lowest-ranking** risk is 'black-out'
- Other **risks identified:**
  - Tired or burnt-out staff
  - Healthcare professionals accessing patient records of patients not in their care (e.g. ex-spouse, family members or curiosity in smaller communities).

Excerpt Results of Survey on Medical Confidentiality

Which measures are most important to safeguard the risks of electronic health records?
Please rank them from top (most important) to bottom (least important).

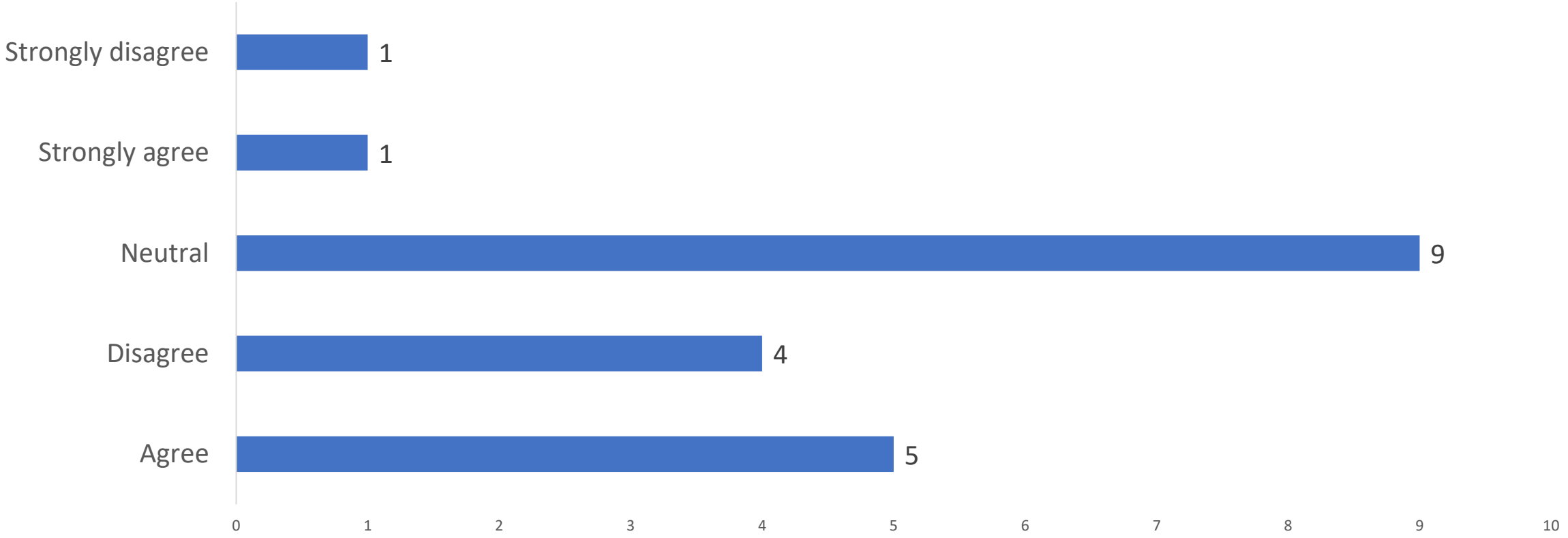
Out of 20 responses:

- the **highest-ranked** measures are:
  - Having rigorous access systems (password or fingerprint protected)
  - Robust cybersecurity systems in place against unauthorised access, disclosure, alteration
  - Provision of data management training

- the l**owest-ranking** measure:
  - Contractual regulation of the confidentiality of health information

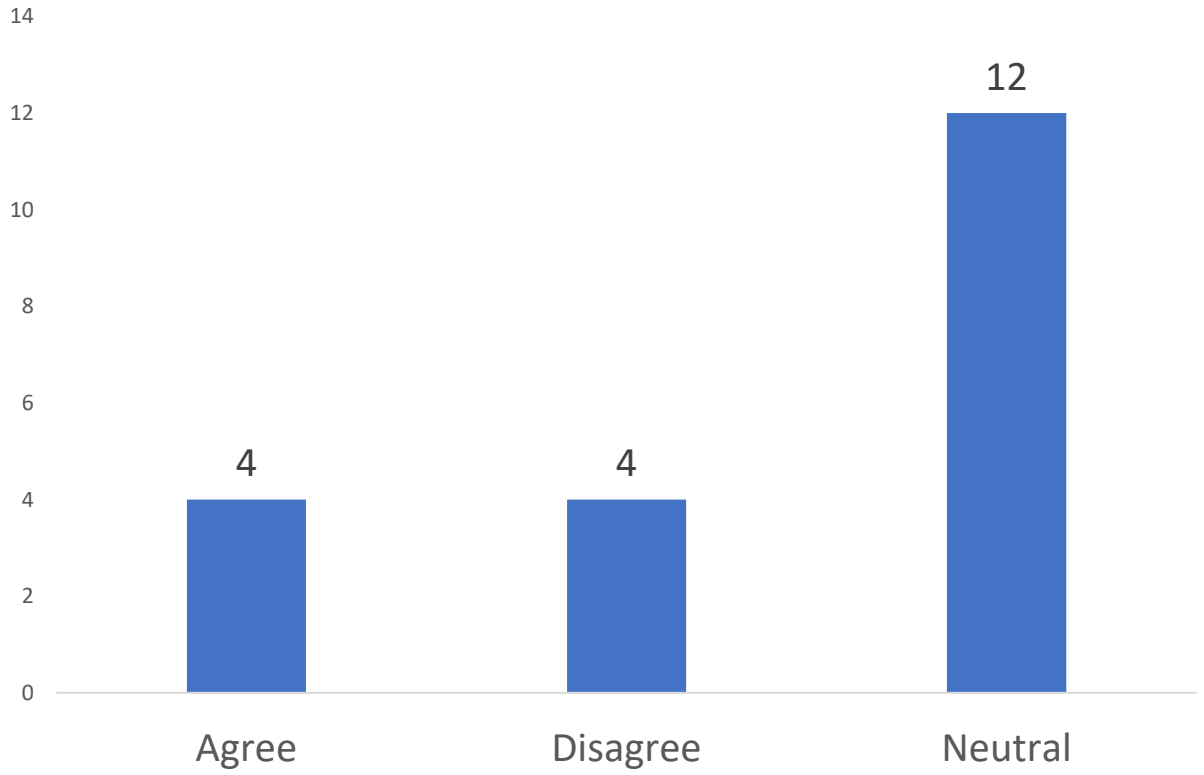
Excerpt Results of Survey on Medical Confidentiality

The digitisation of healthcare will improve medical confidentiality in the future.



Results of Survey on Medical Confidentiality

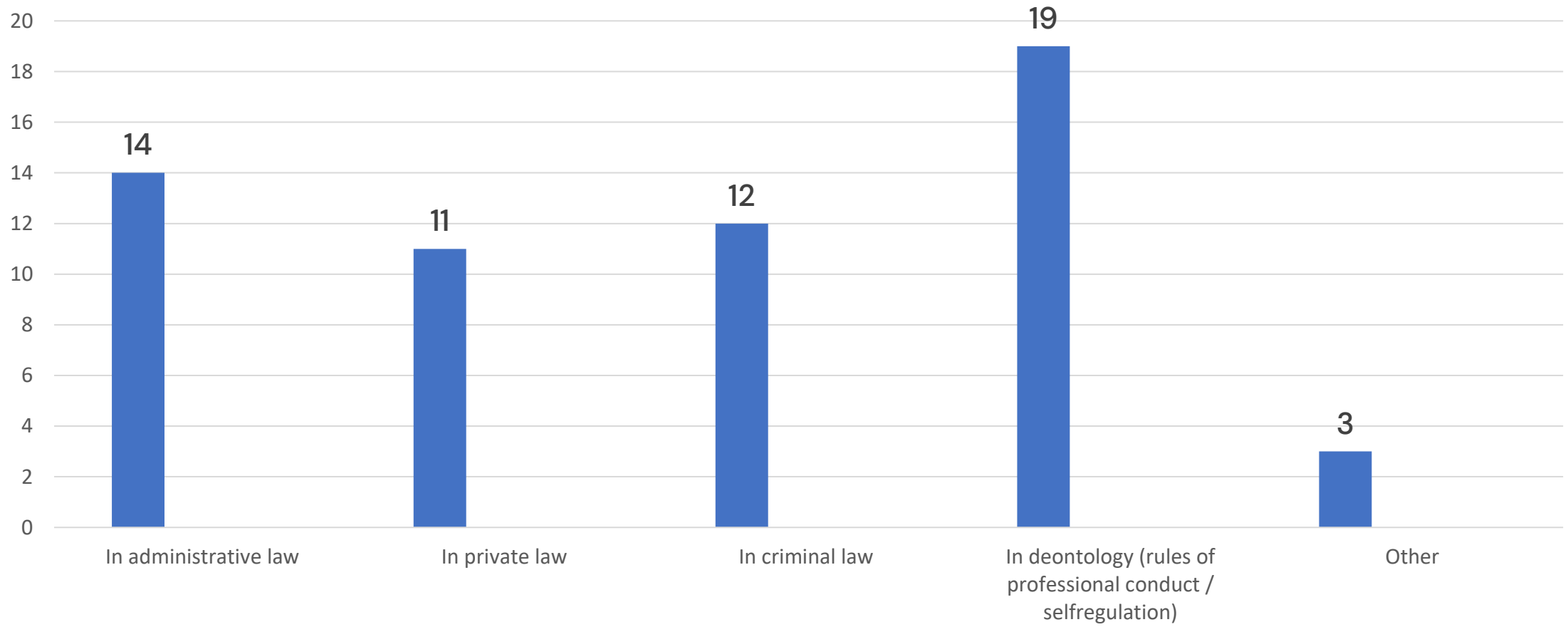
There have been positive developments in medical confidentiality after the COVID-19 pandemic (since 2020).



One national medical association commented that the COVID-19 emergency required information to be shared more quickly and widely than normal across organisations. Long-standing and valued concepts of confidentiality principles were not abandoned (e.g. regulations to assist the flow of confidential information in a public health emergency were adopted and applied; the government issued notices under these powers instructing healthcare organisations to share and use data to support the provision of healthcare services, for disease surveillance to protect public health, and for monitoring the response to the COVID-19 emergency; the notices provided time-limited access to health data to inform crucial work to respond to the pandemic.)

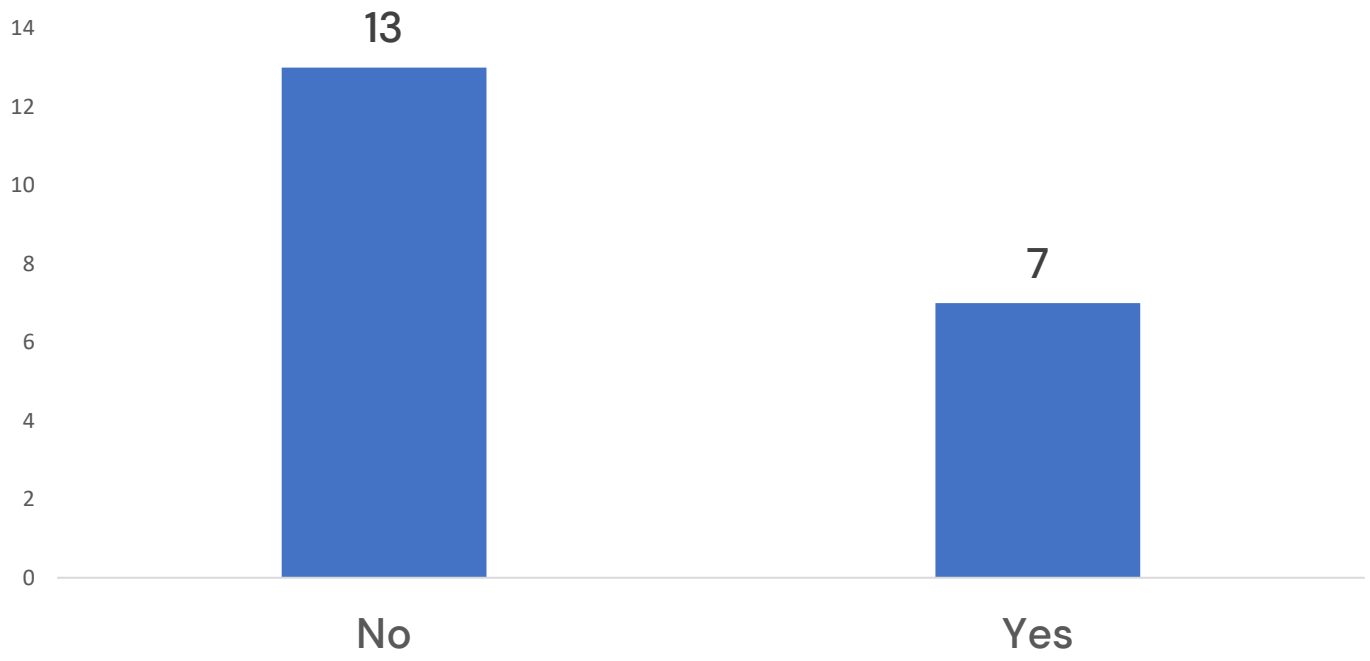
Excerpt Results of Survey on Medical Confidentiality

How is medical confidentiality safeguarded in your country?



Excerpt Results of Survey on Medical Confidentiality

Is your organisation/ National Medical Association (NMA) considering amending its deontology code (rules of professional conduct or ethical self-regulation) to adapt to advancements brought by healthcare technology and electronic health data management?

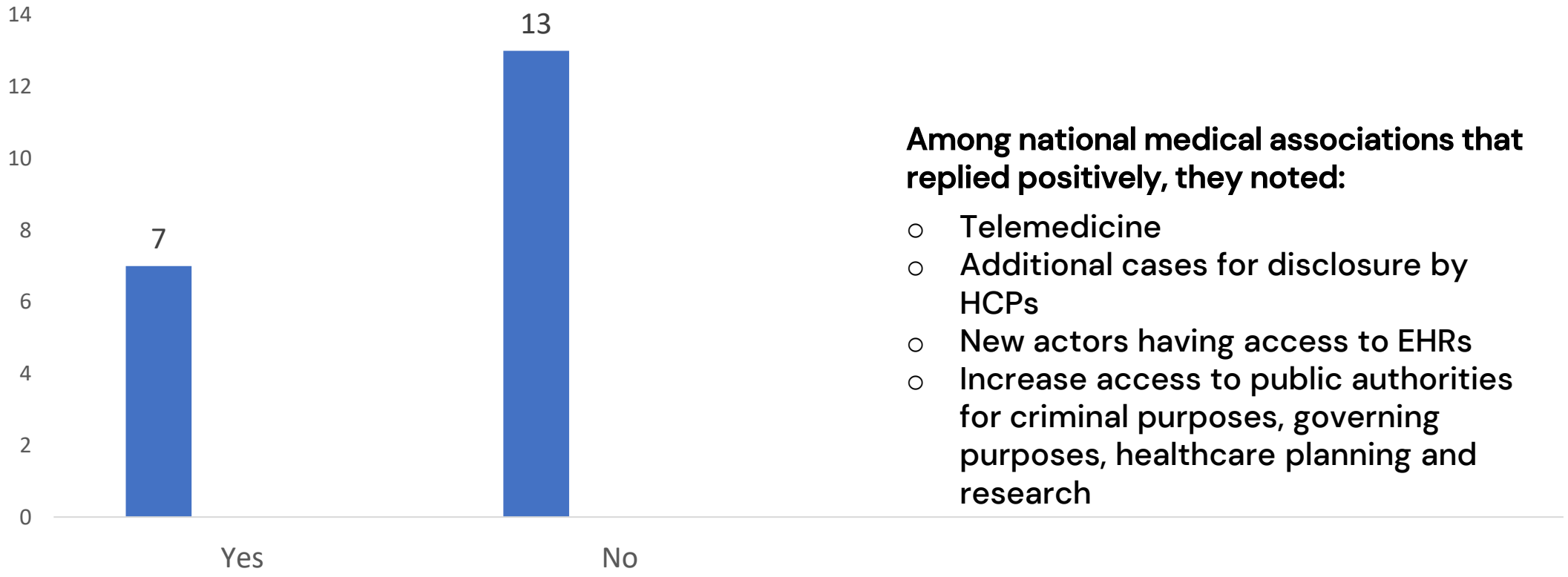


Please specify briefly the main changes:

- One national medical association commented that the code would be changed in the future, once clear legal rules are set.
- One national medical association commented that the proposed amendment to the code called for the addition of a new article on the use of digital health technologies by doctors.
- One national medical association commented that it would be very likely a change in the code, but work was still ongoing.

Excerpt Results of Survey on Medical Confidentiality

Are there any recent national legislative proposals that can raise concerns to the principle of medical confidentiality?



Among national medical associations that replied positively, they noted:

- Telemedicine
- Additional cases for disclosure by HCPs
- New actors having access to EHRs
- Increase access to public authorities for criminal purposes, governing purposes, healthcare planning and research

Excerpt Results of Survey on Medical Confidentiality

Recommendations / additional comments on the digitisation of healthcare:

Recommendations received can be grouped in three main areas:

1) Security

- Secure access to the EHR system with a robust authentication policy.
- Secure telemedicine, remote access, cloud-based health systems
- Secure communication with other healthcare professionals and patients, and protect premises
- Protect data on mobile devices
- Educate patients and providers on data security

2) Transparency in patient-doctor relationship

- Patients must be informed of how their data is processed and how they can exercise their rights.
- Patients should be allowed to exclude certain healthcare provider groups from certain information in all cases.

3) Improvement of internal processes/organisation

- A clear datamatrix should be developed where it is clear to everyone which health data can be accessed by which healthcare provider.
- Provide for specific authorisations ("clearances") so that each healthcare professional or member of staff of the healthcare institution has access only to the files that he/she needs.
- Implement strong data sharing policies

Conclusions

1. Medical confidentiality (MC) remains very important for medical practice and the reference to the Hippocratic Oath continues to be relevant for this principle/obligation.
2. Main reasons to safeguard MC are the (1st) protection of patient's privacy (unanimous), (2nd) ensuring trust in the healthcare system, and (3rd) the protection of patient's health. Other reasons included to avoid discrimination, national security, protect the autonomy of the profession.
3. The majority of respondents agree that MC may be compromised with the use of EHRs in their country, although 1/3 disagree.
4. The entities that can most compromise MC are (1st) other healthcare professionals, 2nd non-medical employers, 3rd family members. **This leads to conclude that educating staff on MC is paramount.** Other entities compromising, e.g. media, criminal organisations, foreign governments, and legislation (forcing disclosure)
5. The most common reasons to disclose patient's data to third parties is (1st) patient voluntary consent, (2nd) legal obligation (duty to disclose) and (3rd) legal authorisation (voluntary to disclose). The lowest reason to disclose is to defend doctor's dignity and honour.
6. In relation to questions about national derogations on how to disclose patients' information to third parties, in some countries, NMA's are contacted often, while others not so frequently. Responses are provided whenever requested but few countries have that information available on their NMA's website.

Conclusions

7. Most respondents **do not find discrepancies** between national law and deontology in relation to MC. Within those few countries where discrepancies exist, these relate to technology being insufficient to protect MC, to the legal definition and derogations being outdated, to the legal definition being stricter, and to patient's requests of not registering not being respected.

8. Based on perception, most respondents are satisfied with how medical practices are applying medical confidentiality when using EHRs.

9. **Best practices** to safeguard MC in EHRs can be grouped into **four** main areas: **technical aspects** (security), **patient's role** and transparency in the patient-doctor relationship, **operational aspects** (improvement of internal processes/organisation/education) and **legal aspects.** These areas are common/transversal whether respondents were satisfied, not satisfied or remained neutral to how MC is being dealt in EHRs.

10. The most likely risks to compromise MC when using EHRs are i) ransomware, ii) hacking of health information, and iii) lack of training on health data management. Other risks not included in the pre-identified list, were tired or burnt-out staff, and HCPs accessing EHRs of patients not in their care.

11. The most important measures to safeguard the risks of EHRs are a i) rigorous access systems (password or fingerprint protected), ii) robust cybersecurity systems in place against unauthorised access, disclosure, alteration, iii) provision of data management training

Conclusions

12. Most respondents are neutral on whether digitalisation will improve MC in the future, although there is some optimism among respondents.
13. **The practical implementation of EHRs implies further assessment on MC.**
14. Recommendation for **only sharing pseudonymised data (already at the source),** and to balance confidentiality, availability and data integrity where the patient shows a preference on a specific element (e.g. confidentiality over availability, or vice-versa).
15. In some countries, secure channels for transmitting medical information are currently insufficient or non-existent.
16. Digitalisation must not serve as a reason for breaching or downgrading medical confidentiality.
17. Respondents generally agree to actively support the disclosure of EHRs to competent authorities in secondary use, as long as appropriate safeguards are in place. BUT there are some exceptions.
18. **National medical associations are invited to prepare a toolkit, including guidelines, to support doctors with secondary use obligations.**

Thank you for your attention

For more information, please contact **CPME Secretariat: Sara Roda (sara.roda@cpme.eu)**

+32 2 732 72 02 | secretariat@cpme.eu | www.cpme.eu | @ CPME_Europa

CPME MEDECINS EUROPEENS
EUROPEAN DOCTORS