

KING KHALID UNIVERSITY

Who may know?

Medical Ethics • MED 431 • Lecture 4

Privacy and confidentiality

Husain Alkhalidy

Three things that will happen in your first clinical week

- A colleague photographs a chest X-ray with an unusual finding and posts it to the department group. The name, hospital number and date of birth are in the corner.
- A husband in the waiting room stops the nurse and asks what his wife's problem is. The patient never mentioned him.
- A family meets you outside the room: “Do not tell him. He has a heart condition. The shock will kill him.”

**Patients do not trust you. They trust
the role — and that what enters the
circle stays inside it.**

Three words, and how they nest

- Privacy — the right of a person to control access to information about themselves; “the right to be left alone”
 - Physical: the body during examination · Informational: who knows what about one's health · and, more broadly, decisional and associational privacy
- Confidentiality — the obligation of the person who receives private information within a relationship of trust to use it only for the purpose it was disclosed for, and not to share it without consent
 - Relational: it arises because of the relationship, and it is the physician's obligation, not an option
- Secrecy — simply keeping information hidden; broader and more passive than confidentiality
- **Privacy is the wide term. Confidentiality is its application to the information inside the circle**

Where the duty comes from: the profession

- Hippocrates: “What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself”
- The WMA Declaration of Geneva: “I will respect the secrets that are confided in me, even after the patient has died”
- The WMA Code: it is ethical to disclose when the patient consents, or when there is a real and imminent threat of harm that can only be removed by a breach
- Three values underneath: autonomy — the information belongs to the patient · dignity — a history should not define a person socially · trust — without it, patients do not disclose
- **Twenty-four centuries, one rule, and one shape of exception**

Where the duty comes from: the Sharia

- “Do not spy on one another” — al-Hujurat 49:12
- “Whoever conceals the faults of a Muslim in this world, Allah will conceal his faults on the Day of Resurrection” — Muslim
- Amanah (أمانة): what the patient discloses is placed in your hands as a trust; betraying it is a moral failing of the gravest kind, not only a professional one
- Ghaybah (غيبه): the unauthorised disclosure of another's private affairs, prohibited whether or not it is true
- **The Code of Ethics opens its confidentiality section with the Sharia, and the Law's Article 5 requires the patient's rights to be respected “in accordance with the Sharia's principles”**

What breaches actually look like

- Most breaches are unintentional: an unguarded conversation, a misdirected document, a screen left open, a bay curtain that was never drawn
- Some are deliberate: looking up a record you have no clinical reason to open
- The consequences, for the patient: embarrassment, stigma, a lost job, worse mental illness
- For the physician: a complaint to the hospital, to the Commission, and legal action
- For the student: a complaint to the College — and the same legal exposure
- **Before opening any record, two questions: do I need this to provide care to this patient, and do I have the patient's consent, implied or express, to access it?**

1 - In practice

The ward round, the examination, the record, the corridor

The ward round

- The ward round is an inherently privacy-compromising activity: diagnosis, results, social history and plan may be audible to every patient in the bay
- Minimise the exposure: draw the curtains, lower the voice, take sensitive discussions to a private room
- Bedside teaching needs the patient's explicit consent. A patient who consented to admission has not consented to being a teaching case
- The Code, Chapter 8: the patient must know they are in a teaching institution and that you are a trainee; the teacher decides what is suitable to discuss in front of trainees
- **The Bill of Rights, §4: privacy and confidentiality when discussing the patient's treatment programme — with the patient or the legal guardian**

Physical privacy: the examination

- The Code, Chapter 7: exposing the awra is prohibited unless there is necessity — then expose only what the purpose needs, for as long as it needs, before as few people as it needs
 - A practitioner of the same sex where one can be found; no exception for the clinical training of students and interns — use the educational alternatives
- The Bill of Rights, §4: private parts covered except what treatment requires; a separate room if the patient's own is unsuitable; a person of the same gender present; no longer in the examination room than necessary
- No examinations in corridors or waiting areas; only relevant staff enter; no unrelated non-hospital person present; proper clothing on the ward and full covering during transfer
- **Always take permission before the examination begins. Give the patient time to expose the part themselves**

The record

- The record is confidential. Access is restricted to those involved in the patient's care
- Unauthorised access — out of curiosity, a colleague's or relative's record without clinical justification — is a serious breach even if nothing is ever shared
- The Code, Chapter 9: the record is kept where only the professionally related may handle it; it belongs to the institution; the patient may see it and have a copy
- The Bill of Rights, §4: access to the file is limited to the treating team, those authorised by the facility's management, the patient or guardian, and the judicial authorities
- **The Data Protection Law, Article 23: access to health data, including medical files, restricted to the minimum number of staff and only to the extent the service requires**

The corridor

- Discussing a case in the lift, the canteen, the corridor or at dinner is a breach if enough identifying detail is included — with or without the name
- Diagnosis, age, hospital and date together identify a person. So does “the consultant's brother-in-law on ward 4”
- The rule is simple and absolute: patient information is for clinical purposes only, and clinical discussion belongs in clinical spaces
- Ghaybah does not become permissible because the story is true, or because the listener is also a doctor
- **The Bill of Rights, §4: the patient is kept from meeting anyone not related to the provision of care — and so is the patient's story**

Consent to share: explicit and implied

- The patient's consent is the clearest and commonest exception — and it is the patient's, not the family's
- Implied: sharing within the treating team, for the purpose of the treatment the patient came for
- Explicit: anything beyond the team, or beyond the purpose — a relative, an employer, an insurer, a teaching session, a publication
 - Explicit where possible, documented, and limited to the specific information and the specific recipient authorised
- The Code, (E)3: disclosure to the family, where useful for the treatment, is permitted after seeking the patient's consent
- **When you are not sure whether you have consent, you do not. Ask**

Education, presentation, publication

- The Code, (E)4: a practitioner may disclose some of a patient's secrets for the education of other team members — limited to that purpose, and without anything that could identify the patient
- The book: anonymisation is the removal of identifying information; the Data Protection Regulation, Article 9: anonymised data are no longer personal data — only if re-identification is impossible
- A case presentation to your group: no name, no number, no date of birth, no photograph of the face; and still the patient's permission to be presented
- A case report for publication: the journal will ask for the patient's written consent; the Code requires it for any published image
- **Anonymise, anonymise, anonymise**

2 • The exceptions



Narrow, serious, and written down

The shape of every exception

- Serious — the harm to be prevented is grave, and the threat is credible and imminent
- Necessary — disclosure will prevent it, and no less privacy-invasive alternative will
- Proportionate — only the information needed, to only the people who need it
- Directed — to the person at risk, or to the official authority the rule names; never to whoever asks
- Documented — what was disclosed, to whom, on what grounds, and what the patient was told
- **Every list in this part — the Law's, the Code's, the Data Protection Law's — assumes these five tests. Apply them before you open the list**

Article 21 of the Law

- “A health practitioner shall maintain the confidentiality of information obtained in the course of his practice and may not disclose it except in the following cases”
 - (A)1 — to report a death from a criminal act, or to prevent a crime: only to the competent authorities
 - (A)2 — to report communicable or epidemic diseases
 - (A)3 — to rebut an accusation about the practitioner's competence or practice made by the patient or the family
 - (B) — if the patient agreed in writing, or if disclosure to the family is useful for the treatment
 - (C) — if ordered by a judicial authority
- **A closed list. Regulation 18-2 adds: the details of a patient's condition go to the patient, the family, or the person the patient designates — and no one else**

The Code's list

- Knowledge of a patient's secrets does not entitle the practitioner to disclose them, “except for the following exceptional conditions”:
 - 1 — to protect the patient's contacts from infection or harm: contagious disease, drug addiction, severe psychiatric illness — confined to those who may be harmed
 - 2 — to achieve a dominant interest of society or ward off an evil from it — only to the official specialised authorities: a criminal death or a crime to prevent; a communicable disease; a judicial request; a defence against the patient's accusation
 - 3 — to the family or others, where useful for the treatment, after the patient's consent
 - 4 — for the education of other team members: limited to that purpose, and de-identified
- **The Code's first exception is the Kingdom's duty to protect third parties. It is directed at the contacts, not the public**

The duty to protect: Tarasoff

- 1969: a university student tells his psychologist he intends to kill a woman who rejected him. The therapist warns no one beyond a failed attempt to have him detained. Two months later he kills her
- 1976, California Supreme Court: “the protective privilege ends where the public peril begins”
- The duty: to breach confidentiality when a patient poses a clear, serious and imminent risk to an identifiable third party
- The tests: the threat is serious, credible and imminent; disclosure is necessary and no less invasive alternative exists; the disclosure is proportionate
- **In the Kingdom the same duty is the Code's first exception, and Article 21(A)1 of the Law: to prevent a crime, to the competent authorities**

Notification, and the court

- Notifiable diseases are reported to the public health authority regardless of the patient's consent — the Ministry's list includes tuberculosis, meningococcal disease and cholera
 - Article 11: the Minister designates the diseases and the procedure; Regulation 11-3: the report goes directly or through the facility
- Suspected criminal injury: Article 11 again — a detailed report, signed by two accredited physicians (Regulation 11-1), to the security and health authorities
- A court order compels disclosure — a legal obligation that overrides the ethical one
- **These are the Law's disclosures for a purpose. Each goes to a named authority, with the information the purpose requires, and nothing more**

Abuse, danger, and the road

- The situations this course has taught for years as grounds for disclosure: abuse of a child, an elder or a spouse · public safety and violence · mental impairment · driving · communicable disease · a court order
- A four-year-old who is “not weight-bearing after a fall from a swing” has a new fracture and several healing ones. The father denies any injury
 - Report the suspicion to the child protection authority. The purpose is protection, not accusation; the authority investigates
- A bus driver with new epilepsy, told not to drive for a year, calls to say he is still driving. He cannot afford to lose the job
- **Each is a Code exception 1 or 2 case: harm to a contact, or a dominant interest of society — and each goes to the person or authority that can prevent the harm**

The spouse

- A 40-year-old woman in the gynaecology clinic has a sexually transmitted infection. Her husband stops the nurse in the waiting room and asks what the problem is
- At the desk the answer is nothing: no diagnosis, no confirmation, no hint. The nurse's duty runs to the patient in the room
- The Code, exception 1: a contagious disease may be disclosed to protect the patient's contacts from infection — confined to those who may be harmed
- The Bill of Rights, on HIV: privacy and confidentiality “to a high degree, knowing that the husband or wife has the right to know if the other party is a carrier”
- **The sequence: treat and counsel the patient; ask her to tell him; help her do it; and only if she will not, and the risk is real, disclose to him what the risk requires**

**The protective privilege ends where the
public peril begins.**

3 - The family, and the record

The request not to tell, the electronic record, and WhatsApp

The right belongs to the patient

- In Arab and Muslim families the family is central and active in healthcare. That reality does not alter the principle: the right to confidentiality belongs to the patient, not to the family
- The family's love, concern and emotional investment do not entitle them to information the patient has not authorised
- The Law, Article 21(B) and Regulation 18-2, name the family as a permitted recipient where disclosure is useful for treatment; the Code, (E)3, adds “after seeking the patient's consent”
- So: ask the patient, early and privately, who may know what — and write the answer in the record
- **A daughter who was told the diagnosis has not been authorised to hear the prognosis, and her brother has not been authorised at all**

The family veto

- The request: “Do not tell him he has cancer.” Four problems with granting it
 - It violates the patient's autonomy over information about their own body
 - It rests on a false premise: most patients want to know their diagnosis, and say so when asked
 - It destroys trust when the patient discovers, as they usually do, that they were deceived
 - It impedes care: a patient who does not know cannot consent to treatment, plan, or say goodbye
- The Law, Article 18, gives the physician latitude in incurable disease to decide whether to inform the patient or the family — unless the patient has forbidden it, or has designated who is to be told
- **The Law's latitude is exercised by the physician on the patient's behalf. It is not a veto for the family**

How to do it

- Meet the family first. Acknowledge the fear: they are trying to protect him, and you are on the same side
- Then see the patient alone, and ask before you tell: “Some people want every detail, some prefer their family to handle it. What would you like?”
- Disclose at the patient's pace, in the patient's words, with the family present if the patient wishes
- If the patient truly prefers not to know, that is his choice, and it is recorded as his — not the family's
- **Case 6.4: he says, “Doctor, I need you to be straight with me. What did you find?” — the question that ends the discussion**

The electronic record

- The same accessibility that helps care means one breach can expose thousands of records at once
- Access only the records of patients under your care · use only authorised, secure platforms · log out when you leave the screen
- Report unauthorised access or a security breach immediately — the facility must notify the authority within 72 hours (Regulation, Article 24), and the patient where it harms them (Law, Article 20)
- Never photograph or screenshot a patient record
- **The audit trail is permanent. Every record you open is logged against your name, and the log is the first thing an investigation reads**

WhatsApp

- Consumer messaging for clinical communication is widespread and ethically problematic: personal devices are lost, stolen and shared; group chats forward patient information and images routinely, usually without consent
- The framework: patient information travels only on approved, encrypted, institutionally governed platforms
- Where clinical necessity forces an unofficial channel: anonymise maximally, and obtain explicit consent for any identifying clinical image
- Lecture 3's rule for the class group applies with more force on the ward: never patient information
- **A department group of twelve is a publication to twelve people, each with a screenshot key**

Photographs of patients: the Code's rules

- The rule: patients are not photographed or recorded, in whole or in part, except for a need required by their care, medical education, or health research
 - Tell the patient the purpose and where the image will be used; obtain consent from the patient or the proxy; never pressure; the patient may withdraw consent even afterwards; a minor's or unconscious patient's guardian consents, and the patient may withdraw on waking
 - No publication in the media, including new media, without written permission, and nothing that could identify the patient; a face only with the eyes covered, unless there is a scientific need
 - Kept without consent, exclusively: images of internal organs, histology slides, endoscopic images, and diagnostic imaging
- **The Law, Regulation 5-3: no photographing or publishing of procedures without written consent, the facility's approval, an approved scientific purpose, and no offence to public morals**

Social media, briefly

- Lecture 3 covered e-professionalism. One reminder belongs here: a patient is identified by the combination — diagnosis, age, hospital and date — with or without the name
- The Data Protection Law calls a post “publishing”: making personal data available by any written, audio or visual means
- A patient's health data are Sensitive Data under Article 1. Publishing them in violation of the Law, to harm or for personal benefit, is the offence in Article 35
- **The white coat in the photograph makes you identifiable. The whiteboard behind you makes the patient identifiable. Case 2.2 is both**

**Anonymise, anonymise, anonymise.
When in doubt, ask.**

4 • The law

Three instruments, one rule

Three instruments at a glance

The Law • M/59, 1426H

- Article 21: the duty, and the closed list of exceptions
- Article 11: reporting criminal injury and notifiable disease
- Article 18 and Regulation 18-2: who may be told the details of a condition
- Regulation 5-3: photographing or publishing procedures
- Article 31: breach of a duty or of the Code is a disciplinary offence

Bill of Rights • MOH

- §4 Privacy and confidentiality: discussion in private; private parts covered; no disclosure, misuse, circulation or access without consent, except the judicial authorities
- File access limited to the treating team, those authorised by management, the patient or guardian, and the courts
- Separate room, same-gender presence, no unrelated visitors
- AIDS: the spouse's right to know

Data Protection Law • M/19, 1443H

- Article 1: health data is Sensitive Data
- Article 4: the patient's rights over their data
- Articles 15 and 16: when disclosure is, and is not, permitted
- Article 23: access to health data at the minimum necessary
- Article 20 and Regulation 24: breach notification within 72 hours
- Articles 35 and 36: the penalties

The Data Protection Law: definitions and rights

- Personal data: anything that identifies an individual, directly or indirectly — name, number, address, images, and combinations that point to one person
- Health data: any personal data related to an individual's physical, mental or psychological condition, or to the health services they received
- Sensitive data includes health data and genetic data — alongside religion, ethnicity, criminal record, and biometrics
- Article 4 — the patient's rights: to be told the purpose of collection; to access their data; to obtain a copy in a readable format; to have it corrected or completed; to have it destroyed when no longer needed
- Article 5 — no processing, and no change of purpose, without consent, except where the Law itself provides; consent may be withdrawn at any time
- **The record you write is the patient's personal data. The Law gives them a copy of it as a right, not a favour**

Article 15: when disclosure is permitted

- “The Controller may not disclose personal data except in the following situations”:
 - 1 — the data subject consents
 - 2 — the data were collected from a publicly available source
 - 3 — a public entity requires them for public interest or security, to implement another law, or to fulfil judicial requirements
 - 4 — disclosure is necessary to protect public health, public safety, or the lives or health of specific individuals
 - 5 — the data will be processed only in a form that makes identification impossible
 - 6 — a legitimate interest of the controller — never where sensitive data are involved
- **Article 16 then forbids disclosure under 1, 2, 5 or 6 if it would compromise an individual's safety, violate another person's privacy, or breach a professional obligation. Article 21 of the older Law is one such obligation**

Articles 23, 20, 35 and 36

- Article 23 — health data: access, including to medical files, restricted to the minimum number of staff and only to the extent the service requires; the Regulation's Article 26 adds graded access, documented stages, and a named person responsible for each
- Article 20 — breach: the facility notifies the authority, and the patient where they are harmed; Regulation 24: within 72 hours of becoming aware
- Article 35 — anyone who discloses or publishes sensitive data in violation of the Law, with the intention of harming the data subject or achieving a personal benefit: imprisonment of up to two years, a fine of up to three million riyals, or both; the Public Prosecution prosecutes; the fine may be doubled on recidivism
- Article 36 — any other violation: a warning, or a fine of up to five million riyals
- **A screenshot forwarded “as a joke” is a disclosure of sensitive data. Whether it was for benefit is a question for the prosecutor, not for you**



Three instruments, one rule: inside the circle, the information is the patient's. Outside it, nobody may know without consent — except where the law names the case, the recipient, and the reason.

Now work one



Two cases from Chapter 6

Case 1 — the WhatsApp ward round

- A junior doctor photographs a chest X-ray with an unusual finding and shares it in the department group of twelve. The patient's name, hospital number and date of birth are visible in the corner
- The patient complains that they did not consent. The doctor says the purpose was educational and no harm was caused
- Which rule was broken — in the book, the Code, the Law, and the Data Protection Law? Was any exception available?
- **What should happen next — for the patient, for the doctor, and for the group?**

Case 2 — the bus driver

- A 35-year-old bus driver is diagnosed with epilepsy, started on treatment, and told he must not drive until he has been seizure-free for a year
- Two weeks later he calls: he is still driving. He cannot afford to lose the job. His employer then calls the hospital asking why he has been absent
- Three duties: to the patient, to the employer, to the public. Run the five tests on each possible disclosure
- **What do you say to him first — and what do you say to the employer?**

Work it in this order

- Whose information is it? The patient's. Say so first
- Who is asking, and by what right — the patient's consent, or a rule that names them?
- Which rule: consent, Article 21 of the Law, the Code's four exceptions, Article 15 of the Data Protection Law?
- The five tests: serious, necessary, proportionate, directed, documented
- **What do you say to the patient — and what do you write in the record?**

Before next time

- This week's second lecture: patients with special needs — Chapter 12
- Week 14, after the autumn break: surgery, women and children, and the end of life — Chapters 9, 8 and 10
- Work the four cases at the end of Chapter 6; the spouse and the family veto were done today, the X-ray and the driver are yours to write up
- Read the Patient Bill of Rights, §4, and Articles 1, 4, 15, 23 and 35 of the Personal Data Protection Law — both on Blackboard under Lectures
- **And before your next ward day: find out which platform your hospital has approved for clinical messages. If the answer is none, the answer is none**



Who may know?