DRAFT: August 2012
Information Risk Assessment: Use of Short Messaging Service (SMS) in NHSScotland

Executive Summary

The information risks relating to SMS are wide-ranging, particularly in regard to a new wave of more complex patient services that allow inbound and outbound traffic and which contain some sensitive personal data. Many risks are obvious, such as unreliability of transport (a message passes through email/Internet and cellular infrastructure to a variety of devices) and the risk of messages read by non-intended persons due to many reasons beyond the board's control. But some risks are less obvious and can have more impact such as the inability to deal with in-bound texts and patient demand because of lack of staff capacity/process, staff copying and pasting highly sensitive content direct from emails into SMS, buying an SMS bolt-on tool from an untrustworthy source or staff being told to immediately switch from SMS to email alerts to patients because of spiralling bills.

The overall exposure to information risks depends greatly on whether texting is to be used in a 'basic' structured way or in a more 'complex' ad-hoc manner for staff and patients.[1] The characteristics of both types of service (described in section 11) must be understood by decision makers at the outset so that the right controls are put in place.

The most important control is user guidance as well as informed decisions at technical design stage. If such controls are in place and working well then residual risks can be managed down greatly to acceptable levels but never removed (see matrix below). Although a relatively old tool, SMS has huge un-tapped potential and the risks associated with it are still much lower than for some of the less tried and tested digital media.

	Basic	**Complex**
Patient	Very low	Medium
Staff	Very low	Low

1) Purpose and context

This risk assessment, and associated good practice guide, has been commissioned jointly by ehealth leads and Scottish Government in response to the following:

1.1 New services for patients: Although SMS is already well established for patient appointment reminders there is now the intention to use it for a range of other and more complex purposes (e.g. test results, polling, public health alerts, monitoring and other data capture etc). Some of these services require in-bound as well as out-bound traffic and likely to be more un-structured and contain sensitive personal

[1] Detail can be found in the Information Risk Assessment.

and/or clinical data. The expansion of such services is entirely in accordance with the eHealth strategic aim for people to be "able to communicate with NHSS using the communication channel of their choice." Information risks need to assessed before these new purposes are explored. SMS-based services can quickly multiply in a viral and sometimes uncontrollable manner to meet demand: e.g. patients get accustomed to appointment text reminders from GP and then are surprised when they do not get such texts prior to screening activities which may take place in a GP surgery. Managing expectations and putting in place necessary capacity to meet demands can be difficult even for relatively old and simple technologies such as SMS.

1.2 New national email/SMS service pending: Some boards currently rely heavily on NHSMail, via the Cable and Wireless contract, to provide their SMS services. And even in boards with NHS.uk email accounts it is standard to find nhs.net accounts opened up specifically so that the SMS function can be used. With the exception of some GP and dental practices, it is currently uncommon to find other companies providing SMS for boards. But this will soon change. The national NHSS email service (due c. 2014) has SMS as an optional bolt-on rather than a 'must have' requirement. So if the chosen supplier does not have SMS integrated into its offering (or the SMS module is not selected on cost or other grounds) then boards will need to make their own arrangements. Differences in pricing models and functionality will mean that there are likely to be lots of smaller bolt-on SMS services. Some of the technical controls used to mitigate information risks need to be considered before companies are signed up.

1.3 Billing models and staff behaviour: The financial cost of consuming NHSMail-originated SMS services has until recently been rather opaque to boards as billing was absorbed centrally. This has meant that the problem of staff sending high volumes of long text messages for example (which deliver only first part of message) and the lack of clarity over who should even be using SMS for different purposes has not been addressed.[2] Such concatenated messages create information risks and can be an unnecessary drain on resources i.e. the monthly bill could be reduced by x if staff kept to the character limit.[3] Moving to the position where boards do know exactly how many texts are sent (and by whom) should in theory iron out some of the wastage. But there could be unintended information risks if for example a team was instructed to switch to email for patient communications because SMS was becoming too expensive. Instead, there needs to be an information risk assessment of which channel is suitable for the purpose rather than which is cheapest.

1.4 SMS and internal communications: Another outcome of the NHSmail/SMS integration is that staff now use SMS extensively for internal communications. The highest proportion of messages are from generic accounts and part of well structured services (e.g. staff-rostering, business continuity alerts). But there is evidence that SMS is also being used increasingly in a much more ad-hoc manner (e.g. cutting

[2] Cable and Wireless/Connecting for Health: Using NHSmail with applications (March 2012) states "if using SMS as an alerting or notification system you should ensure you have carried out a relevant risk assessment in relation to the limitation of SMS, particularly its insecure nature and lack of delivery guarantee."

[3] In April 2012 xx fragments were sent which represent xx messages. If staff kept to a formula of '20 words per message' then the number would be reduced by x.

and pasting an email and sending as texts to colleagues). Given that users of NHSMail can already access emails remotely on any internet-enabled device (including a personally-owned mobile device) it raises questions as to why SMS is being used in this way. Although sending highly sensitive emails intra-NHSScotland (to/from nhs.uk to nhs.net) has been deemed permissible the same is not true of the less reliable and less secure SMS.[4] Building on the email guidance, staff need to be made aware of the limitations of SMS and types of information that it should not be used for (internally and externally).

2) Scope and limitations

This is a high level assessment that encompasses every possible type of SMS service currently used or being proposed in NHSScotland. Evidence was collected between May and July 2012 via interview (e.g. eHealth clinical lead, practice nurse, vendors of SMS products, National Services Scotland, who currently manage NHSMail, and board information security officers) as well as using published UK case studies. It is designed to provide a framework for boards to use when risk assessing new services (rather than a replacement for local assessment).

3) Risk analysis methodology

Firstly, a broad-brush assessment is made of the five main business impacts – in terms of confidentiality, integrity and availability – relating to SMS. This is then followed by a determination of the threats and the vulnerabilities that could lead to them being realised. These are then ranked according to relative likelihood and impact and plotted out on a risk matrix. The risks are then grouped into clusters and prioritised according to what is known about the stated aims and risk appetite of NHSScotland.

Finally, a set of controls (people/procedural and technical) are recommended with an indication of what residual risk is still left.

A key control is in the form of 'good practice guidance' and this is appended.

4) Negative business impacts

There is a perception that SMS poses little or no risk because of the small amount of content a standard message contains. But there are some negative impacts when things go wrong:

[4] NHSMail Good Practice Guide (2012); highly sensitive email can be shared between official NHSScotland email addresses subject to handling instructions. However, putting a highly sensitive email into an SMS is not permissible because the medium is far less trustworthy and reliable.

Generic Business Impacts (C)=Confidentiality (I)=Integrity (A)= Availability	**Description of worst case scenarios**
Message is delayed or not received by intended recipient (A)	This can mean the person does not do something (e.g. visit hospital) or act upon some information (e.g. employee not aware of something). The severity increases if the message relates to something important, if SMS channel is relied upon and if sender has no way of knowing that message was not received.
Message is inaccurate, incomplete, duplicated, confusing or not authentic (I)	This can mean the person does not act in the way intended (takes no action or wrong course of action that could lead to inconvenience or distress).
Message is sent to or read by non-intended recipients (C)	Breach in confidentiality; could lead to distress or harm. Severity depends on sensitivity level of information, the ease of identification of individuals and number of non-intended readers. Possible legal action, reputational damage and/or action by ICO.
Messaging service not available (A)	This can mean that persons do not act or make decisions as intended. The severity increases depending on how far SMS is relied upon and the duration of the outage.
Messaging service leads to disruption or abuse (C,I,A)	A service could be hijacked or abused in some way leading to lack of user trust in authenticity of NHS messages; senders may receive high volumes of replies or queries which they are unable to deal with and staff could be targeted as a result of their contact details being in public domain.

5) Threats and Vulnerabilities

The following potential threats and vulnerabilities have been generated as a result of interviews and known incidents. Although labelled (A, B, C, etc) they are listed in no particular order:

Threat	**Vulnerabilities**
A) Illegal Interception of data en route by third party	SS7 probes can be installed to capture data for legal intercepts. Some analysts consider GSM to be an 'un-trusted' network just like the Internet. Although signalling information on the sender etc may be captured by illegal methods it is very difficult to get actual content. Content capture is usually by other methods (see below)

B) Capture and misuse of data by telco	SMS data resides at SMS gateways and staging posts (i.e. companies providing SMS are different from the big telcos who actually do the transport). In theory the operatives at telcos/re-sellers could obtain data in bulk if they had right system permissions.
C) Recipient's phone is tampered with meaning third party can read texts	Kits can be easily purchased which allow a person to capture all inbound and outbound text messages (even if the phone owner deletes texts as they go along). To work, someone does need initial access to your phone to install software and for it to go undetected. Thereafter, they can read the messages remotely.
D) Recipient's phone has mobile applications installed which mean a provider (e.g. social network site owner) can read messages	Users often unaware of the small print that allows companies to snoop on their data, including texts, held on the SIM card.
E) Message sent to the wrong phone number(s) via the integrated email tool route	This can be simply a key stroke error; choosing the wrong number from a list. The automated aspects (e.g. mailshot to all on a list) can lead to a high volume of errors
F) Message sent to the wrong number via the manual entry route	Not all boards might use an integrated email/SMS tool. The manual ad-hoc approach is far more time consuming (e.g. practice nurse having to key into an actual telephone many times a day on a small screen) can lead to errors.
G) Capacity issues mean texts are delayed sent in wrong order or not delivered for technical reasons	Most telcos make clear in contracts that there is no guarantee of delivery let alone a specific time-frame. Speed varies depending on lots of factors including time of day, coverage, type of phone used by recipient.
H) Malicious person sends a message that purports to be from NHS	It is difficult to be sure that a text from NHS is authentic unless there is unique and clearly understood sender address identifier. Some users are bombarded by spam texts that purport to be from their bank etc.
I) Information is not all intelligible because of formatting problems	Special characters, symbols or even pictures that look fine on a smart phone/online tool may be unintelligible on more basic phones. Vulnerabilities increase if languages other than English used.
J) Perception of text bombardment (or received at anti-social times) meaning user is irritated and no longer wishes to be engaged with the health board by text.	It is difficult getting consent for different activities in NHS; and although a person may be content for texting for one specific purpose (e.g. appointments) they may not be content to receive messages in other areas (e.g. public health). Maintaining these preferences is very difficult.
K) Message not received and/or to the wrong person as a result of recipient not	It is common to give away phones to friends and family members without alerting all potential callers to this change. People often have more than one phone, change contracts etc. Difficult for NHS to keep up to date with

keeping board up to date with phone number	residential addresses let alone mobile numbers.
L) Message is received by intended recipient's phone but is not actually read	Although the sender may receive a 'message delivered' alert this does not mean that the message has actually been read for any number of reasons (e.g. a child plays with parent's phone meaning no new messages are displayed) or accidentally deleted as spam.
M) Message is delivered to intended device but is read by someone else with access to the phone (e.g. family member)	Once a message has been delivered to the device, the NHS has no control over what then happens to the message. The device may not have any PIN or form of protection meaning those with access to the device can view data.
N) Information inputted by the sender is longer than the standard 160 characters and is split up into message fragments (meaning they arrive in wrong order, or with parts missing etc)	There is nothing technically to prevent users from going over the character limit. And telcos/suppliers have no interest in stopping this as they are generally paid for each fragment.
O)Information inputted by the sender has been cut and pasted from an email in their inbox (in the case of services with SMS/email integration) without editing out parts that should not be sent via SMS and has gone astray.	It is currently easy in the case of NHSmail for existing content from emails in an inbox to be cut and pasted into a new message and sent via SMS. There is little or no user guidance that informs users what type of content should **never** be communicated by SMS. SMS could become the 'new fax' in terms of security risks.
P) Some attribute of the text message gives details of the physical and mental state and identity of the recipient and creates a breach if non-intended person reads	Although the message may reveal little or nothing about a medical condition there are often subtle ways for a non-intended reader to glean information (e.g. contact phone number or address in text can be identified with a particular area of medicine such as sexual or mental health).
Q) Recipient is distressed as there is no easy way to query content of message (e.g. ambiguous news about a test result)	Most SMS services are on a 'do not reply' basis. And the standard phone number given may not be suitable/current and lead to user 'phoning around the houses'.
R) Sender includes individual email address and/or work contact	If a sender includes own contact details for patient messaging rather than some kind of generic address then it can lead to disruption of usual channels (e.g. patient

telephone number to patients leading to administration or even personal safety problems	feels he should make direct contact with clinician rather than secretaries). Once a clinician's address is 'out there' in the public domain it could lead to unwanted emails (e.g. social engineering attack that lead to employee opening up a plausible file that has malware embedded within it).
S) Content is not understood or confusing and leads to unintended actions (e.g. which appointment, which day of the week?)	If a message is delayed it could mean that the content is out of date by the time it arrives. Often the senders of texts are not aware that the recipient may be receiving NHS texts from several sources (e.g. dentist, public health, GP etc). The desire to protect confidentiality by using cryptic language could lead to the message not being understood.
T) Message is delivered to the subject's fixed line number by mistake so the content is read as an automated voice response to whoever answers the phone	There is no clear process here such as screening out non-mobile numbers or making clear to patients that this is a mobile only service.
U) Inbound texting (i.e. from patient to board) risks	User could chose to put in highly confidential or time-critical information onto a reply without being fully aware of the risks (e.g. non-delivery, sent to wrong person etc). There is often an unrealistic expectation that something is 'secure' just because it is sent to the NHS. A person may send a message who is not on the known contact list. Employees may not consider how to deal with volumes and fact that texts cannot be diverted.

6) Likelihood

Each of the threats are ranked according to *relative* likelihood (1-5) with an indication (↔; ↑; ↓) of how far the likelihood might increase, stay the same or decrease over the next 12 months.

Threat	**Likelihood**	**Reasoning**
A) Illegal Interception of data en route by third party	1 ↔	Unlikely; no evidence of this occurring with SMS and the type of content in NHS texts unlikely to motivate an attacker to put resource here now or near future
B) Capture and misuse of data by telco	1↑	Unlikely, but there are cases of insiders selling personal mobile numbers to insurance companies etc of a target group and the risk could increase as telcos are legally obliged to keep content for longer. There are many 'cowboy' SMS re-sellers who might try to sell to NHS (e.g. dentists/GPs).
C) Recipient's phone is tampered with meaning third	1↔	Unlikely; kits are available (mainly in US). But a relatively niche area (would

party can read texts		most parents/partners resort to such tools to spy on each or use simpler methods?)
H) Malicious person sends a message that purports to be from NHS	1↑	Unlikely; no evidence of this in NHSScotland but an emerging threat as health texting takes off. Already a problem in banking, insurance and utility sectors. Nothing to stop someone prefixing a text with 'NHS'.
I) Information is not all intelligible because of formatting problems	1↓	Unlikely; as more people use online tools to send texts, so too is the temptation to use characters or even images not compatible with the most basic mobile with black and white browsers. But software is also getting cleverer to iron out these formatting issues.
D) Recipient's phone has mobile applications installed which mean a provider (e.g. social network site owner) can read messages	2↑	Will occur in a relatively small proportion; this is an emerging problem for those with latest smart phones who download social media applications.
J) Perception of text bombardment (or received at anti-social times) meaning user is irritated and no longer wishes to be engaged with the health board by text.	2↔	Will occur in a relatively small proportion even when consent is given; we know that some people are already plagued by SMS spam. As NHS texting increases so too will the likelihood of a small sub-set of recipients getting 'turned off' communicating with NHS in this way or even see it as a nuisance.
S) Content is not understood or confusing and leads to unintended actions (e.g. which appointment, which day of the week?)	2↔	Will occur in a relatively small proportion given the character length restriction it is always going to be difficult to be succinct in regard to some areas and persons with multiple conditions may have several NHS appointments and get confused.
Q) Recipient is distressed as there is no easy way to query content of message (e.g. ambiguous news about a test result)	2↑	Will occur in a relatively small proportion; virtually all current SMS services for patients are outward bound only. Not all will have a valid contact number so patient will need to phone around if further detail is required. Likelihood to grow as texting is used for more complex purposes such as test results rather than just reminders for appointments.
F) Message sent to the wrong number via the manual entry route	2↔	Will occur in a relatively small proportion; this is easy to do via key stroke error; although boards may get a

		receive receipt this does not mean it has gone to the right person. And given the relatively low sensitivity of the content in texts compared to a paper letter an unintended recipient may just ignore it rather than complain to NHS about a mystery text.
E) Message sent to the wrong phone number(s) via the integrated email tool route	2↔	As above
P) Some attribute of the text message gives details of the physical and mental state and identity of the recipient and creates a breach if non-intended person reads	2↔	Will occur in a relatively small proportion in conjunction with risks E and F; It is difficult not to mention at least something that may denote a medical condition (e.g. a particular hospital or clinician that specialises in an area of medicine is mentioned).
T) Message is delivered to the subject's fixed line number by mistake so the content is read as an automated voice response to whoever answers the phone	2↑	Will occur in a relatively small proportion by mistake; but in most cases delivery to fixed line is because the customer has made this their preference or given wrong number.
L) Message is received by intended recipient's phone but is not actually read	2↑	Will occur in a relatively small proportion; texts from NHS, provided the sender name appears clearly on the access device, do tend to get noticed. But some will be ignored or deleted in error without being read. And SMS spam is growing.
U) Inbound texting (i.e. from patient to board) risks	3↑	Likely to occur; a small number of board services currently allow inbound texting. Although boards can educate own staff on texting there will always be patients who choose to write highly sensitive things in a reply text and who rely on the text being received by the board. Once an NHS contact number is out there a board could get texts from an unknown source (e.g. "I got this number from my wife, can I also make an appointment"?)
K) Message not received and/or to the wrong person as a result of patient not keeping board up to date with phone number	3↑	Likely to occur; feed-back from boards shows how difficult it is to keep track of numbers.
M) Message is delivered to intended device but is read by someone else with access to	3↑	Likely to occur; although a traditional mobile phone may be kept about the person of the owner, a text can be

the phone (e.g. family member)		received by one or more shared device (e.g. Internet-enabled tablet kept on the sofa). Board has no control over what happens to a message once it has been delivered.
R) Sender includes individual email address and/or work contact telephone number to patients leading to administration or even personal safety problems	4↑	Highly likely to occur. The proportion of individual employee contact details enclosed in patient messages is likely to grow as more tailored services develop other than bulk appointment reminders. Standard to include personal details for internal board messaging (e.g. nurse bank).
O)Information inputted by the sender has been cut and pasted from an email in their inbox (in the case of services with SMS/email integration) without editing out parts that should not be sent via SMS and has gone astray.	5↑	Most likely; we know that this is already happening in the case of NHSmail by user statistics. Although more analysis need to be done on behaviour the fact that so many texts are fragments (i.e. parts of a message) suggests people are not tailoring short messages but pasting in longer ones without sufficient editing.
G) Capacity issues mean texts are delayed, sent in wrong order or not delivered for technical reasons	5↔	Most likely; we know that this is already happening. Suppliers do not offer any formal SLAs. Far fewer texts get through than for email etc. Telcos have increased capacity greatly but this risk will never go away.
N) Information inputted by the sender is longer than the standard 160 characters and is split up into message fragments (meaning they arrive in wrong order, or with parts missing etc)	5↔	Most likely; statistics in regard to NHSmail show a high proportion of fragments being sent (rather than users keeping to 160 characters). There is not the functionality to stop users from doing this.

7) Impact

Each of the threats are ranked according to *relative* impact on NHSScotland organisations. Note: although there are instances where there might be substantial privacy impacts on individuals (e.g. a family member snooping on another by looking at messages) not all of these would have an impact on the board if it could demonstrate to a regulator like ICO that these areas were beyond its control.

Threat	**Impact**	**Reasoning**
T) Message is delivered to subject's fixed line number by mistake so the content	1	Lowest impact for board; could mean unintended person in shared house-hold listens to message. Board may be

is read as an automated voice response to whoever answers the phone		able to demonstrate that it sent message to the number provided by user and can update preferences to mobile for future messages.
I) Information is not all intelligible because of formatting problems	1	Lowest impact for board; could create inconvenience for some recipients but if the whole message not understood could check with board about missing words using contact number/address.
J) Perception of text bombardment (or received at anti-social times) meaning user is irritated and no longer wishes to be engaged with the health board by text.	1	Low impact; user does have the option to change communications preferences and with the exception of public health messages (e.g. anti-smoking) patients in the main find well targeted NHS messages helpful.
C) Recipient's phone is tampered with meaning third party can read texts	2	Low impact; there is some impact in terms of privacy to the individual but this is not strictly a risk the board can control or be responsible for in terms of the law.
D) Recipient's phone has mobile applications installed which mean a provider (e.g. social network site owner) can read messages	2	Low impact; there is some impact in terms of privacy to the individual but this is not strictly a risk the board can control or be responsible for in terms of the law.
M) Message is delivered to intended device but is read by someone else with access to the phone (e.g. family member)	2	Low impact; there is some impact in terms of privacy to the individual but this is not strictly a risk the board can control or be responsible for in terms of the law.
H) Malicious person sends a message that purports to be from NHS	2	Low impact; there is some potential inconvenience to the individual and increases if it can be proven the NHS failed to take reasonable steps to ensure patients know what an authentic NHS text looks like (e.g. email address/identifier).
G) Capacity issues mean texts are delayed, sent in wrong order or not delivered for technical reasons	3	Medium impact; patient or employee is not alerted to something and texting service is not working as intended. Impact increases if there is a single point of failure (e.g. whole of NHSScotland relies on email to deliver its SMS).
L) Message is received by intended recipient's phone but is not actually read	3	Medium impact; patient or employee is not alerted to something and texting service is not working as intended

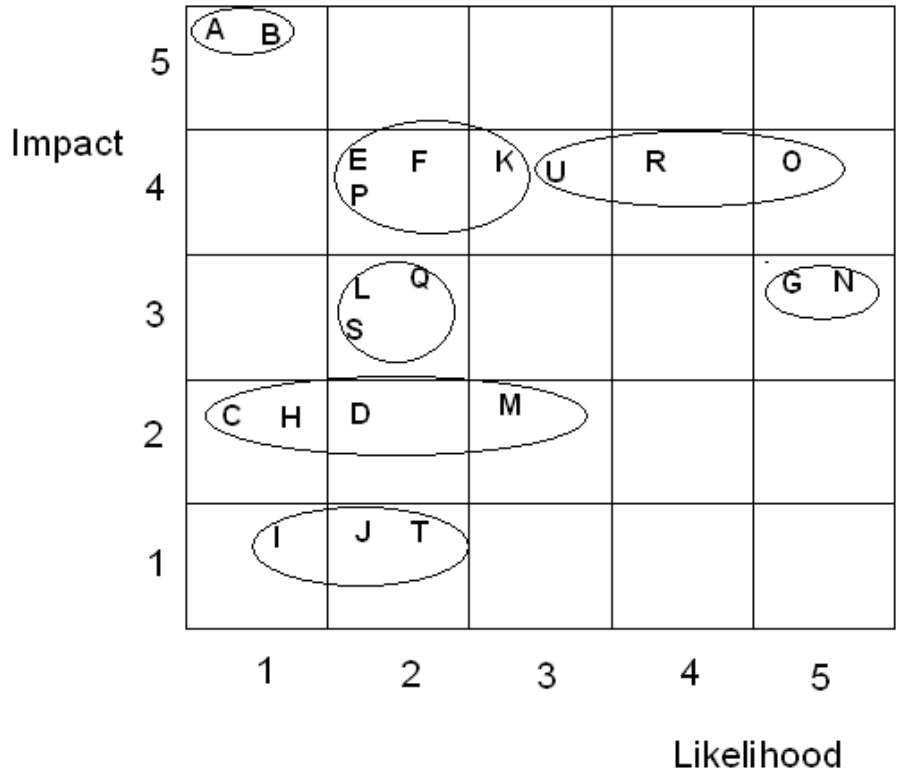
N) Information inputted by the sender is longer than the standard 160 characters and is split up into message fragments (meaning they arrive in wrong order, or with parts missing etc)	3	Medium impact; patient or employee is not alerted to something and texting service is not working as intended.
Q) Recipient is distressed as there is no easy way to query content of message (e.g. ambiguous news about a test result)	3	Medium impact; patient or employee is not alerted to something and texting service is not working as intended.
S) Content is not understood or confusing and leads to unintended actions (e.g. which appointment, which day of the week?)	3	Medium impact; patient or employee is not alerted to something and texting service is not working as intended.
E) Message sent to the wrong phone number(s) via the integrated email tool route	4	Higher impact; this is a potential privacy breach in addition to the patient or employee is not alerted to something.
F) Message sent to the wrong number via the manual entry route	4	Higher impact; this is a potential privacy breach in addition to the patient or employee is not alerted to something.
K) Message not received and/or to the wrong person as a result of recipient not keeping board up to date with phone number	4	Higher impact; this is a potential privacy breach in addition to the patient or employee is not alerted to something.
P) Some attribute of the text message gives details of the physical and mental state and identity of the recipient	4	Higher impact; this is a potential privacy breach in addition to the patient or employee is not alerted to something.
U) Inbound texting (i.e. from patient to board) risks	4	Higher impact; although the patient may be the one who reveals personal details the NHS does have a duty of care if it expecting patients to reply to a service. And there is an impact if incoming message is not received by right department/clinician in a timely way etc.
O)Information inputted by the sender has been cut and pasted from an email in their inbox (in the case	4	Higher impact; cutting and pasting in this way means there is scope to send content which should never be sent via this method (i.e. equivalent of sending

of services with SMS/email integration) without editing out parts that should not be sent via SMS and has gone astray.		a 'red' highly sensitive email in fragments to the wrong address).
R) Sender includes individual email address and/or work contact telephone number to patients leading to correspondence or personal safety problems	4	Higher impact; if replies from patients are not handled efficiently then there is scope to create process failures (e.g. recipients phoning to ask "did you not get my text", messages unread due to staff unable to manage different channels). And if an employee's email address is used for malicious purposes then could have a high impact.
A) Illegal Interception of data en route by third party	5	Highest impact; if this were shown to occur then the whole service is compromised and will need to be halted. Trust severely dented and service not available for some time.
B) Capture and misuse of data by telco	5	Highest impact; as above.

8) **Risk determination and priority**

The risks, once plotted onto a matrix, can be grouped together into clusters to aid analysis. Each cluster has some common characteristic that can help eventual prioritisation and treatment plan (i.e. controls which can reduce several risks).

Fig 1: Risks plotted by likelihood and impact



	Components	Common Characteristics	Level
1	U;R;O	Relates to more complex and ad-hoc SMS services that involve sending or receiving long messages (perhaps individually composed and cut and pasted from email); where individual sender addresses/numbers are enclosed and where the recipient has an opportunity to reply to a service (creating administrative handling issues).	HIGH
2	E;F;K;P	These are all confidentiality risks relating to outbound messaging to the wrong person (whether it be via an automated or manual method or number not kept up to date) that may contain a little or a lot of information about the physical or mental state of an individual. The intended person may also not carry out a task or being alerted to something because the message has gone astray.	MEDIUM
3	G,N	A message or part of a message does not reach the intended person because of capacity issues. This is often aggravated by the fact that the message is too long (i.e. over 160 characters). There is also a threat of a single point of failure if the email tool/telco is relied upon to send out SMS	MEDIUM
4	L;Q;S	This cluster relates to where a message has arrived with the intended person but causes some inconvenience or in exceptional cases distress because some aspect of the content is not clear,	LOW

		there is no contact number to query. The message may simply not be read due to recipient deleting prematurely etc.	
5	C;H;D;M	These risks relate to a person's privacy being compromised in some way by something happening when a message has arrived onto the device (or being taken in by a spoof SMS) but are beyond the control of the NHS.	LOW
6	I;J;T	This cluster relates to where a message has arrived with the intended person but causes some inconvenience because there may be some formatting errors, it has gone to a fixed line phone or there are perceived to be simply too many messages.	LOW
7	A;B	The two risks here relate to a third party carrying out a systematic attack on NHS texting services. Although the impact is potentially very high there is no evidence that this is happening or that an attacker would find it worthwhile to put resource here.	LOW

9) Risk acceptance level and appetite

Recommendations for treatment of the risks need to take into account the following:

- **Confidentiality concerns**: Protecting patient confidentiality is central to the Information Assurance Strategy and other public pronouncements. The consequences of information going to non-intended persons (and any poor press and/or fines) are generally perceived to be higher than information risks relating to availability and integrity of SMS.
- **Low risk appetite for new services**: NHSScotland organisations are very risk averse in relation to new confidentiality risks (i.e. almost to the point where some ICT-related services such as SMS either do not happen or are delayed because of concerns about theoretical risks). But paradoxically the same organisations are slow to address pre-existing 'low tech' confidentiality risks (e.g. highly sensitive information in paper mail, misfiling patient information etc).
- **Availability and integrity concerns set to grow:** At the moment boards tend to use SMS as an added-extra to existing channels, so there is not too much impact if a message does not arrive (or is delayed). The 'best endeavours' clauses in NHSmail and other telco contracts have been accepted without question. But this is set to change as texting is used for a greater variety of purposes and where there is two-way contact with patients. The reliability of the service will become more important.
- **Bottom-up growth in SMS:** Although most boards use NHSmail for SMS there is no extant NHSScotland SMS policy or national guidance.[5] In a sense

[5] NHSmail in its user manual recommend local risk assessments where SMS integration is used. But this has generally not happened and any member of staff can use this functionality.

the 'genie is out of the bottle' as there is no technical way to prevent users from accessing the current SMS service or going over 160 characters. But there is scope in relation to email replacement (and bolt on SMS services) to have governance in place from the start (i.e. who can use SMS for different purposes?). Some NHS organisations, especially dentists, already use bolt-on SMS because it gives them more functionality and control.

- **Billing issues:** Much of the current behaviour around SMS is in part determined by cost issues rather than an analysis of what channels are suitable for the purpose. If a SMS service is perceived to be 'free' (or until now had no formal per-board billing) then it may be used far more than necessary (e.g. sending long messages broken up into fragments). Conversely, a relatively high per message charge that is accurately billed per organisation could lead to use of other channels (e.g. email to patients) without assessing the new risks that this may bring.
- **Limits to NHSScotland control and risk retention:** Some risks may be medium or high but cannot be treated for technical, cost or other reasons. The cost of getting a telco to provide a service that delivers 99.5% of messages within two hours may be too high and still lead to residual risks such as a person not reading the message for other reasons beyond the telco's control. And some of the privacy risks relating to the recipient's home environment (i.e. other people reading the message or a patient replying with too much detail) are beyond the technical control of the board. But impact can be lessened through better guidance to patients and consideration over the content of outbound messages sent via this method.
- '**Quick easy wins'**: Given that a new email replacement which may or may not have integrated SMS functionality is two years away and boards are already keen to use more SMS-based services now there is a need to have some simple measures in place that are effective, low-cost and build up public trust in e-communications.

10 Recommended risk treatment plan

The recommended controls recommended are a mixture of people/procedural and technical. There are no relevant environmental controls (e.g. physical security):

Control	**Prevent messages sent longer than 160 characters**
Implement	NHSmail for example allows a user to input a long message but then only delivers the first c. 300 characters. But other standalone SMS services may be able to prevent a single message going over a pre-agreed limit or making clearer online how many characters the user has 'spent' before sending). Procedure should make clear to users that a single message should not go over standard 160 characters (e.g. roughly 20 English words with spaces).
Residual Risk	Can be greatly reduced if staff follow guidance but cannot be removed completely. A bi-product of this is potential cost savings.

Control	**Provide only designated staff integrated SMS/email functionality for patient services**

Implement	Currently this cannot be achieved technically with NHSmail. But there are products that manage permissions (i.e. only segment of staff can use the service) for bolt-on services. Procedure should make clear which staff can use structured or un-unstructured texting services to patients and/or staff. There cannot be a 'free for all'.
Residual Risk	Can reduce the risks greatly by focussing on structured services to patients and staff. But there will always be some ad-hoc texting direct from staff to patients and staff need to be better aware of the risks when patients then reply directly.

Controls	**Prevent 'copying and pasting' emails into texts**
Implement	Currently this cannot be achieved technically with NHSmail. But controls over message length and over who use the service will help. Staff training is main control (i.e. dangers of pasting un-edited emails into SMS and that 'red' level email content should never be texted). Greater promotion of other means to get email while away from desk (i.e. both nhs.net and nhs.uk services allow access via mobile devices) would help.
Residual Risk	Going to be difficult to remove risk entirely as long as there is the functionality to do it.

Controls	**Keeping to pre-agreed character formats**
Implement	May be able to prevent use of special characters etc but otherwise simple advice to users on standard upper and lower case letters, basic punctuation and numbers only. Need to test if non-English language to be used.
Residual Risk	Can almost eliminate this risk if simple format is followed.

Controls	**Preventing delivery to fixed line numbers**
Implement	Some services do screen out non-mobile numbers. Can legitimately state to customers that service is mobile only (and persons with special needs still get voice calls etc)
Residual Risk	Can almost eliminate this risk if the policy is adopted.

Controls	**Agreed contact number/address with every message**
Implement	It could be a principle that any message should be accompanied by an agreed phone number/address: Note: often the sender's full address/number does not appear as a header so the contact details could be at end of message.
Residual Risk	Can almost eliminate this risk if the policy is adopted.

Controls	**Due diligence when contracting SMS providers**
Implement	There are a plethora of companies providing SMS services as a package which may or may not be managed via an eHealth

	department. These vary from large established telcos with a good record to small untested start-ups that may have a short commercial life and are basically re-sellers making a business out of charging premium rates per transaction without any knowledge of the strict Information Governance expected in NHS. The architecture in place is often opaque (i.e. where is the SMS server based? Who is actually doing your transport?).As part of procurement/purchase need to check out resilience and security.
Residual Risk	Can greatly reduce the risks of abuse by third party if suitable checks are made prior to signing company up and if there is some control in the boards over who can purchase SMS services.

Controls	**Employee guidance on un-structured outbound messaging to patients**
Implement	No technical way of supporting this. Clinician may wish to use a work mobile phone number/email address to contact specific patients in an ad-hoc manner (in addition to the more structured bulk texting services managed by administrative staff using online tools). Need to respect the judgement of clinicians while pointing out some of the risks (e.g. patient then circumvents normal channels and putting individual email address in public domain) and provide some 'model messages'.
Residual Risk	As services become more personalised this will always remain a risk area. But clinicians would argue the benefits of using text in this way outweigh any confidentiality risks as the amount of content is more limited than might be received by paper mail. But the risk of NHS staff being targeted for spam or malware, because their email address is in public domain, is set to grow.

Controls	**Administrative staff have process for in-bound texts**
Implement	Where texting is two way (i.e. patient can reply) thought needs to be given as to which staff will handle them, what number/email box is to be used and whether some kind of receipt needs to be given to the sender. Capacity and channel management issues need to be considered (i.e. a patient may reply to a text with a text. But equally could phone/email in addition to the text). To also consider how to manage texts which come from un-known sources. (e.g. to make voice call). To consider that although phone messages can be diverted when someone is away text messages cannot.
Residual Risk	Provided the process (e.g. return message for blood-sugar for diabetes patients) is thought through the risk can be reduced greatly

Controls	**Guidance to patients to manage expectations**
Implement	When a patient consents to one or more text based services he/she needs to clear what type of content will be received, how often, what to do with the contact number enclosed. In the case of inbound services needs to know how to reply (i.e. keeping content to minimum), the risks of messages not getting through, whether there will be a read-receipt from NHS etc and importance of keeping organisation up to date with their phone number. At the same time it

	needs to be clear that although NHS will take care in what messages it sends it cannot control how you use your device or who you share the information with (e.g. if you decide to not put a PIN on your phone etc).
Residual Risk	The risks can be reduced substantially if a board is clear and upfront with patients about the limitations of the service. But the '24/7 connected online' generation of patients with mobile devices often have unrealistic expectations as to how quickly the NHS can respond.

Controls	**Devise model content formulae which reveal little or nothing about mental or physical state OR business sensitive information**
Implement	For appointment reminders using online tools this is already common. But for other services (e.g. test results) a formula needs to be pre-agreed. Particular attention needs to be paid to the address/contact number as this can indicate health (e.g. snooping family member wonders why teenager has a text from x clinic and 'Googles' telephone number). This means that if the message is sent to a non-intended recipient there is a negligible breach in privacy (just inconvenience). In the case of internal texting to colleagues it needs to be clear via guidance that the content should if at all possible be unclassified and never above 'amber' (or PROTECT level). For example it is better to text a colleague to say "check your email, clinical director is concerned" than to cut and paste a sensitive email from the clinical director and send it as several SMS fragments.
Residual Risk	The risk can be reduced substantially. But in the case of unstructured texting a lot more detail could be revealed and it is possible (even with consent) that a sensitive message could go adrift as with paper mail.

Controls	**Management of contact lists in email/online tools**
Implement	Structured messaging services allow an operative to pull patient or colleagues names from a list. Given the similarity of many names the tools can often be configured to show several fields at once (e.g. surname, first name, post-code, name of dentist, mobile number etc) so there is greater certainty the right person has been selected for the message. Auto-population should be avoided.
Residual Risk	The risk of sending to wrong person can be reduced but never avoided completely.

Controls	**Use of delivery receipts**
Implement	To use the delivery receipt functionality to monitor the effectiveness of the service. i.e. if only 80% of texts seem to be getting through that might lead to some investigation as to why this is the case (e.g. telco problems, out of date contact lists, target group such as elderly not switching on phones often enough etc).
Residual Risk	It will always be the case that some messages will not be delivered or are delayed as SMS is not the most reliable tool. But the board is better able to plan its digital communications strategy if it can estimate the delivery rates of SMS compared to paper mail, phoning round etc).

Controls	Position SMS as a secondary communications tool or primary tool with a viable back-up
Implement	To date SMS is generally a back-up to existing channels such as appointment letters. But if SMS is chosen as the primary channel (e.g. patient prefers to get test results in this way) then a back-up must be in place (e.g. patient informed when tested that if they do not receive the text within x days then they should use agreed telephone number).
Residual Risk	Not relying on SMS means the risk of a patient/colleague not being alerted to something or behaving in way not intended is greatly reduced. But there is always a risk that some patients with mobile devices do start to expect alerts for things which the health organisation does not provide for ("I missed my bowel screening appointment because I expected you to text me just like you do for my GP and dental appointments").

11) Summary of residual risk

The overall exposure to information risks depends greatly on whether texting is to be used in a basic structured way or in a more complex ad-hoc manner for staff and patients.[6] The characteristics of both types of service (see below) need to be understood by decision makers at the outset so that the right controls are put in place.

Basic Patient Texting Services

- Texting patients and the wider public for an agreed purpose which is not mission critical (i.e. text is not relied upon as only channel).
- Relatively narrow group of staff (e.g. GP practice secretary) are trained and confident using the SMS tools.
- Usually sent in relatively high volumes (e.g. appointment reminders) using an online interface and the task has become routine.
- The message content tends to follow a pre-agreed formula with little or no personal data.
- The text cannot be replied to but a phone number or generic email address is enclosed.

Basic Staff Texting Services

- Texting staff within a board for an agreed purpose (e.g. nurse-bank, business continuity alerts). There may be quite a number of staff doing but all aware of the usage guidelines.
- Volumes vary greatly but the tasks are routine
- The message may be slightly tailored but follows guidelines (as to length, sensitivity) and does not contain patient identifiable data.
- The text cannot be replied to but either an individual or generic email address is enclosed.

[6] Detail can be found in the Information Risk Assessment.

Complex Patient Texting Services

- The board has agreed the purpose and the type of staff who should be able to use SMS in this more complex and often ad-hoc manner following an assessment of risks and benefits
- The messages are much more targeted and for niche areas (e.g. Diabetes Youth Outreach).
- Content of messages will be much more personalised (including sensitive personal data) but still within pre-agreed boundaries as to sensitivity level.
- More likely to enclose an individual email address and support replies by text and/or phone/email.

Complex Staff Texting Services

- All staff with email/SMS functionality send messages to colleagues for a variety of business purposes (e.g. alerting someone subject to guidelines/sensitivity level)
- Each message tends to be personalised and may be prompted by something received in an email (but never cut and pasted directly from an email) or a phone call.
- Only in exceptional circumstances would a patient name/identifier be enclosed (i.e. to alert a colleague to do something) but would not include any clinical data.

The most important control is 'user guidance' as well as informed decisions at technical design stage. If such controls are in place and working well then residual risks can be managed down greatly to acceptable levels but never removed (see matrix below):

	Basic	**Complex**
Patient	Very low	Medium
Staff	Very low	Low

Although a relatively old tool, SMS has huge untapped potential and the risks associated with it are still much lower than for some of the less tried and tested digital media.

DMB